Installation et mise en œuvre du module Horus

EOLE 2.6.2



création : Février 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 : Février 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 11
1. Les objectifs d'EOLE 11
2. Historique du projet EOLE 11
3. Versions des modules EOLE 15
4. Logiciel Libre 18
5. Méta-distribution EOLE 19
6. EOLE 2.6 20
7. Eolebase 22
8. Quelques références 24

Chapitre 2 - Introduction au module Horus 25
1. Qu'est ce que le module Horus ? 25
2. À qui s'adresse ce module ? 27
3. Les services Horus 27
4. Structure des conteneurs 28
5. Pré-requis 28
6. Les différences entre les versions 2.5 et 2.6 29
7. Errata 2.6.n 33

Chapitre 3 - Fonctionnement du module Horus 34
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 Horus 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 Samba : Configuration du contrôleur de domaine 98
2.6. Onglet Directeur bareos 100

2.7. Onglet Messagerie 100
3. Configuration en mode normal 102
3.1. Onglet Général 103
3.2. Onglet Services 107
3.3. Onglet Interface-0 108
3.4. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs 112
3.5. Onglet Clamav : Configuration de l'anti-virus 113
3.6. Onglet Annuaire 114
3.7. Onglet Dhcp : Configuration du serveur DHCP 114
3.8. Onglet Esu : Configuration du proxy ESU 117
3.9. Onglet Samba : Configuration du contrôleur de domaine 119
3.10. Onglet Onduleur 121
3.11. Onglet Applications web : Configuration des applications web 127
3.12. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 128
3.13. Onglet Directeur bareos 133
3.14. Onglet Stockage bareos 136
3.15. Onglet Nginx 136
3.16. Onglet Reverse proxy : Configuration du proxy inverse 137
3.17. Onglet Messagerie 141
4. Configuration en mode expert 142
4.1. Onglet Général 144
4.2. Onglet Services 148
4.3. Onglet Système 149
4.4. Onglet Sshd : Gestion SSH avancée 157
4.5. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système 158
4.6. Onglet Logs : Gestion des logs centralisés 158
4.7. Onglet Interface-0 160
4.8. Onglet Interface-n 165
4.9. Onglet Réseau avancé 170
4.10. Onglet Certificats ssl : gestion des certificats SSL 175
4.11. Onglet Dépôt tiers 181
4.12. Onglet Eoledb : Gestion des bases de données 183
4.13. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs 184
4.14. Onglet Clamav : Configuration de l'anti-virus 186
4.15. Onglet Annuaire 189
4.16. Onglet Dhcp : Configuration du serveur DHCP 190
4.17. Onglet Tftp : Configuration d'un serveur PXE/TFTP 195
4.18. Onglet Esu : Configuration du proxy ESU 196
4.19. Onglet Samba : Configuration du contrôleur de domaine 198
4.20. Onglet Nscd 205
4.21. Onglet Onduleur 206
4.22. Onglet Saltstack 211
4.23. Onglet Applications web : Configuration des applications web 211
4.24. Onglet Apache : Configuration avancée du serveur web 213
4.25. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 217
4.26. Onglet Ead-web : EAD et proxy inverse 224
4.27. Onglet Mysql : Configuration du serveur MySQL 225
4.28. Onglet Openldap : Configuration du serveur LDAP local 226
4.29. Onglet Directeur bareos 228
4.30. Onglet Stockage bareos 231
4.31. Onglet Cups : Configuration du serveur d'impression 232
4.32. Onglet Nginx 234
4.33. Onglet Applications web nginx 235
4.34. Onglet Reverse proxy : Configuration du proxy inverse 236

4.35. Onglet Proftpd : Configuration du serveur FTP 240
4.36. Onglet Messagerie 243
4.37. Onglet Eoleflask 249
5. Prise en charge d'applications supplémentaires 250
5.1. Téléchargement et mise en place 250
5.2. Configuration Apache 252
5.3. Configuration MySQL 253
5.4. Configuration du logiciel 254
6. Authentification unique avec EoleSSO 255
6.1. Présentation du produit EoleSSO 255
6.2. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 257
6.3. Protocoles supportés 264
6.3.1. Compatibilité CAS 264
6.3.2. Compatibilité SAML2 265
6.3.3. Compatibilité RSA Securid 266
6.3.4. Compatibilité OpenID Connnect 267
6.4. Gestion des attributs des utilisateurs 273
6.4.1. Ajout d'attributs calculés 274
6.4.2. Filtrage des données par application 276
6.4.3. Définition de filtres d'attributs 278
6.5. Fédération avec une entité partenaire 279
6.5.1. Déclaration d'un serveur parent 279
6.5.2. Fédération SAML : Gestion des Associations 280
6.5.3. Fédération SAML : Gestion des méta-données 285
6.5.4. Fédération SAML : Accès aux ressources 286
6.5.5. Gestion des sources d'authentification multiples 288
6.6. Personnalisation de la mire SSO 291
6.7. Configuration d'EoleSSO en mode cluster 293
6.8. Répartition de charge EoleSSO en mode cluster 296
6.9. Compléments de configuration EoleSSO 310
6.9.1. Résumé des fichiers et liens 310
6.9.2. Astuces d'exploitation 312
6.9.3. Exemple de Fédération avec RSA/FIM 312
6.9.4. Fédération entre 2 serveurs EoleSSO 314
6.9.5. Mise en place de l'authentification OTP 315
6.9.6. Application de redirection : Eole-dispatcher 317
6.9.7. Configuration du fournisseur d'identité France Connect 322
6.9.8. Configuration du fournisseur d'identité Google (Google APIs). 324
7. Activation et configuration de Bareos 325
8. Gestion des bases de données avec EoleDB 330
9. Configuration du module Eclair avec un module Horus 338
10. Mise en place de l'agrégation de liens Ethernet (bonding) 340
11. Mise en place du protocole ISCSI sur un module EOLE 341
Chapitre 7 - Instanciation du module 343
1. Principes de l'instanciation 343
2. Lancement de l'instanciation 344
2.1. Les mots de passe 344
2.2. Création d'un deuxième administrateur 345
2.3. Activation automatique de la mise à jour hebdomadaire 346
2.4. Le redémarrage 346

Chapitre 8 - Administration du module Horus 347
1. Administration généralités 347
1.1. Principes de l'administration 347
1.2. Découverte de GNU/Linux 348
1.2.1. Les Bases 348
1.2.2. Quelques Commandes 354
1.2.3. Les conteneurs 355
1.2.4. La gestion des onduleurs 355
1.2.5. Les manuels 356
1.2.6. L'éditeur de texte Vim 357
1.2.7. Les commandes à distance avec SSH 362
1.2.8. Quelques références 367
1.3. Reconfiguration 368
1.4. L'interface d'administration EAD 369
1.4.1. Principe général 370
1.4.2. Premier pas dans l'administration d'un serveur 374
1.4.3. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur 375
1.4.4. Ajout/suppression de serveurs 376
1.4.5. Surveillance de l'état du serveur 379
1.4.6. Authentification locale et SSO 382
1.4.7. Redémarrer, arrêter et reconfigurer 383
1.4.8. Mise à jour depuis l'EAD 384
1.4.9. Arrêt et redémarrage de services 384
1.4.10. Rôles et association de rôles 387
1.4.11. La console 408
1.4.12. Listing matériel 410
1.4.13. Bande passante 411
1.4.14. Résoudre des dysfonctionnements liés à l'EAD 411
1.5. L'interface d'administration EAD 3 415
1.5.1. Présentation 416
1.5.2. Installation 416
1.5.3. L'application web 416
1.5.4. Généralités sur les actions 420
1.5.5. Créer une nouvelle action 422
1.5.6. Type d'actions 424
1.5.7. Compléments techniques 427
1.6. L'interface d'administration semi-graphique 427
1.7. Les mises à jour 428
1.7.1. Les différents types de mises à jour 430
1.7.2. Les procédures de mise à jour 433
1.7.3. Ajout de dépôts supplémentaires 438
1.7.4. Désactivation temporaire des mises à jour 438
1.8. Installation manuelle de paquets 439
1.9. Les administrateurs locaux à droits restreints 440
1.10. Passage d'une version d'EOLE à une autre 441
1.11. Passage d'une version RC à une version stable 441
2. Fonctionnalités de l'EAD propres au module Horus 442
2.1. Gestion des comptes Horus 442
2.1.1. Gestion des groupes 442
2.1.2. Gestion des utilisateurs 444
2.1.3. Gestion des partages 447
2.1.4. Suppression des comptes de machine 448

2.2. Gestion fine des groupes et des utilisateurs : ACL 449
2.3. Gestion des connexions 450
2.4. Visualisation des quotas disque dans l'EAD 451
2.5. Observation des virus 453
2.6. Scripts administratifs 453
2.7. Extraction AAF 454
2.8. Réservation d'adresse IP dans l'EAD 455
3. Gestion des utilisateurs sur le module Horus 455
4. Les sauvegardes 458
4.1. Généralités sur la sauvegarde 458
4.1.1. Sauvegarde totale 458
4.1.2. Sauvegarde incrémentale 458
4.1.3. Sauvegarde différentielle 459
4.1.4. Des outils de sauvegarde 459
4.2. La sauvegarde EOLE 460
4.2.1. Le vocabulaire Bareos 460
4.2.2. Architecture de Bareos 462
4.2.3. Configuration des sauvegardes 464
4.2.4. Programmation des sauvegardes 475
4.3. La restauration des sauvegardes EOLE 477
4.3.1. Restauration complète 477
4.3.2. Restauration partielle 481
4.4. Ajouter des données à sauvegarder 485
4.5. Réinitialisation de la sauvegarde 486
4.6. bareos-webui : outil d'administration pour Bareos 486
4.7. Diagnostic, rapport et résolution de problème 490
4.7.1. Outils de diagnostic et rapport 490
4.7.2. Base de donnée sqlite de Bareos irrécupérable 492
4.8. Annexes 494
4.8.1. Autres outils d'administration pour Bareos 494
4.8.2. Quelques références 496
4.8.3. Un répertoire partagé Windows 7 comme support de sauvegarde 496
4.8.4. Un répertoire partagé Windows XP comme support de sauvegarde 499
5. Les imprimantes 504
5.1. L'interface simplifiée 504
5.2. L'interface de gestion CUPS 505
5.2.1. Création de l'imprimante 505
5.2.2. Choix du pilote 509
5.2.3. Quotas d'impression 514
5.3. Gestion des imprimantes sous Windows 514
6. Compatibilité entre GFC et le module Horus 515
7. Mise en place des sondes EQOS 515
8. Les clients Windows 516
8.1. Installation et configuration des clients Windows 516
8.1.1. Principe 516
8.1.2. Configuration réseau 516
8.1.3. Intégration et installation du client Horus automatique 517
8.1.4. Intégration et installation du client Horus manuelle 525
8.1.5. Mise à jour du client Horus 540
8.1.6. Désinstallation du client Horus 541

8.2. Administration des clients Windows 542
8.2.1. Scripts personnalisés 543
8.2.2. Les profils utilisateurs 544
8.2.3. Gestion des configurations clientes avec ESU 550
8.3. Déploiement d'applications pour Windows avec WPKG 560
8.3.1. Installation et configuration 561
8.3.2. Les packages WPKG 565
8.3.3. Journalisation des actions WPKG 569
8.3.4. WPKG scripts de pre et post installation 572
8.3.5. WPKG logiciels avec traitement particulier 576
8.3.6. Quelques références 576
9. Les clients FTP 577
10. Les applications web sur le module Horus 580
10.1. L'authentification unique avec EoleSSO 581
10.2. Applications pré-installées 581
10.2.1. phpMyAdmin : gestionnaire de base de données MySQL 582
10.3. Prise en charge d'applications supplémentaires 583
10.3.1. Téléchargement et mise en place 584
10.3.2. Configuration Apache 585
10.3.3. Configuration MySQL 586
10.3.4. Configuration du logiciel 587
11. Réplication LDAP 588
12. Transformer un module Horus en module HorusAD 591
Chapitre 9 - Personnalisation du module 596
1. Panorama des services 596
1.1. Services liés aux bases de données 596
1.1.1. eole-annuaire 596
1.1.2. eole-client-annuaire 597
1.1.3. eole-db 597
1.1.4. eole-interbase 598
1.1.5. eole-mysql 598
1.1.6. eole-postgresql 598
1.2. Services liés aux serveurs de fichiers 599
1.2.1. eole-ad-dc 599
1.2.2. eole-fichier-primaire 599
1.2.3. eole-fichier-membre 600
1.2.4. eole-cups 601
1.2.5. eole-proftpd 601
1.2.6. eole-dhcp 602
1.2.7. eole-nfs 602
1.3. Services liés au web 603
1.3.1. eole-web 603
1.3.2. eole-reverseproxy 604
1.3.3. eole-wpad 604
1.4. Services liés à la messagerie 605
1.4.1. eole-exim 605
1.4.2. eole-spamassassin 605
1.4.3. eole-courier 606
1.4.4. eole-sympa 606
1.5. Services liés au proxy et à l'authentification 607

1.5.1. eole-proxy 607
1.5.2. eole-radius 608
1.6. Services liés à la virtualisation 608
1.6.1. eole-libvirt 608
1.6.2. eole-one-frontend 609
1.6.3. eole-one-node 609
1.6.4. eole-one-singlenode 610
1.7. Autres services réseau 610
1.7.1. eole-antivirus 610
1.7.2. eole-apt-cacher-ng 611
1.7.3. eole-bareos 611
1.7.4. eole-dns 612
1.7.5. eole-dhcrelay 613
1.7.6. eole-ltsp-server 613
1.7.7. eole-nut 613
1.7.8. eole-open-iscsi 614
1.7.9. eole-pacemaker 614
1.7.10. eole-snmpd 615
1.7.11. eole-vpn 615
2. Personnalisation du serveur à l'aide de Creole 616
2.1. Répertoires utilisés par EOLE 616
2.2. Création de patch Creole 617
2.3. Les dictionnaires Creole 619
2.3.1. Ajouter un en-tête XML 619
2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu 620
2.3.3. Utiliser des familles, variables et des séparateurs 628
2.3.4. Comportement des variables 633
2.3.5. Mettre en place des contraintes 633
2.3.6. Afficher de l'aide 641
2.4. Le langage de template Creole 642
2.4.1. Déclarations du langage Creole 643
2.4.2. Fonctions prédéfinies 647
2.4.3. Utilisation avancée 651
2.4.4. Exemple 652
2.5. Le fichier de configuration Creole 653
2.6. Les scripts Creole 654
2.6.1. CreoleLint et CreoleCat 654
2.6.2. CreoleGet et CreoleSet 656
2.6.3. CreoleRun et CreoleService 659
2.6.4. CreoleLock 660
2.6.5. Indications pour la programmation 661
2.7. Ajout de script exécuté à l'instance ou au reconfigure 664
2.8. Ajout d'un test diagnose 665
2.9. Gestion des noyaux Linux 666
2.10. Gestion des tâches planifiées eole-schedule 667
2.11. Gestion du pare-feu eole-firewall 672
Chapitre 10 - Résolution de problèmes 674
1. Problèmes à la mise en œuvre 674
2. Problèmes à l'exploitation 675
3. Trouver de l'information 680
4. Demander de l'aide / Signaler un problème 683

5. Contribuer au projet EOLE 688

Chapitre 11 - Documentations techniques 690
1. Les dépôts EOLE 690
2. Gestion des journaux systèmes sur EOLE 692
3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation 693
3.1. Contexte juridique 693
3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation 694

Chapitre 12 - Compléments techniques 698
1. Les services utilisés sur le module Horus 698
1.1. eole-annuaire 698
1.2. eole-antivirus 698
1.3. eole-bareos 700
1.4. eole-client-annuaire 700
1.5. eole-cups 701
1.6. eole-dhcp 701
1.7. eole-exim 702
1.8. eole-fichier-primaire 702
1.9. eole-interbase 703
1.10. eole-mysql 703
1.11. eole-nut 704
1.12. eole-proftpd 704
1.13. eole-reverseproxy 705
1.14. eole-web 705
2. Ports utilisés sur le module Horus 706
3. L'annuaire LDAP du module Horus 708
3.1. Arborescence de l'annuaire 709
3.2. Utilisateurs spéciaux 709
3.3. Entrée ordinateur du domaine 710
3.4. Entrée partage 711
3.5. Annuaire : diagnostic et résolution de problème 711
4. La gestion du SID 713

Chapitre 13 - Questions fréquentes 715
1. Questions fréquentes communes aux modules 715
2. Questions fréquentes propres au module Horus 735
3. Questions fréquentes propres à la sauvegarde 745

Glossaire 752

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.755] :
- 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.784].

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.773] ;
  - **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.769] ;

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

- intégration d'Envole[p.760] 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.768] 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.769].

2012

- portage d'Eclair en 2.3 (juillet), repose sur ltsp-cluster, le serveur embarque le logiciel Gaspacho[p.763] ;
- 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.778] 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.778] 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.772].
- 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.769]).

  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.767] 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.769] (SSL interception) ;
  - mise à disposition des paquets `eole-fog` et `eole-lts-server` permettant respectivement la mise en œuvre de FOG[p.762] et d'un seveur LTSP[p.775] sur un module EOLE.

2023

- EOLE 2.9.0 LTS (février)
  - intégration du moteur de conteneur[p.756] Podman[p.774] 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.767].

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.

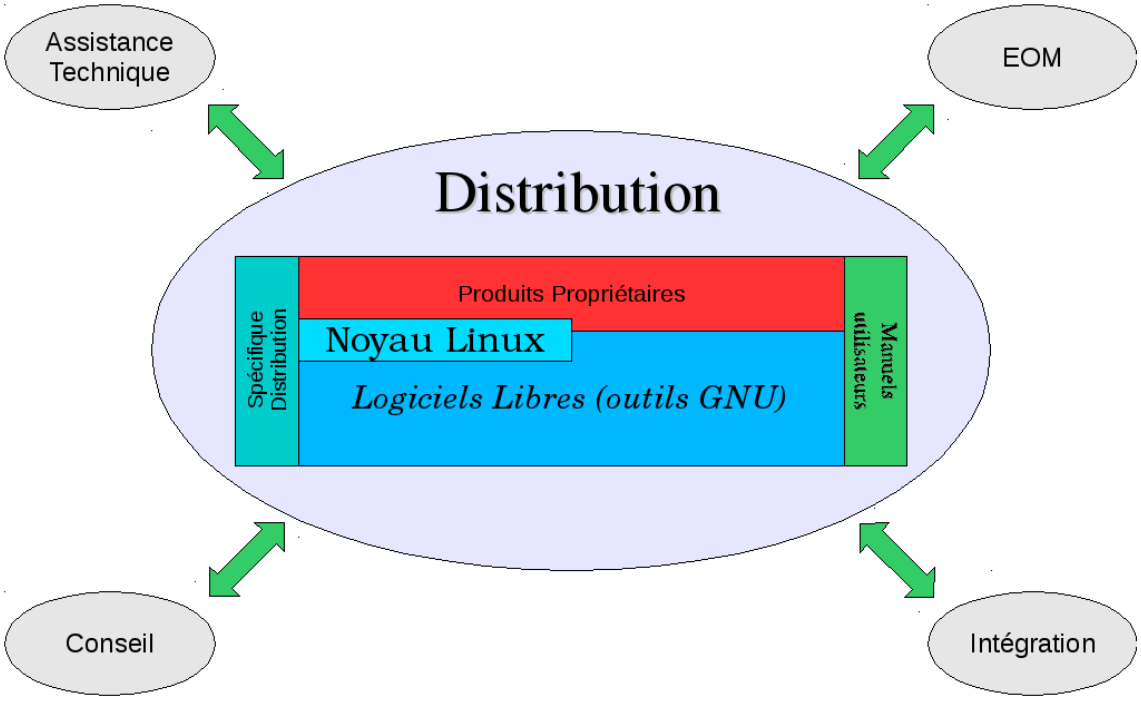
Une distribution GNU/Linux

Une distribution[p.758] GNU/Linux[p.767] 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

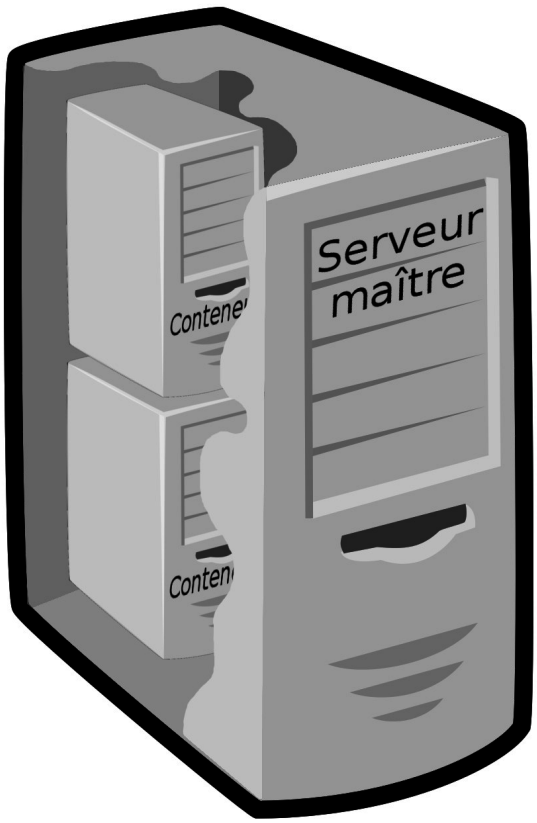
Logo officiel d'Ubuntu par Canonical Ltd

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

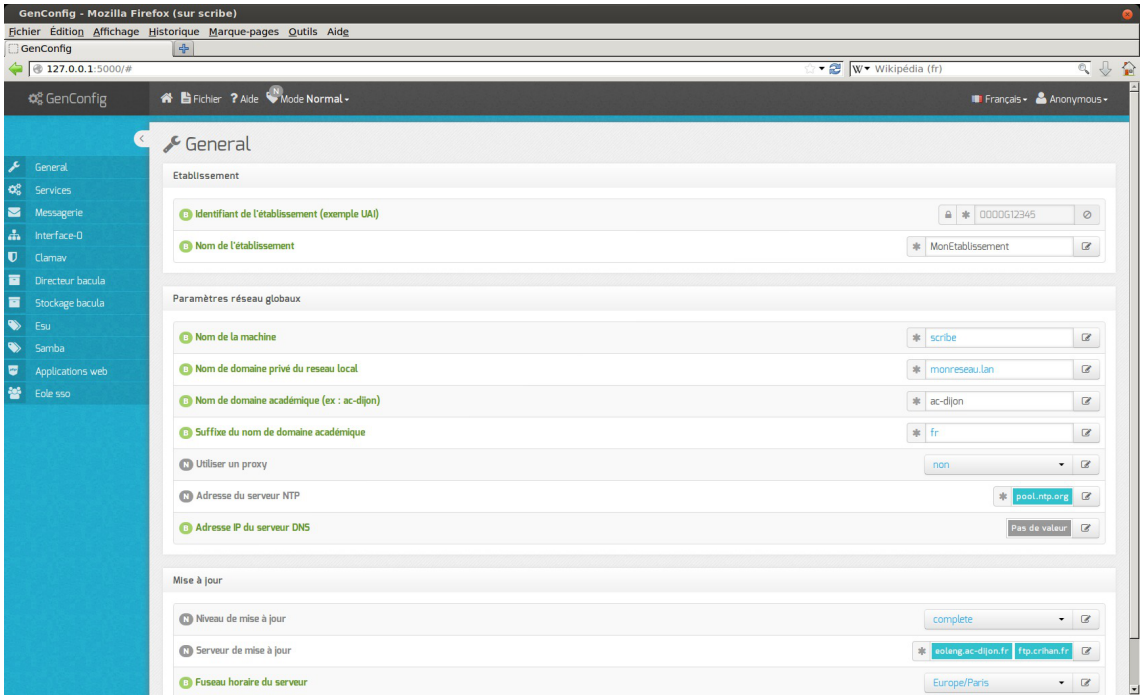
Ubuntu 16.04 LTS est disponible depuis le 21 avril 2016. Portant le label LTS[p.767], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2021. Le Pôle de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2021.

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

Module



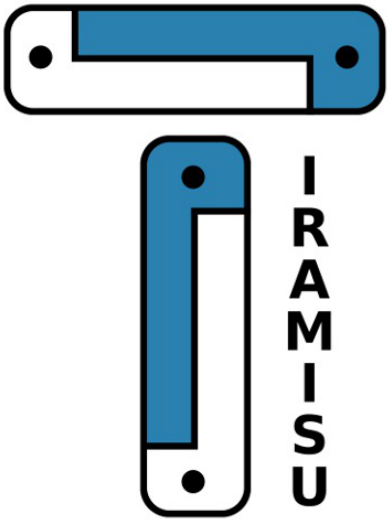
La version 2.6 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule 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.781].



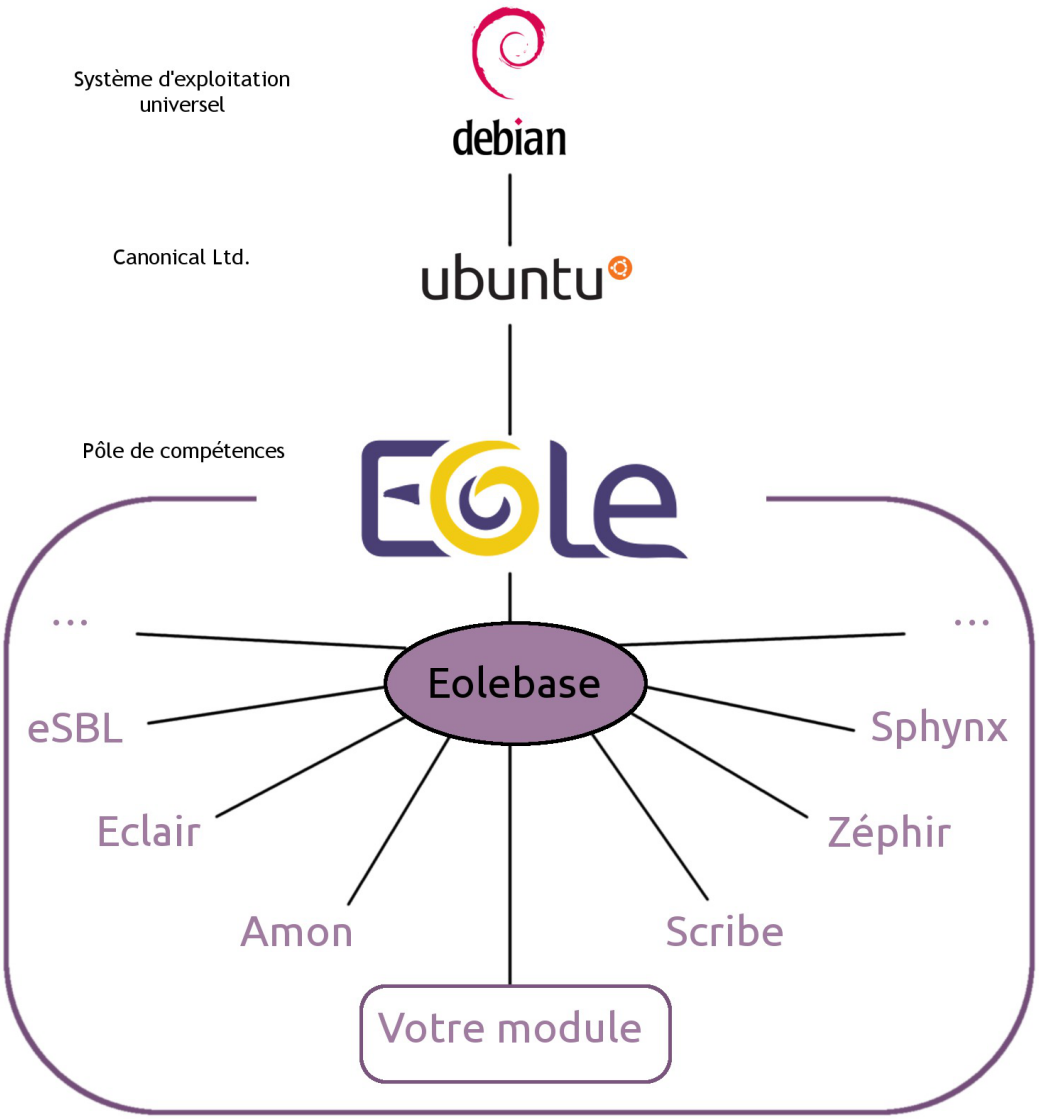
Logo du logiciel Tiramisu

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 Horus

Le module Horus est un contrôleur de domaine pour le réseau administratif d'un établissement scolaire ou d'un service académique.

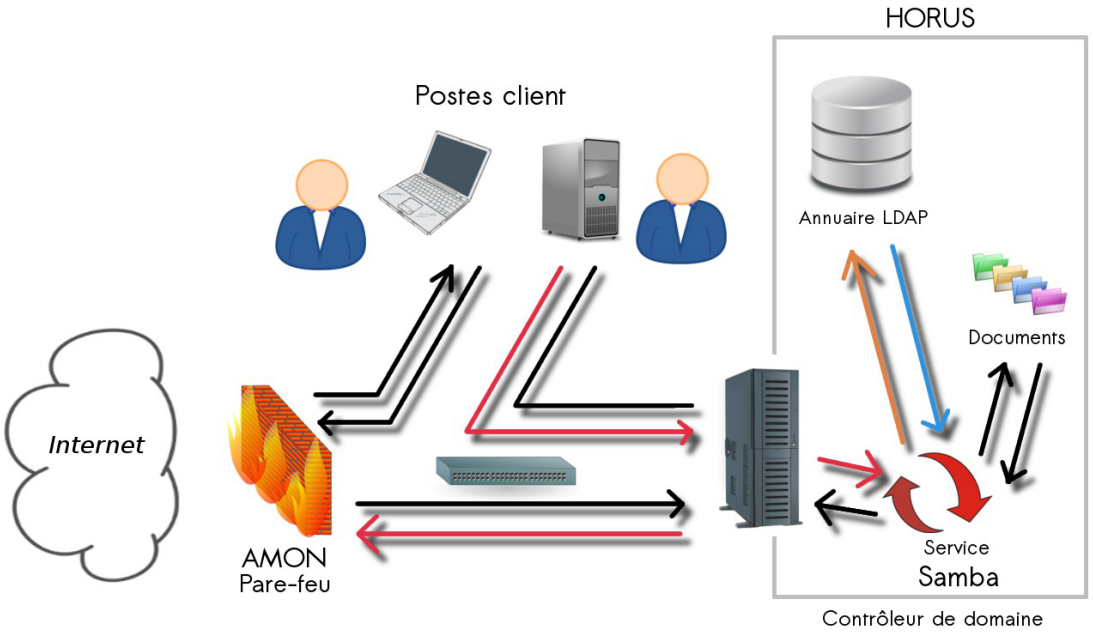
Il est également utilisable dans n'importe quelle autre structure nécessitant un contrôleur de domaine.

Un contrôleur de domaine est un serveur central qui est en charge des contrôles d'accès.

Un domaine est une entité logique qui reflète le plus souvent une organisation hiérarchique. Le domaine permet à l'administrateur système de gérer efficacement les utilisateurs des stations déployées car les informations (comptes et autorisations d'accès) sont centralisées dans une même base de données.

Le contrôleur de domaine permet donc :

- de gérer des comptes utilisateur : ajouter, supprimer et modifier un utilisateur ;
- de créer des groupes d'utilisateurs : créer des groupes pour simplifier la gestion des politiques (permission sur des dossiers, permission sur des services,...) ;
- de créer des politiques de sécurité qui seront appliquées aux utilisateurs et aux groupes d'utilisateurs.



L'utilisateur peut, sur une machine cliente raccordée au réseau, faire le choix de démarrer une session avec un compte du domaine ou avec un compte local s'il en existe. Il est ainsi possible d'ouvrir une session sur n'importe quel poste du domaine.

1. Qu'est ce que le module Horus ?

Le module Horus est un **serveur de fichiers administratif** qui, à l'origine, était destiné à remplacer, dans les établissements scolaires, les serveurs équipés du système d'exploitation réseau Novell,

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

système d'exploitation dont le support s'est arrêté en 2010.

Il peut également se substituer à un contrôleur de domaine NT[p.756], pour l'authentification des utilisateurs, l'exécution des scripts de connexion, la gestion des droits sur les partages.

Il est donc tout à fait possible de s'affranchir d'un serveur Microsoft et de le remplacer par le module Horus.

Les applications nationales ainsi que toutes les fonctionnalités de partage de fichiers et de gestion des utilisateurs de clients Windows sont intégrées sur le module Horus. Le module Horus est doté d'une base de données InterBase[p.765]. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP[p.758] pour l'attribution dynamique d'adresse IP.

Depuis plusieurs années, les applications nationales utilisées en Établissement Public Local d'Enseignement[p.760] (EPLE) sont qualifiées pour fonctionner sur le module Horus :

- GFC : Gestion Financière et Comptable ;
- PRESTO : PREstation et STOcks.



Les applications nationales sont décrites à l'adresse suivante :
http://www.esen.education.fr/fr/ressources-par-type/outils-pour-agir/le-film-annuel-des-person

Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL[p.752] ;
- quotas disque ;
- partage d'imprimantes ;
- gestion des comptes utilisateurs et des accès ;
- exécution d'applications utilisateur.

Annuaire :

- l'annuaire est initialisé à partir d'importation de comptes (AAF[p.752], CSV[p.758], ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- un service de messagerie instantanée (standard XMPP[p.784]) ;

Serveur web :

- une authentification centralisée ;
- des applications.

Gestion avancée des utilisateurs et des postes clients :

- appliquer des restrictions ou pré-configurer des applications, en fonction du login de l'utilisateur ou de ses groupes et du nom de la machine sur laquelle il se connecte ;
- surveiller la détection de virus par le serveur ;
- surveiller et éventuellement purger les files d'attente des imprimantes connectées au serveur (locales ou distantes).

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

2. À qui s'adresse ce module ?

Le module Horus s'adresse principalement aux réseaux administratifs d'un établissement scolaire.

Il peut toutefois être utilisé partout où il est nécessaire d'avoir un serveur de fichiers.

3. Les services Horus

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 Horus

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseau ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL[p.752] ;
- *CUPS* : serveur d'impression ;
- *InterBase* : système de gestion de base de données utilisé pour les anciennes applications nationales ;
- *MySQL* : système de gestion de base de données utilisé pour les nouvelles applications nationales ;
- *Bareos* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP.

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

4. Structure des conteneurs

Le module Horus s'installe par défaut en mode non conteneur[p.756].



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.

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 installés.

Exemple d'usage du module Horus dans un collège. Il y a environ 12 comptes utilisateurs, 12 postes clients et 8 connectés en moyenne. Cette machine est équipée d'un processeur Intel Xeon CPU 3.20GHz avec 8Go et 1To de disque dur.

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

6. Les différences entre les versions 2.5 et 2.6

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.767], 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.780] est, dorénavant, la seule méthode valide pour la gestion des services. upstart[p.782] est encore accepté pour assurer la rétrocompatibilité. Cependant, le service est, dans tous les cas, géré par systemd.

Interfaces réseau

Sur la nouvelle version d'EOLE les cartes réseau respectent la convention Consistent Network Device Naming[p.755] de udev[p.782] 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.782].

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 :

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

- 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.

PHP 7

La version de PHP disponible sur Ubuntu 16.04 est PHP 7.

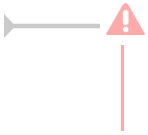
Outre les évolutions liées au langage lui-même, plusieurs modifications majeures sont à en prendre en compte :

- modification des noms de paquets : `php5-sqlite` => `php-sqlite3` ;
- modification des chemins de configuration : /etc/php5 => /etc/php/7.0 ;
- modification du nom de certaines commandes : php5enmod => phpenmod.

MySQL 5.7

La version de MySQL disponible sur Ubuntu 16.04 est MySQL 5.7.

Certains scripts existants pourraient ne plus être compatibles avec cette nouvelle version du logiciel.



Dans MySQL 5.7, le champ `password` de la table `mysql.user` a été renommé `authentication_string`.

Anti-virus

Certains répertoires sont affichés comme fichiers inconnus sous Windows lorsque Scannedonly est utilisé. Le logiciel Scannedonly[p.777] n'étant plus compatible avec la version de Samba, la fonctionnalité Anti-virus temps réel ClamAV sur les fichiers n'est plus disponible à partir de la version EOLE 2.6. L'observatoire des virus a été supprimée de l'EAD.

Une nouvelle variable permet de choisir la profondeur maximale pour le balayage des répertoires. Des valeurs de variables ont été augmentées.

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

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

l'espace libre à une partition au travers de l'interface de configuration du module pour ajuster le partitionnement avant l'instance.

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.776] de liens Ethernet.

Gestion des certificats Let's Encrypt

L'autorité de certification Let's Encrypt[p.767] 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.

Nom de domaine des applications web

Les adresses IP ne sont plus autorisées pour la variable `Nom de domaine des application`s

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

`web`.

Cette restriction est notamment due au durcissement du support du protocole HTTPS[p.764] par les navigateurs.

EoleSSO cluster

EoleSSO peut être paramétré pour stocker les sessions SSO dans une base de données Redis[p.776] (locale ou distante).

En branchant plusieurs services EoleSSO sur la même base, il est possible de mettre en place une configuration de type cluster en répartition de charge ou en basculement.

Adresses autorisées à accéder à MySQL

Des variables ont été ajoutées dans l'onglet expert `Mysql` afin de déclarer les adresses IP ou les réseaux autorisés à accéder au serveur MySQL local.

2.6.2

Accès au backend EAD

À partir de la version EOLE 2.6.2, pour permettre à un frontend EAD[p.759] 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.779].

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`.

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

DHCP

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

La prise en charge de l'API OMAPI[p.772] permet de changer la configuration DHCP à chaud.

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

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.



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)

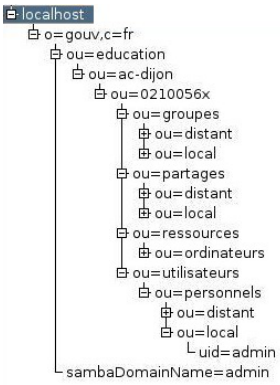
Chapitre 3
Fonctionnement du module Horus

Pour jouer son rôle, le module Horus repose sur beaucoup de projets libres : OpenLDAP, Samba, ProFTPD, CUPS, ESU, Bareos, Apache, MySQL, phpMyAdmin.

Tous les services sont activables, désactivables, pour construire un serveur administratif sur mesure.

Un nombre conséquent de services s'appuient sur l'annuaire OpenLDAP du module :

- authentification des utilisateurs ;
- définition des partages Samba ;
- définition des groupes
  - utilisateur dédié à toutes les tâches d'administration ;
  - groupes dédiés à l'environnement Windows ;
  - groupes propres au module Horus.
- définition des utilisateurs.



Une importation massive de comptes peut être réalisée depuis les formats AAF et Texte.

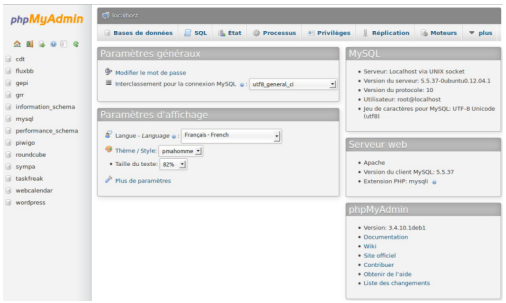
L'annuaire OpenLDAP associé au logiciel Samba permet la mise en place d'un contrôleur de domaine qui offre les fonctionnalités suivantes :

- authentification centralisée des postes clients ;
- partage de fichiers et de répertoires ;
- support des ACLs ;
- quotas disques par utilisateur ;
- analyse anti-virus en temps réel.

Le service web basé sur les logiciels libres Apache, MySQL et phpMyAdmin permet d'accueillir le logiciel métier GFC ainsi que d'autres applications web pré-packagées : Pydio, Rouncube, Dokuwiki, Jappix ou encore Piwigo.

L'authentification unique est assurée par le service EoleSSO.

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

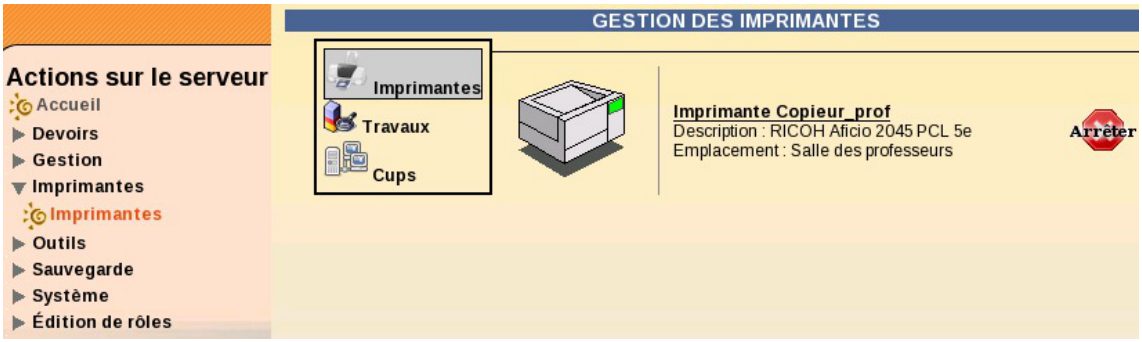


Édition de tables avec phpMyAdmin

Le système de gestion de base de données propriétaire InterBase permet, quant à lui, d'accueillir l'application métier PRESTO.

Le serveur d'impression permet :

- le partage automatique des imprimantes installées sur le serveur ;
- le stockage centralisé des pilotes d'imprimantes ;
- l'utilisation de l'interface simplifiée de gestion des imprimantes (EAD) ;
- l'utilisation de l'interface de gestion CUPS.



Interface simplifiée de gestion des imprimantes (EAD)

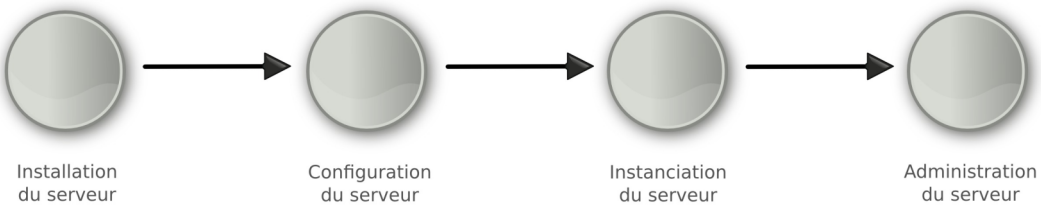
La gestion des clients se fait au travers de plusieurs applications :

- ESU pour l'édition des règles :
  - paramétrage de l'environnement des utilisateurs ;
  - paramétrage d'applications (Firefox, Thunderbird) ;
  - en fonction du nom du poste, du nom de l'utilisateur ou du système d'exploitation.
- Client EOLE pour l'application des règles :
  - à chaque ouverture de session ;
  - pendant la session (exemple : mode devoir).
- EAD :
  - surveillance des quotas ;
  - historique des connexions ;
  - liste des virus détectés ;
  - extinction / redémarrage à distance des postes clients ;
  - déconnexion forcée des utilisateurs.

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.765] 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.779], e2guardian[p.759], 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)

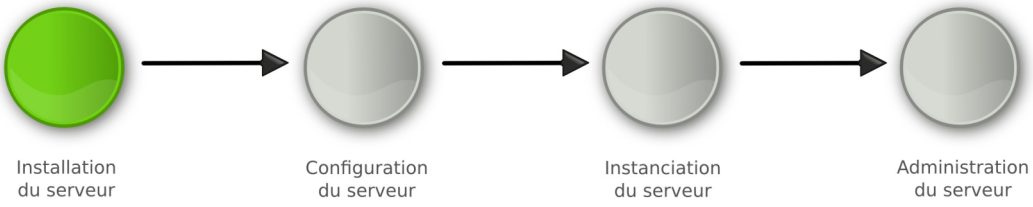
Chaque module possède des fonctionnalités propres, souvent complémentaires.
Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

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.765] 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.782].

Architecture

Depuis la version EOLE 2.6 seule l'architecture 64 bits (AMD64[p.753]) 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.764] :

- 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.769] 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.



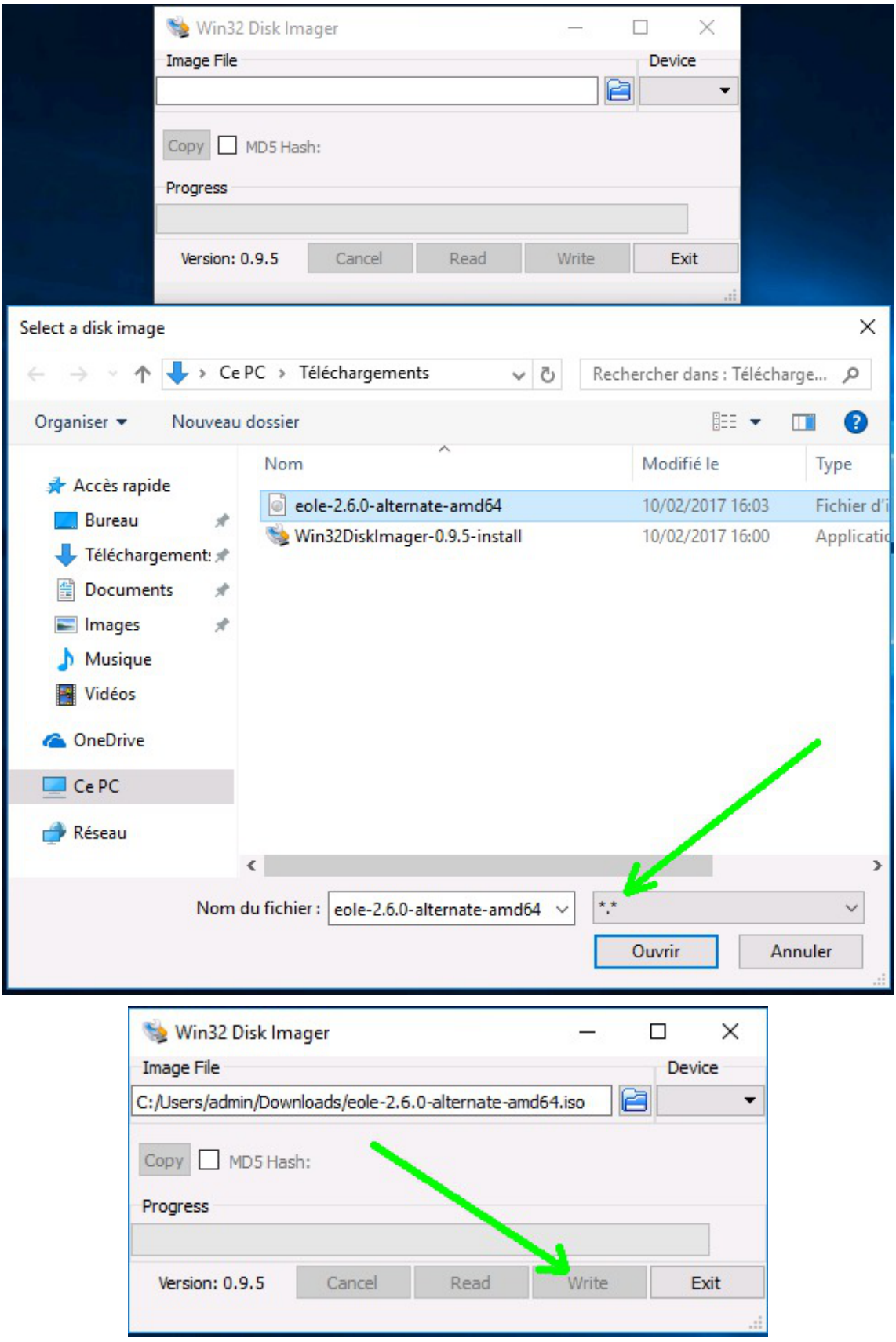
La commande `dd` écrase intégralement le contenu de la clé.

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.775] 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.768] 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 :

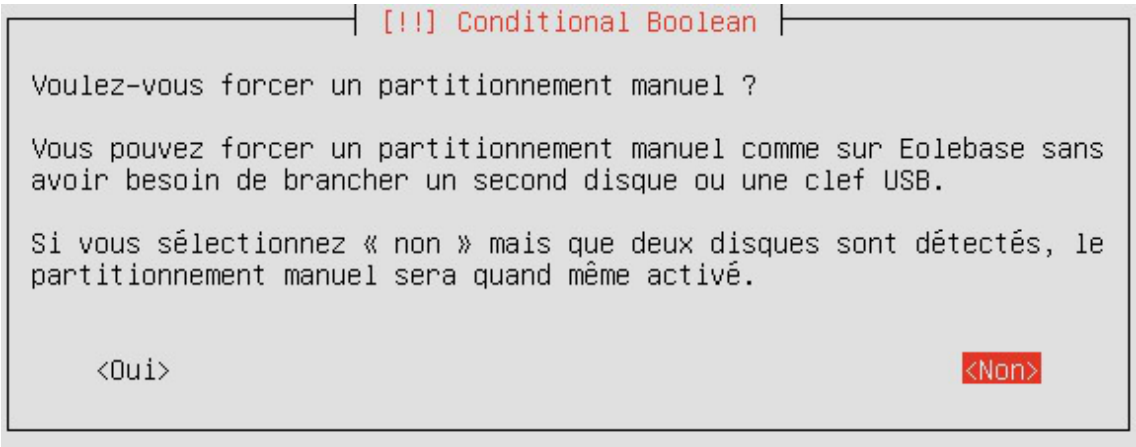
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.768] 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.753]) ;
10. choisir et installer des logiciels ;
11. installation du programme de démarrage GNU GRUB[p.763] ;
12. fin de l'installation.

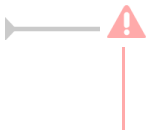
À la fin de l'installation l'écran suivant est affiché.



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.

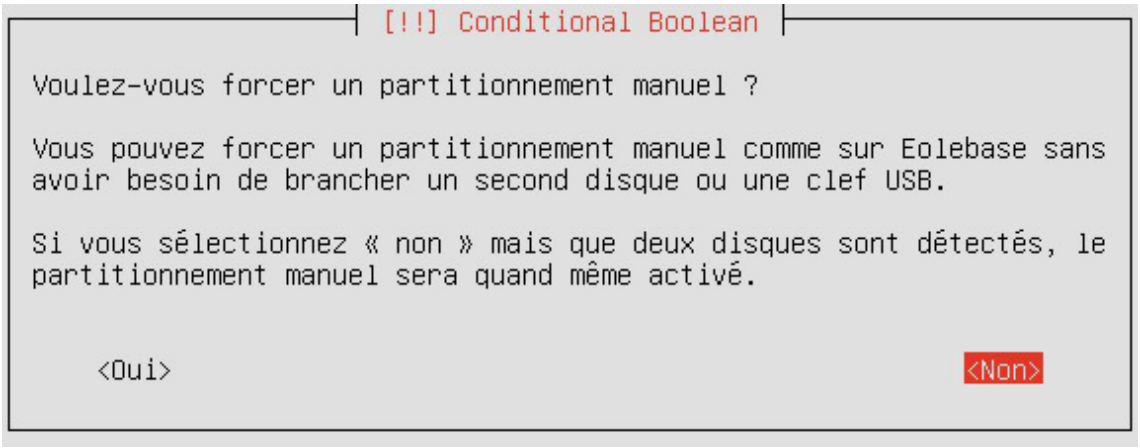
Voir aussi...

Les mots de passe [p.344]

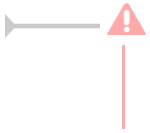
4. Partitionnement personnalisé

Le partitionnement utilise le logiciel LVM[p.768].

- 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

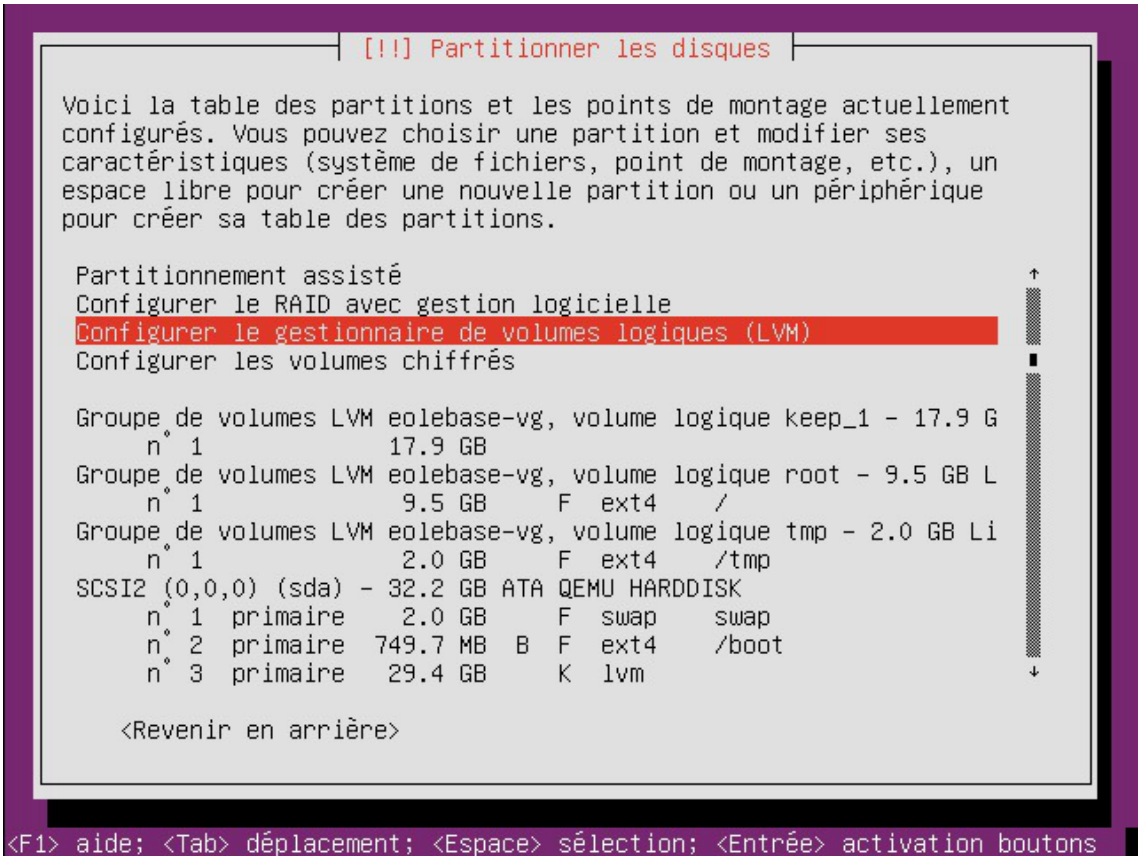
Lorsque le partitionnement manuel est déclenché une fenêtre propose de choisir le disque qu'il faut partitionner pour accueillir le système d'exploitation.



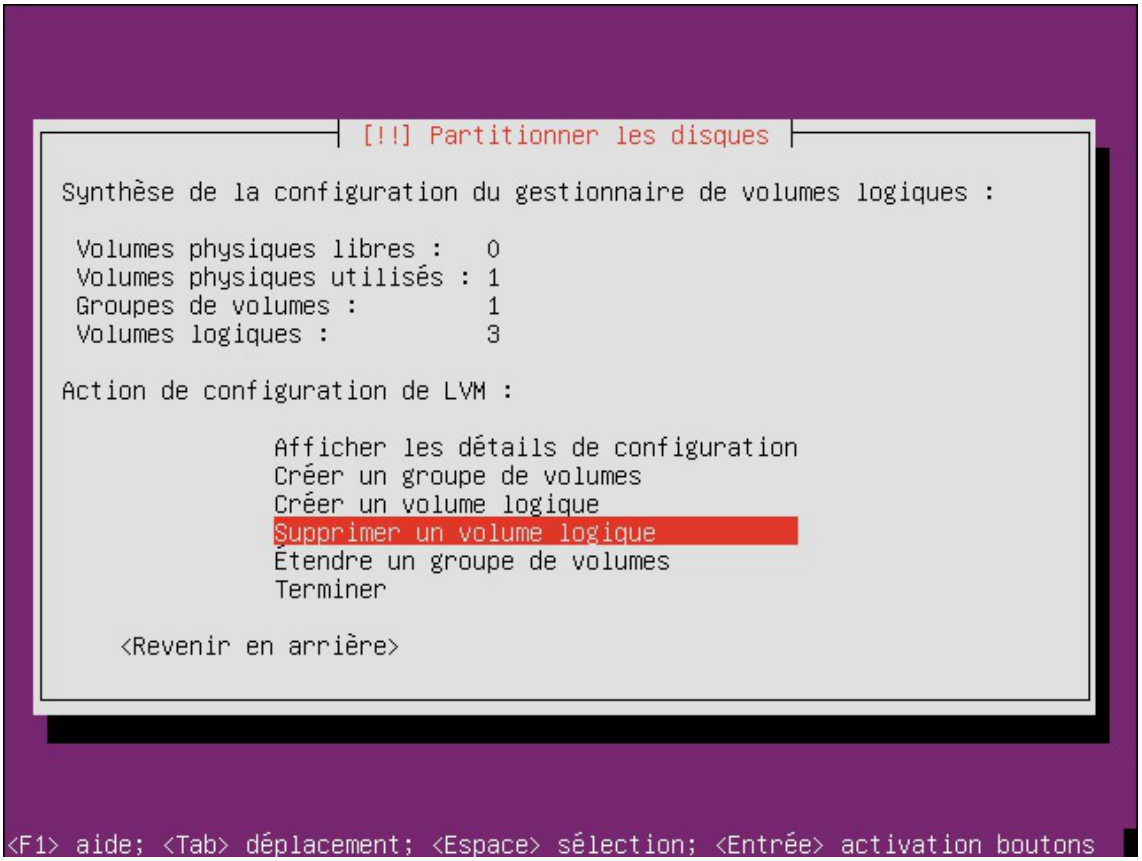
Un volume logique nommé `keep x` sans point de montage et sans système de fichiers contient l'espace qui n'a pas été attribué lors du calcul des autres volumes.
Sur un Eolebase il n'y a pas de volume proposé pour le point de montage `/home`.

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

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

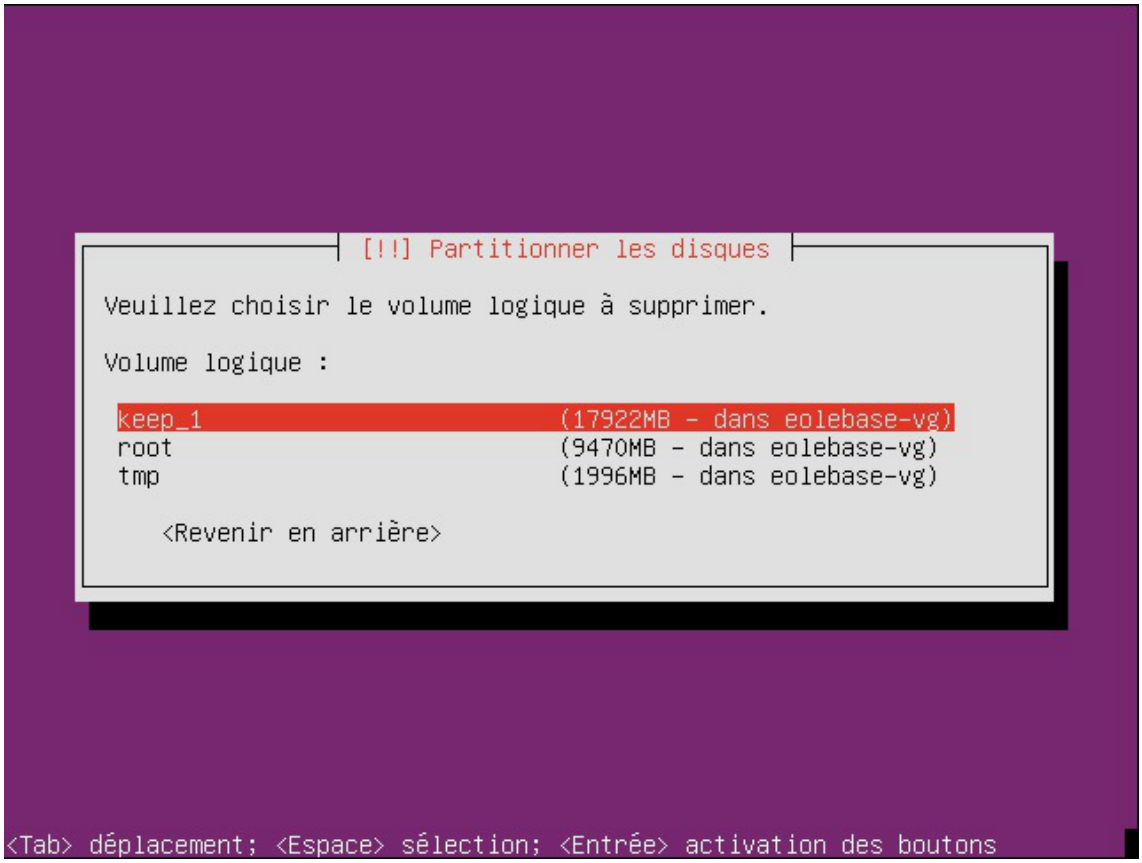


- Sélectionner `Supprimer un volume logique`

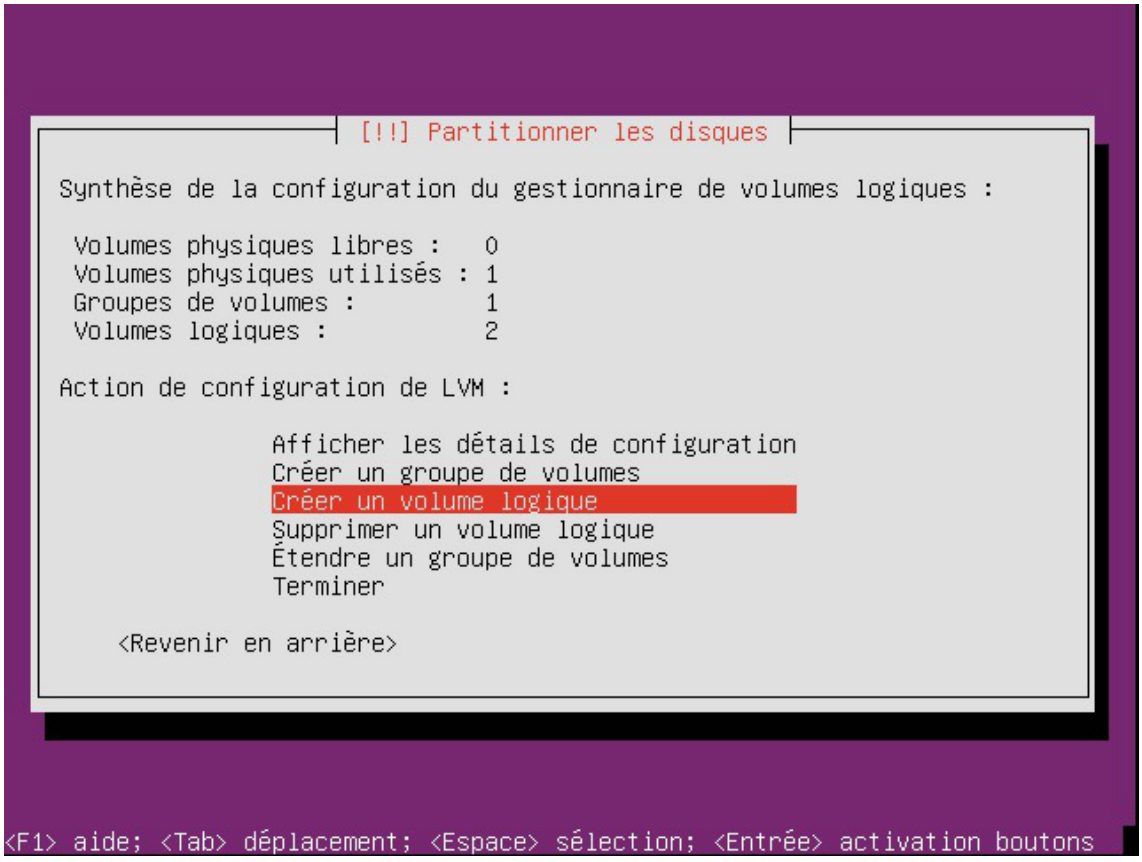


- Sélectionner le volume logique `keep_x`

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

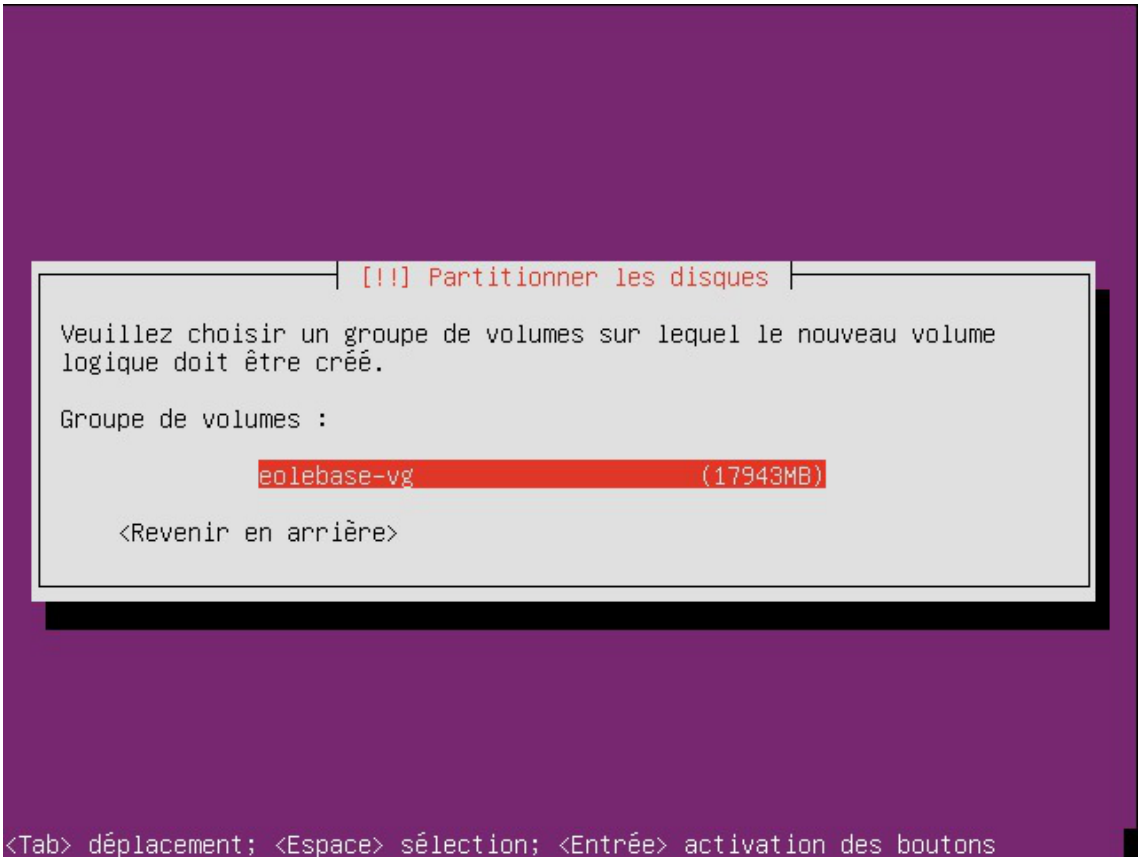


- De retour sur la gestion des volumes logiques, sélectionner `Créer un volume logique`

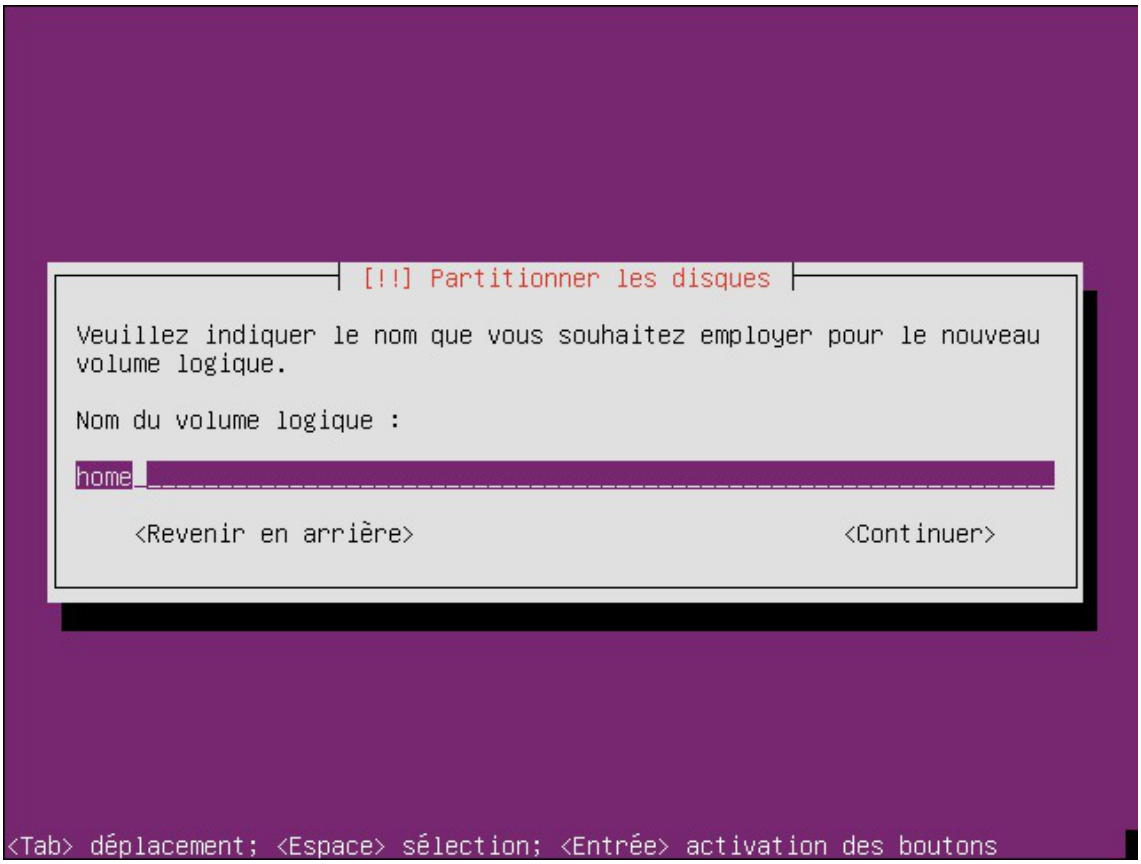


- Valider l'unique `Groupe de volumes` proposé

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

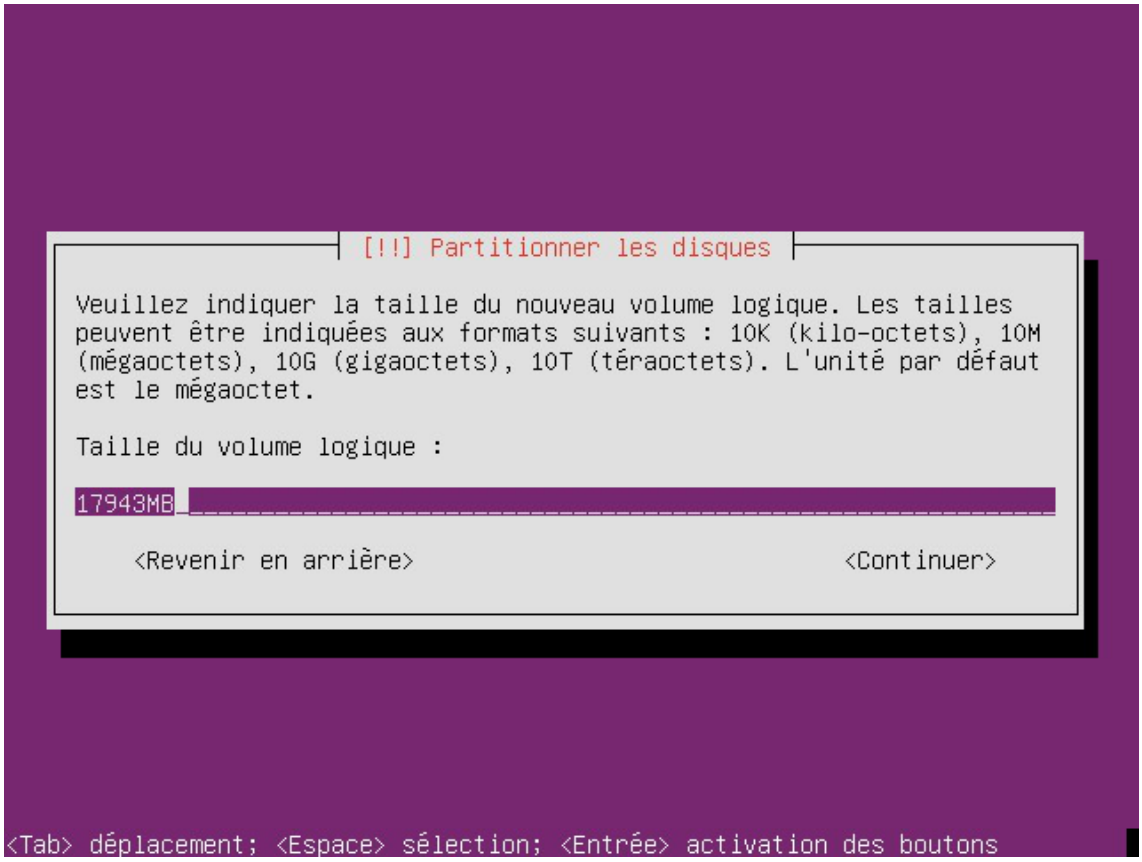


- Choisir le nom du nouveau volume logique

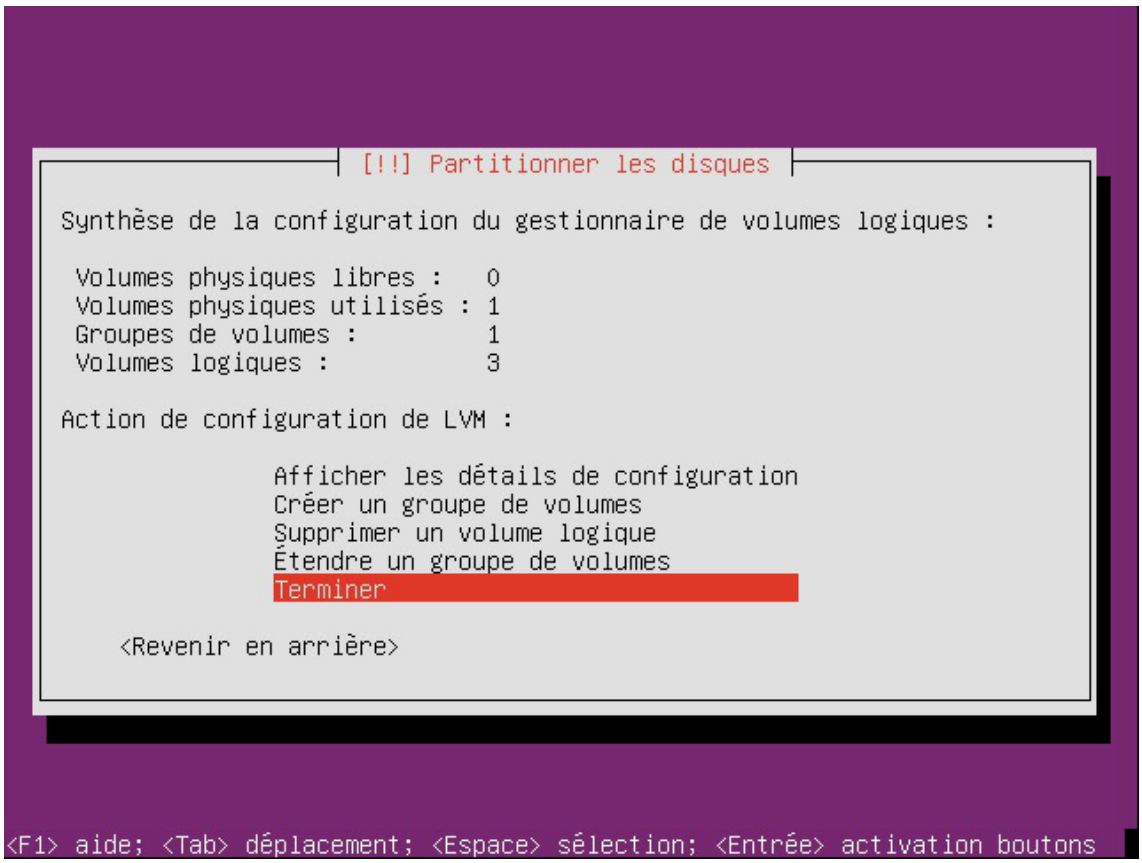


- Puis choisir l'espace à octroyer au nouveau volume, par défaut la taille affichée est la taille maximale

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

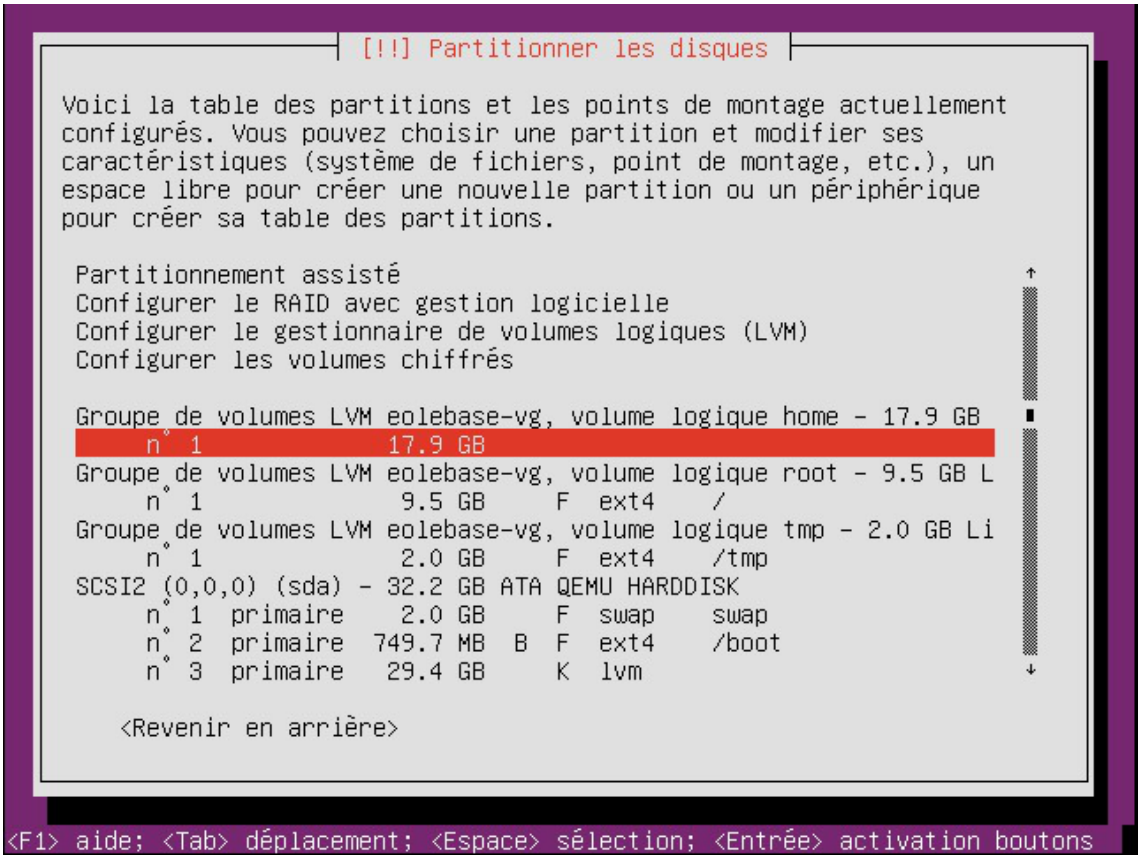


- De retour sur la synthèse de la configuration, sélectionner `Terminer`

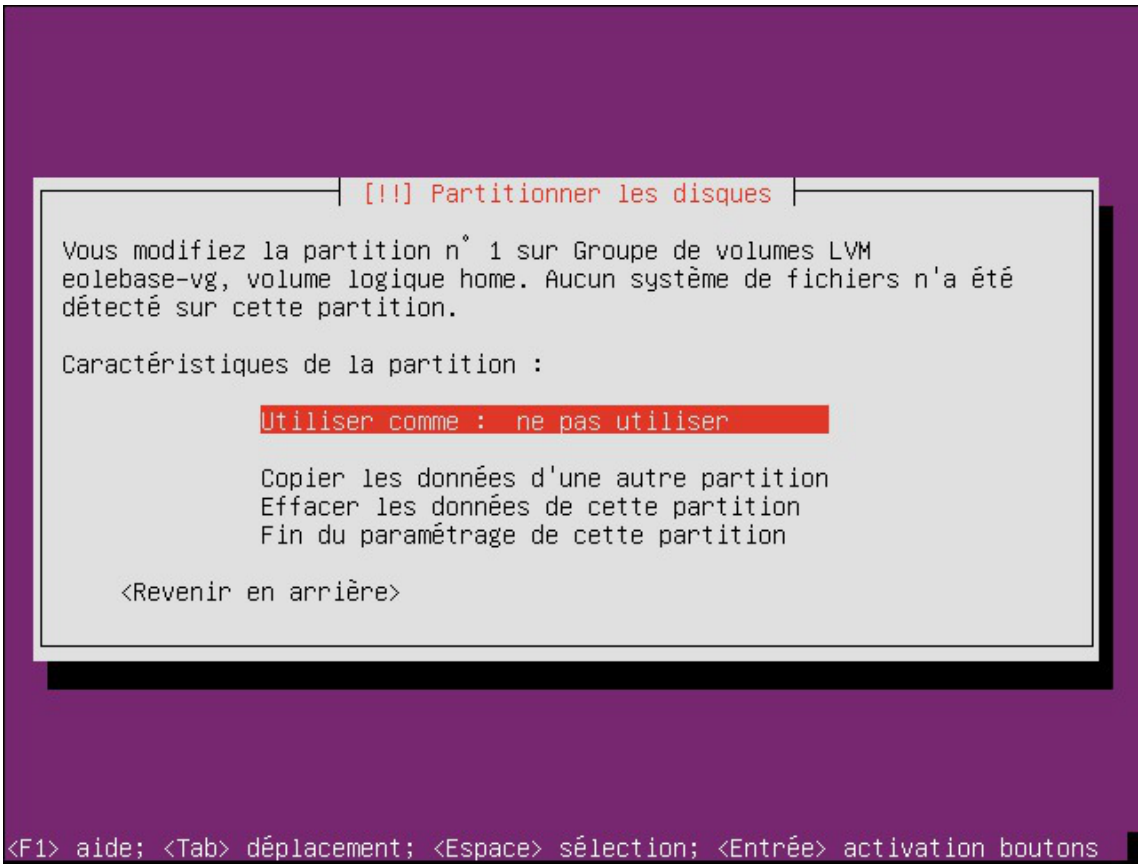


- L'outil de partitionnement affiche maintenant le volume `home`, sélectionner le pour édition

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

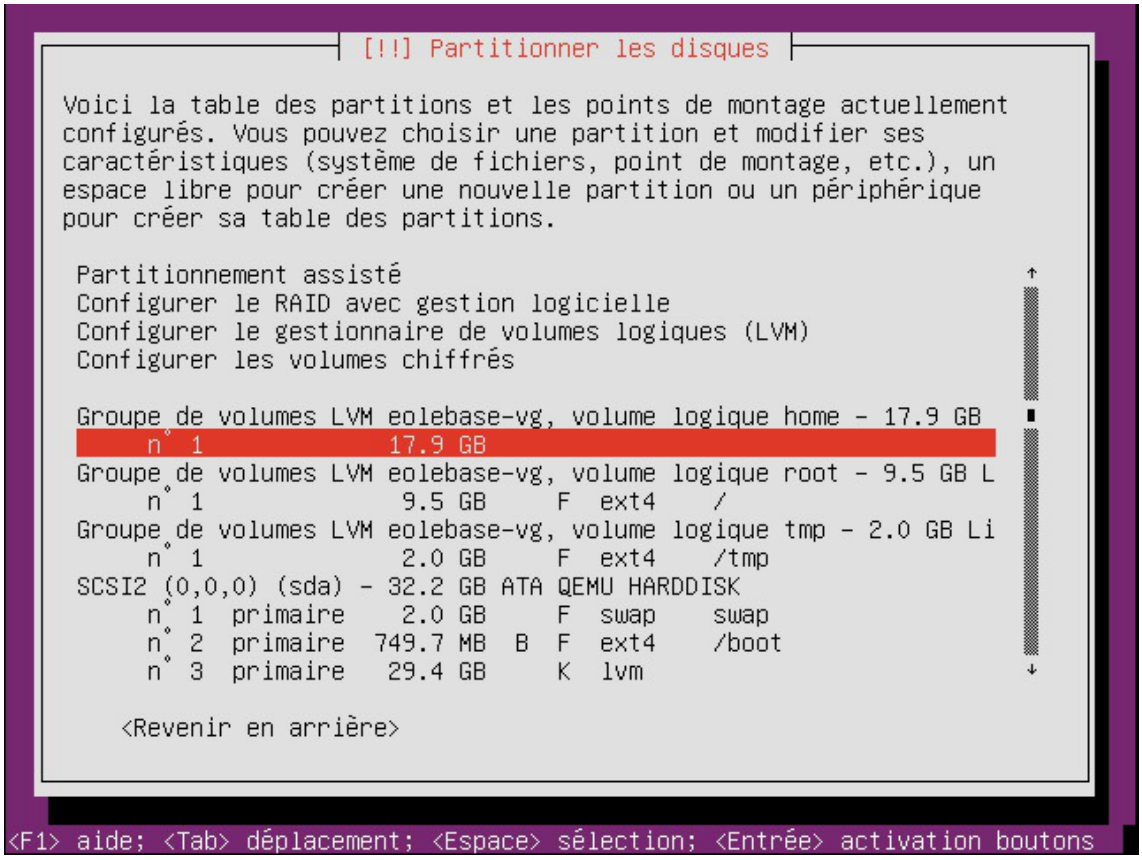


- Sélectionner `Utiliser comme : ne pas utiliser` pour choisir les caractéristiques du volume

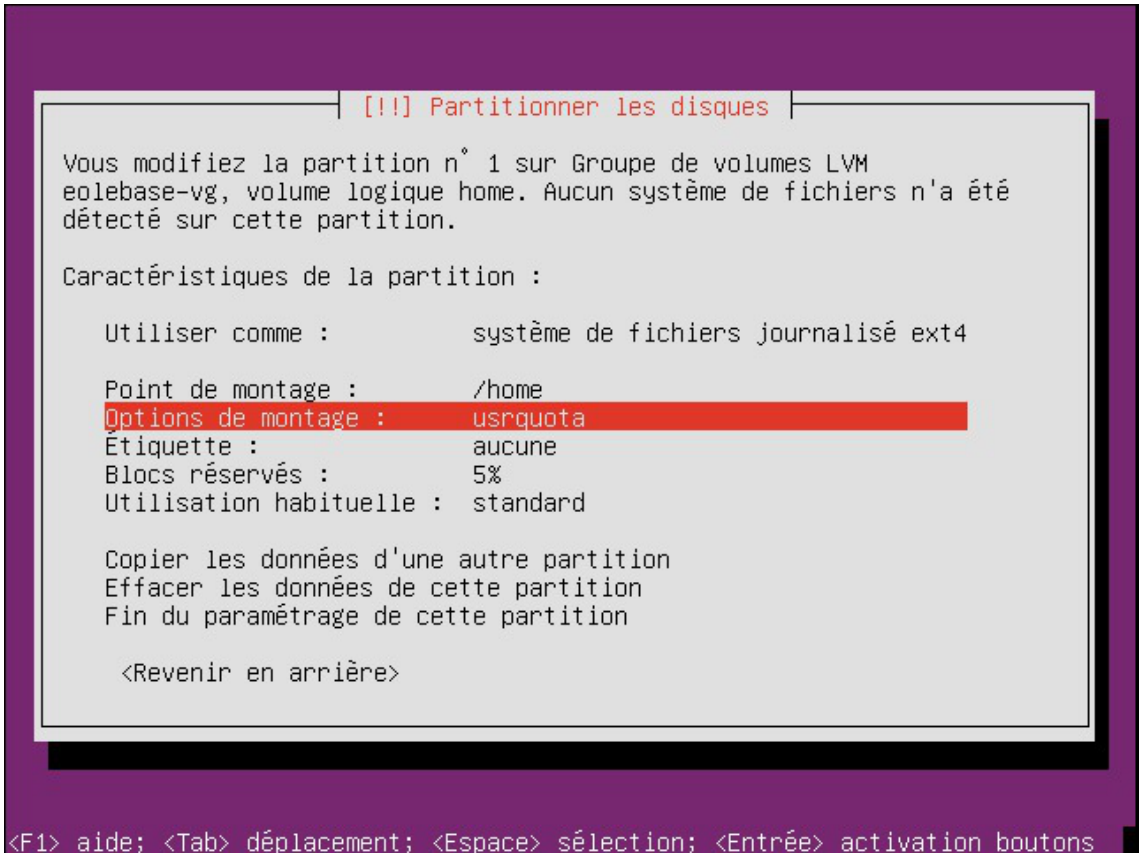


- Sélectionner le type système de fichier

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

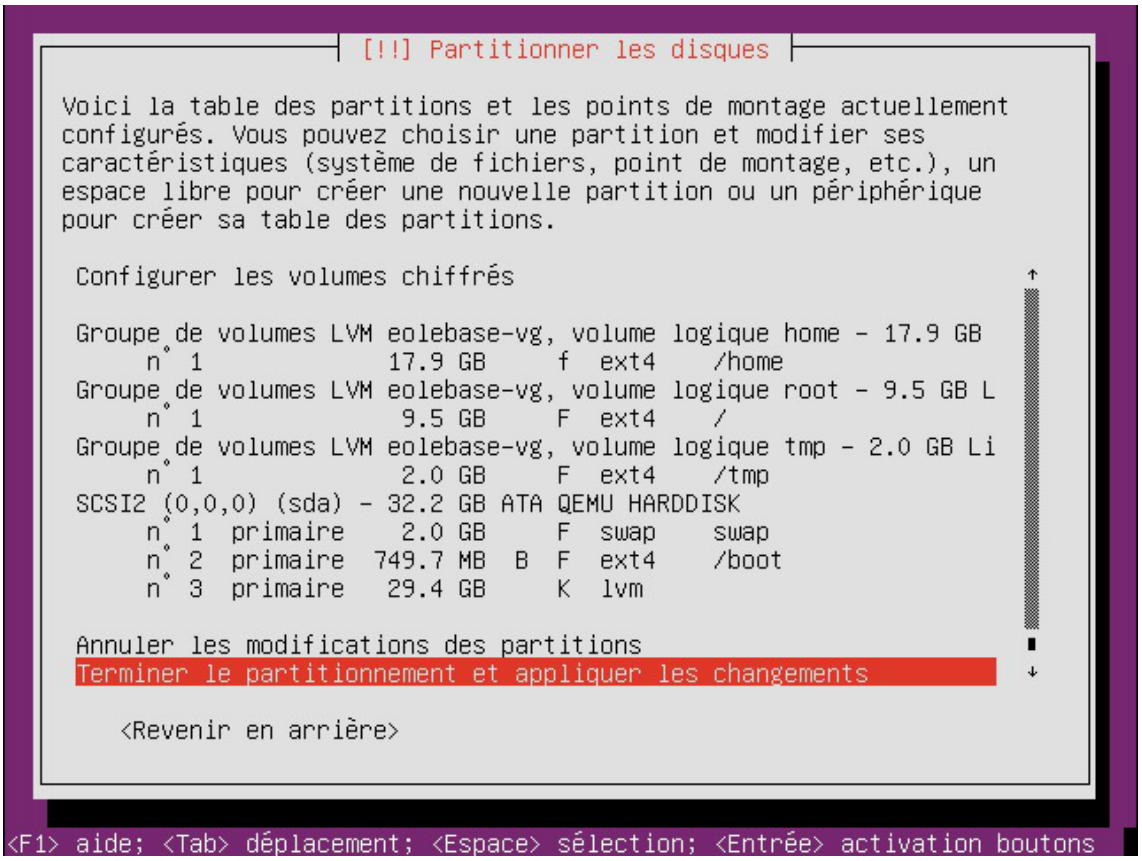


- Puis définir le point de montage et les options de montage

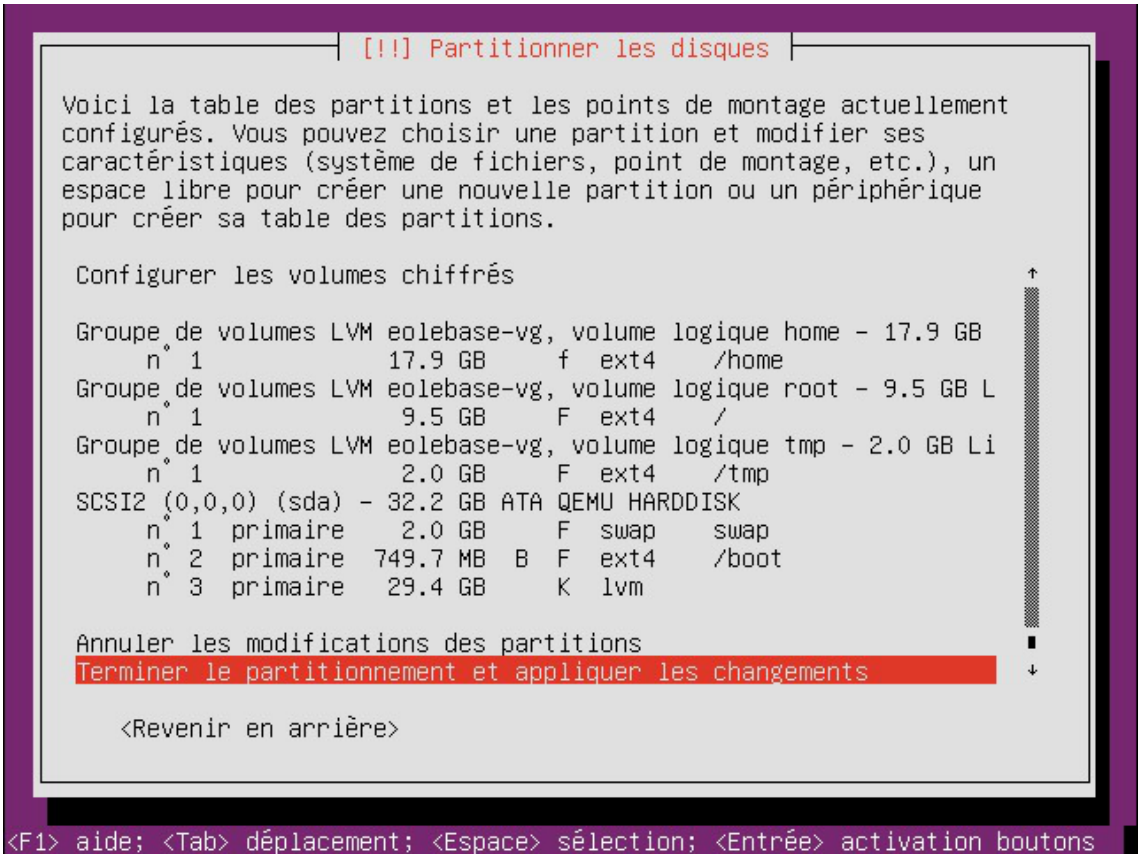


- Sélectionner la `Fin du paramétrage de cette partition`, de retour sur la fenêtre principale du partitionnement

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

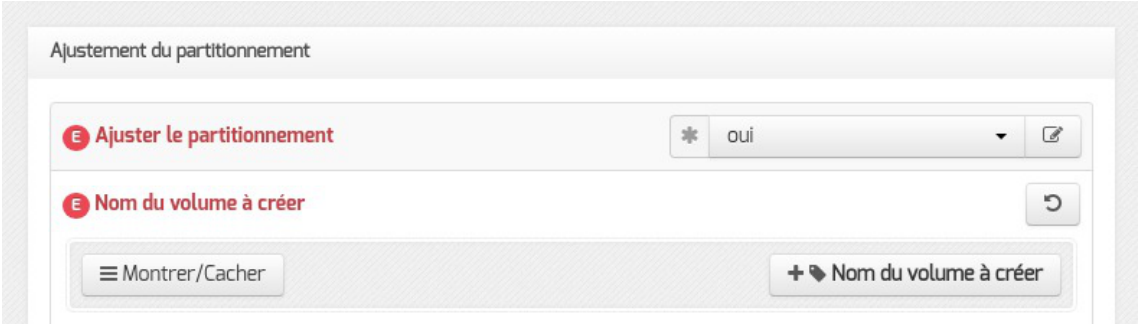
[...]
```

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`.

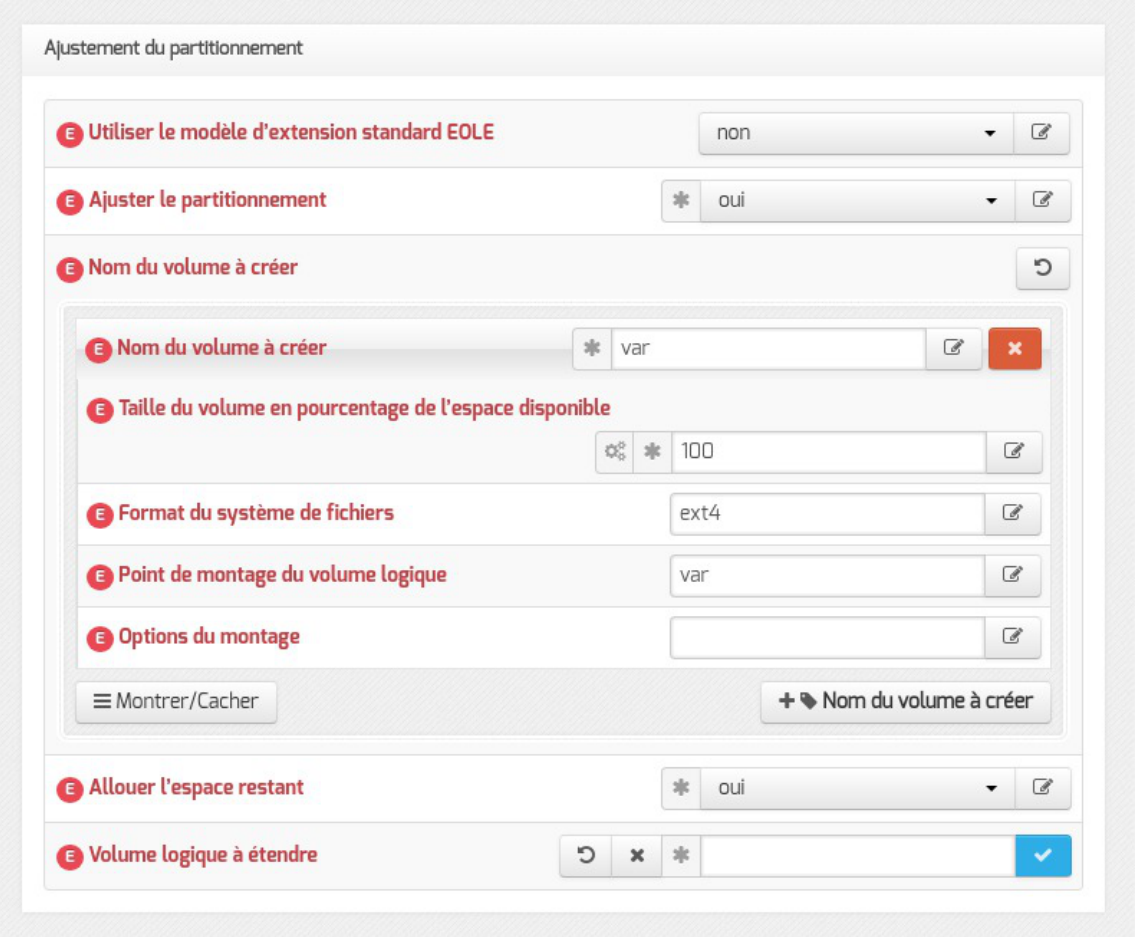
Ajuster le partitionnement sur une version d'EOLE supérieure ou égale à 2.6.2

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).

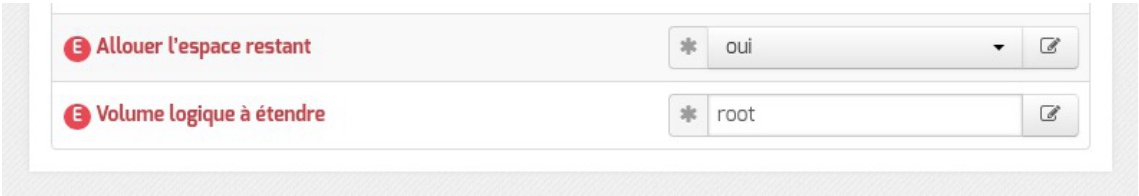
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



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.756].

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.

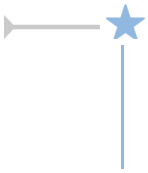
Modules en mode non conteneur

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

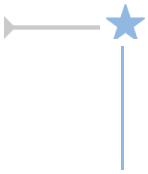
Après l'installation du module, la mise à jour n'est pas obligatoire mais fortement recommandée. Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto`.

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.

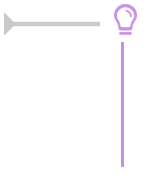
À partir d'un module



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`.

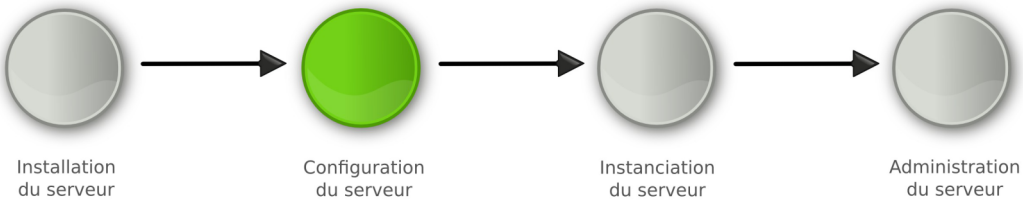
Voir aussi...

Les mises à jour [p.428]

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

Chapitre 6

Configuration du module Horus



Configuration

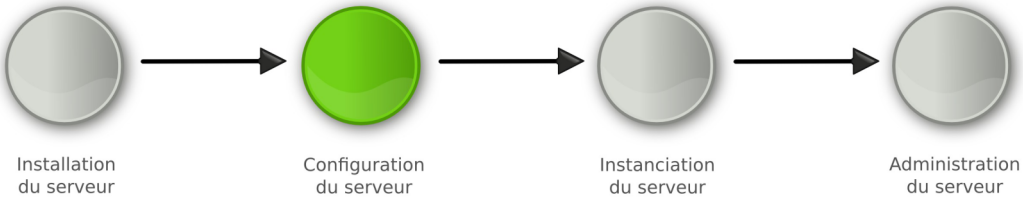
- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config` .

  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.779], e2guardian[p.759], 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.759], l'adresse du serveur de temps NTP[p.771], ...). Cette étape nécessite une bonne connaissance de l'architecture réseau dans laquelle sera installé le serveur.

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

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

l'effectuer en plusieurs temps.

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

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

Il existe deux modes de configuration :

- **mode autonome**

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

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

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

- **mode Zéphir**

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

1.1. Configuration en mode autonome

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

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

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

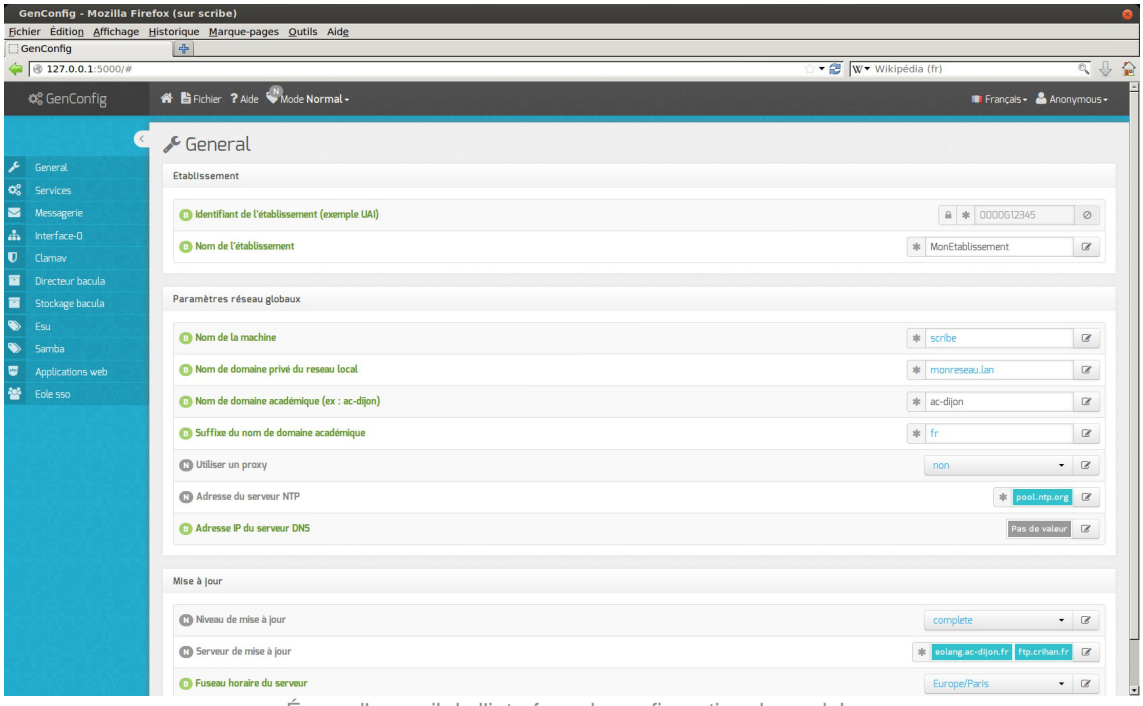
Il est donc possible d'utiliser le fichier `config.eol` d'un serveur en production pour en *instancier* un nouveau.



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

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

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



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

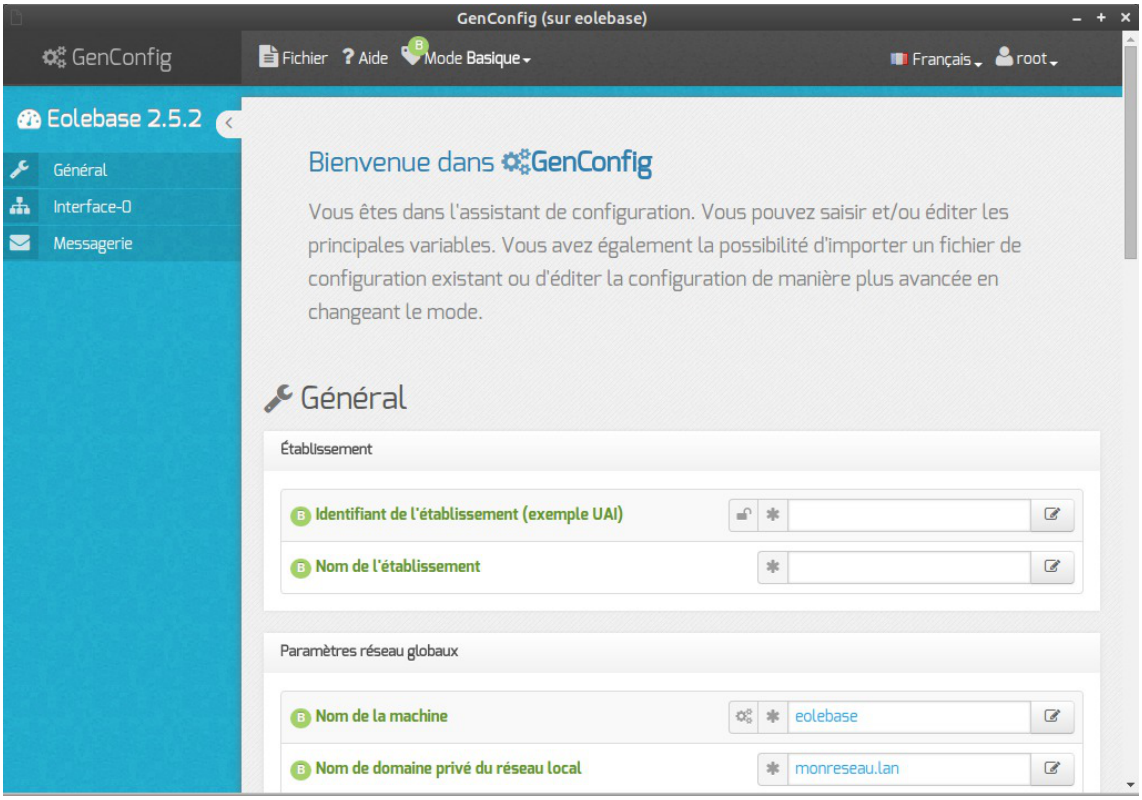
Une fois la commande `gen_config` lancée, comme indiqué dans la mire, vous devez ouvrir une session avec l'utilisateur **root** et le **mot de passe aléatoire** généré à l'installation.



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

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

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



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

L'interface se découpe en quatre zones :

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

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

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

1.1.1. Accès distant

Accès distant via le port 7000

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

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

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

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

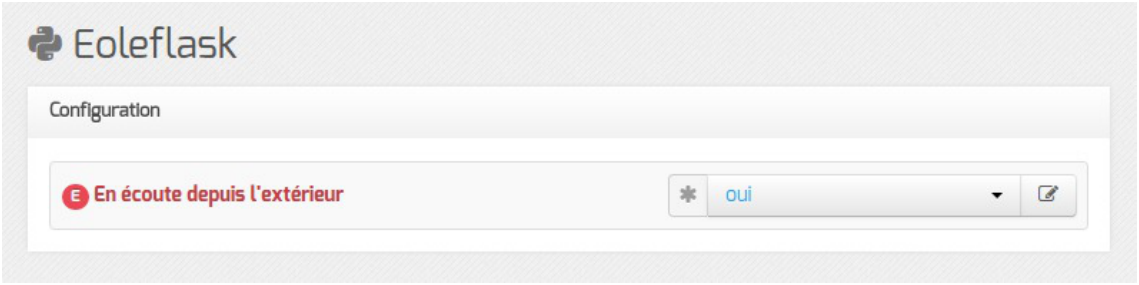
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

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

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



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

Accès distant via le port 443

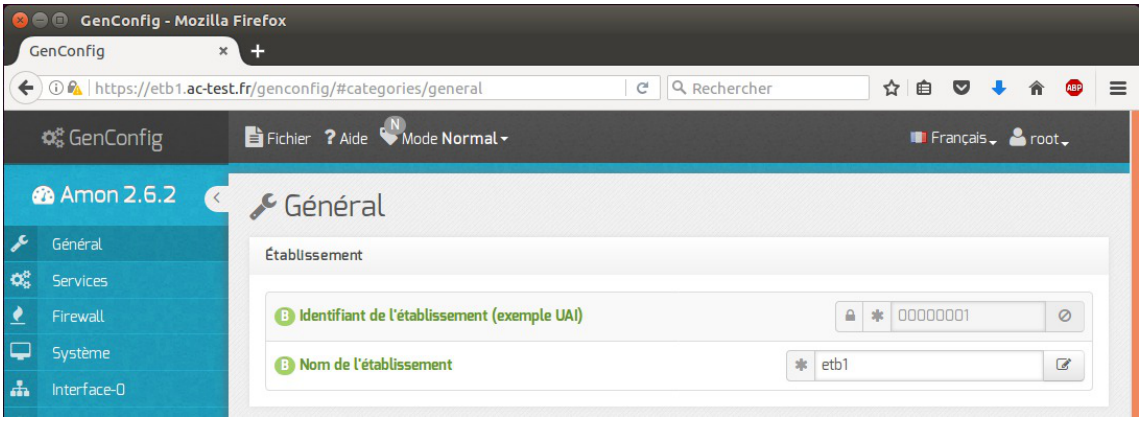
À partir d'EOLE 2.6.1, l'interface est également disponible sur le port 443 si la variable experte `Activer l'interface de configuration du module (GenConfig)` est à `oui` dans l'onglet `Services`. C'est le cas par défaut à partir d'EOLE 2.6.2.

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

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

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

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



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

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

1.1.2. La zone Menu

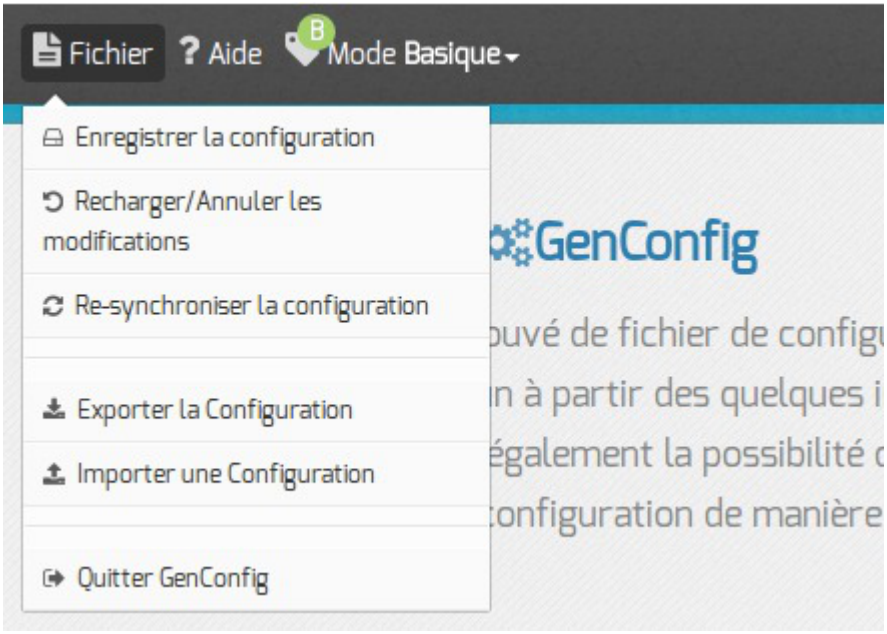
La zone de Menu, en haut de l'interface, propose les items suivants :

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

Sous-menu Fichier

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

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



Sous menu Fichier

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

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

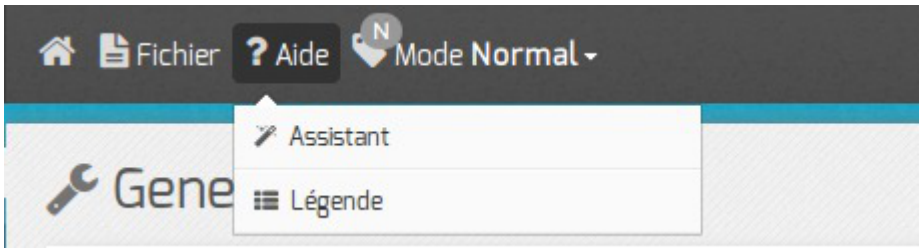
Re-synchroniser la configuration permet de récupérer les informations stockées en session sur le serveur si une coupure arrivait pendant la configuration.

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

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

Sous-menu Aide

- Assistant
- Légende



Sous menu Aide

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

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

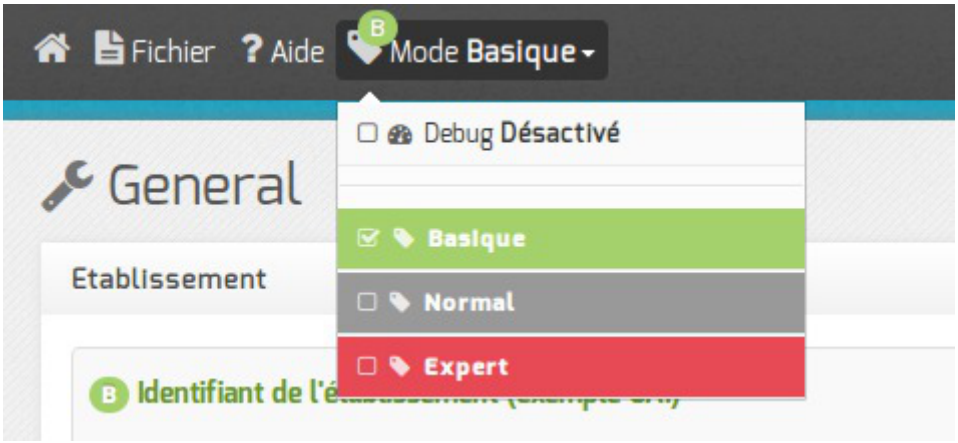
La légende présente un récapitulatif des différentes icônes que l'on peut rencontrer dans l'interface.

Sous-menu Mode

- Debug
- Basique

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

- Normal
- Expert



Sous menu Mode

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

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

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

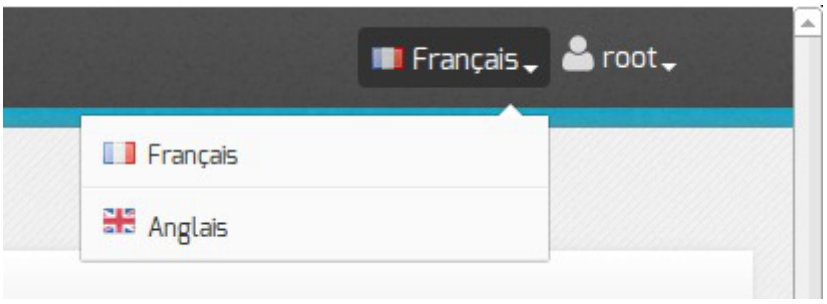
Le mode *Expert* active les onglets et les variables pour une configuration avancée.

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

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

Sous-menu Langue

- Français
- Anglais

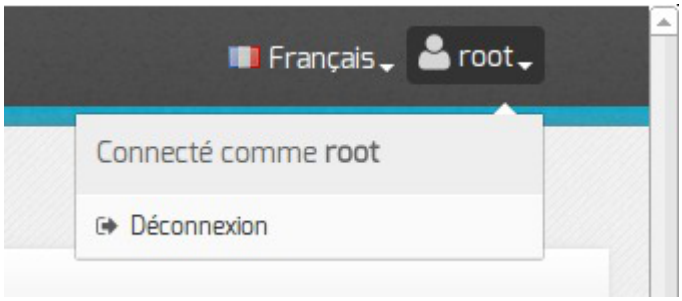


Langue permet de choisir la langue utilisé dans l'interface.

Sous-menu Session

- Connecté comme
- Déconnexion

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



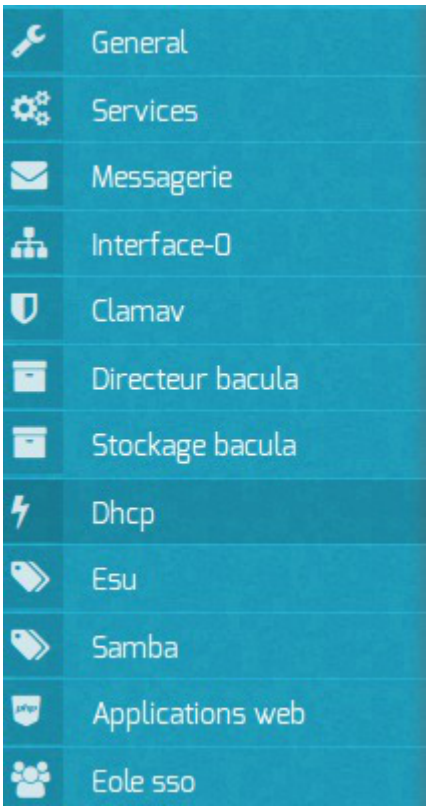
Session permet de connaître l'utilisateur courant et de se déconnecter.

1.1.3. La zone Onglet

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

- **les onglets de base** sont systématiquement présents au lancement de l'outil `gen_config` ;
- **les onglets optionnels** s'affichent si un paramètre du formulaire est activé.
  Exemple : si dans l'onglet `Services` le paramètre `Activer DHCP` est passé à `oui`, l'onglet `Dhcp` s'affiche dynamiquement au même niveau que les onglets de base ;
- **les onglets experts** correspondent essentiellement au paramétrage de fichiers de configuration d'outils spécifiques.
  Ils sont disponibles si le mode *Expert* est activé.

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



L'onglet courant

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

1.1.4. La zone Formulaire

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

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

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



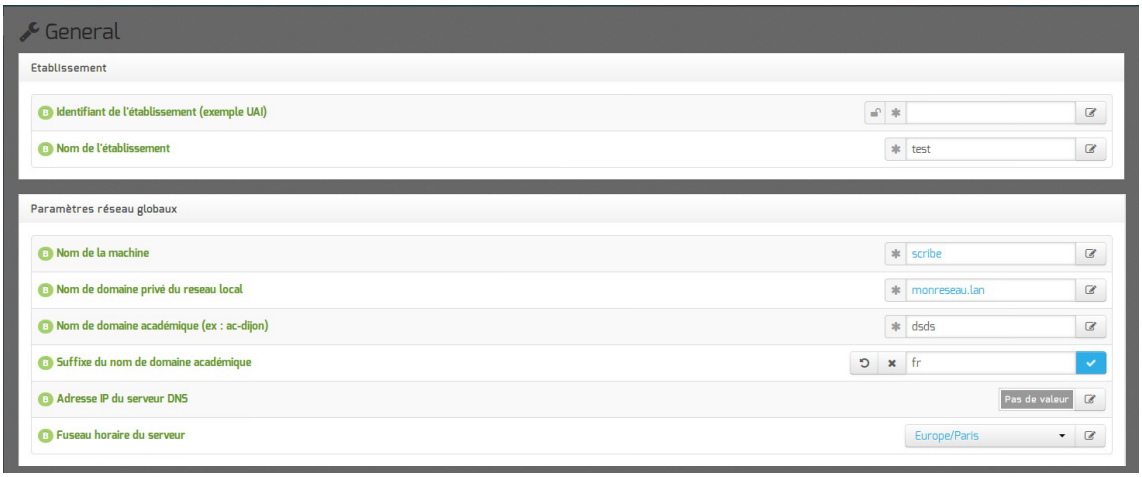
Bouton modifier sur la première ligne à droite, la deuxième ligne a le focus

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

Regroupement des paramètres par bloc

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

Chaque bloc regroupe un ou plusieurs paramètres.

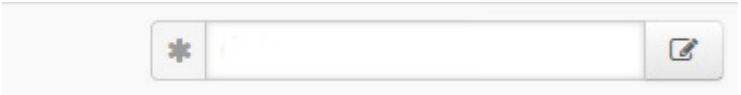


Les blocs thématiques

Les variables obligatoires

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

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



Les variables obligatoires sont précédées d'une étoile

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

Les variables des modes basiques, normales et expertes

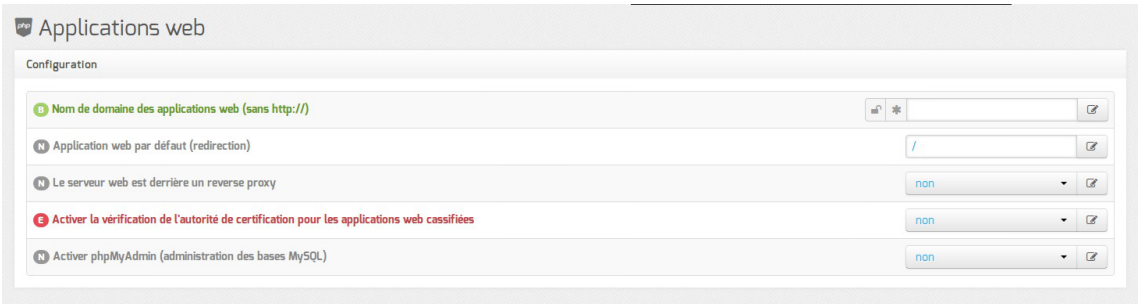
Le mode détermine l'affiche de variable plus ou moins complexes : basiques, normales ou expertes.

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

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

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

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

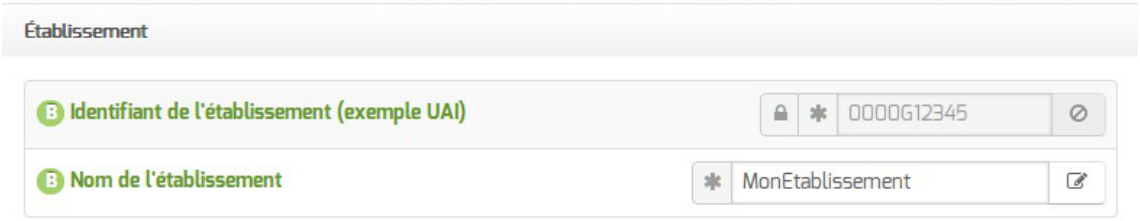


Les variables et leur niveau de complexité

Les variables simples

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

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



Les variables multiples

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

Les variables multiples se présentent sur fond coloré :

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

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



Apparence graphique des variables multiples

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

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



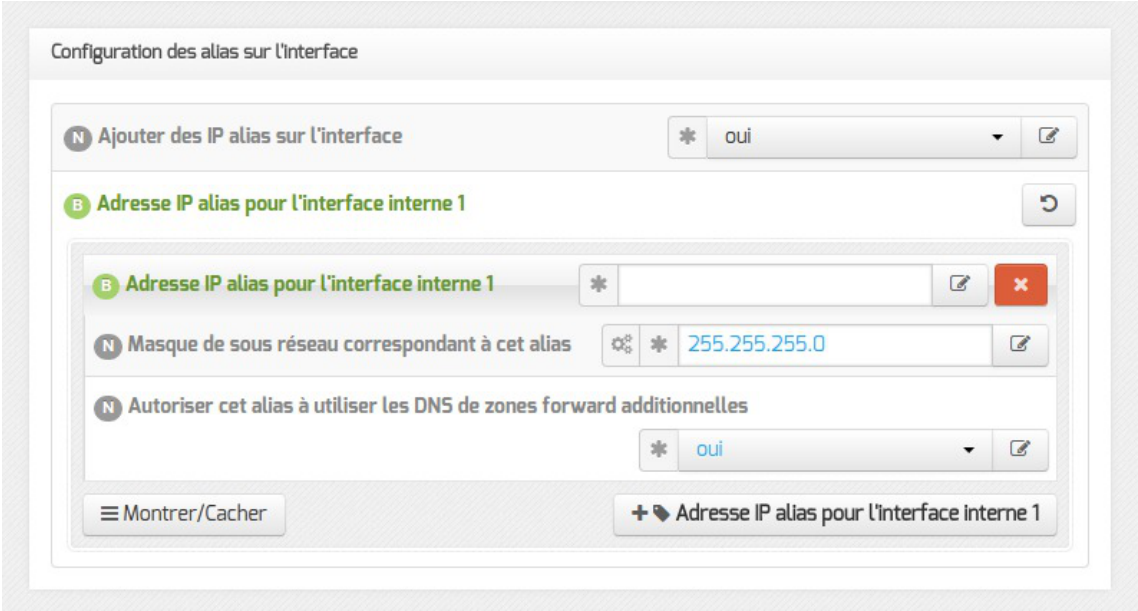
Édition d'une variable multiple

Les variables multiples groupées

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

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

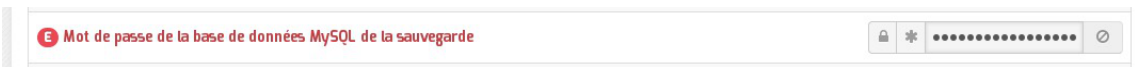
- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée.



Les variables brouillées

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

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



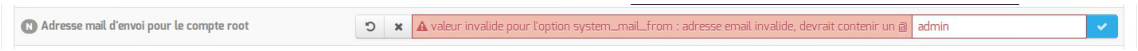
Validation des variables

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

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

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

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



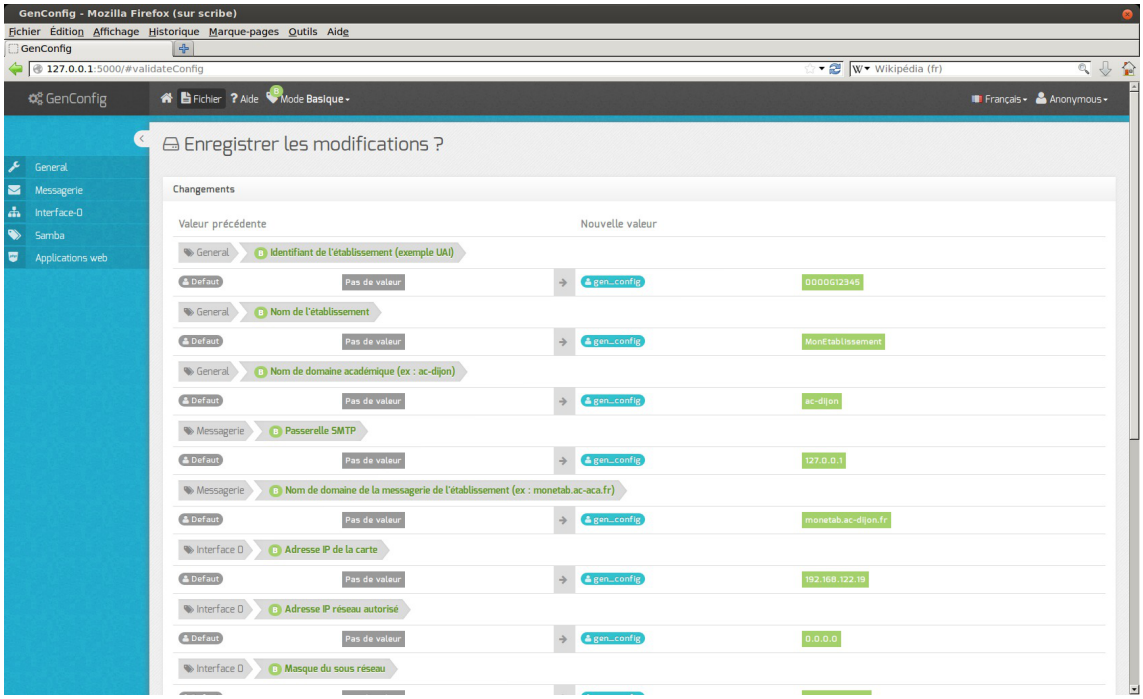
Validation d'une variable

1.1.5. La zone Validation

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

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

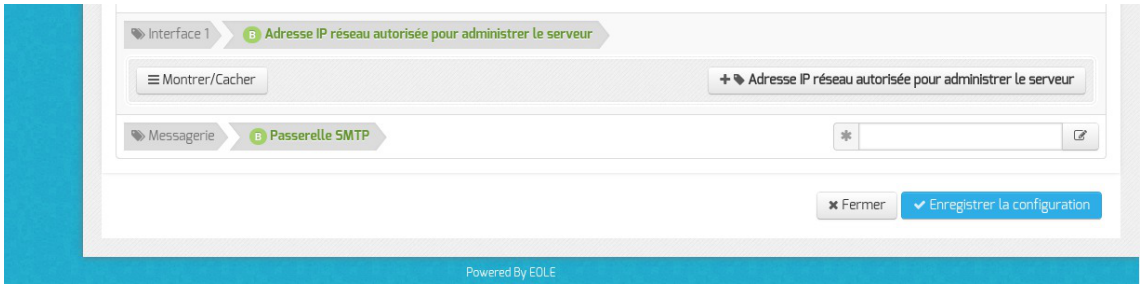
Lors d'une réédition de la configuration cette zone ne montre que les changements qui ont eu lieu.



Zone de validation

1.1.6. Enregistrer la configuration

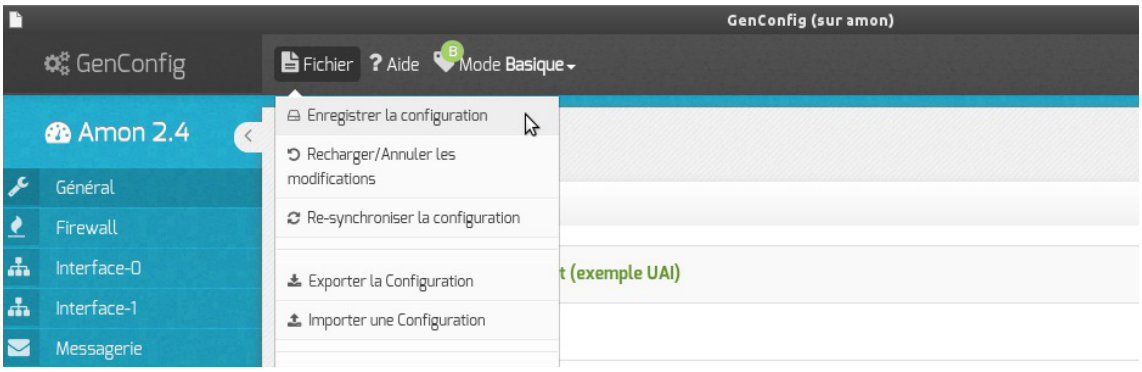
L'utilisation du mode assistant propose l'enregistrement de la configuration en bas de page avec le bouton Enregistrer la configuration.



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

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

`configuration` dans le menu `Fichier`.



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

Les différentes valeurs attribuées aux variables sont enregistrées dans un fichier `config.eol` au format JSON[p.766] 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.781] 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.764].

> 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.781] 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.764].



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

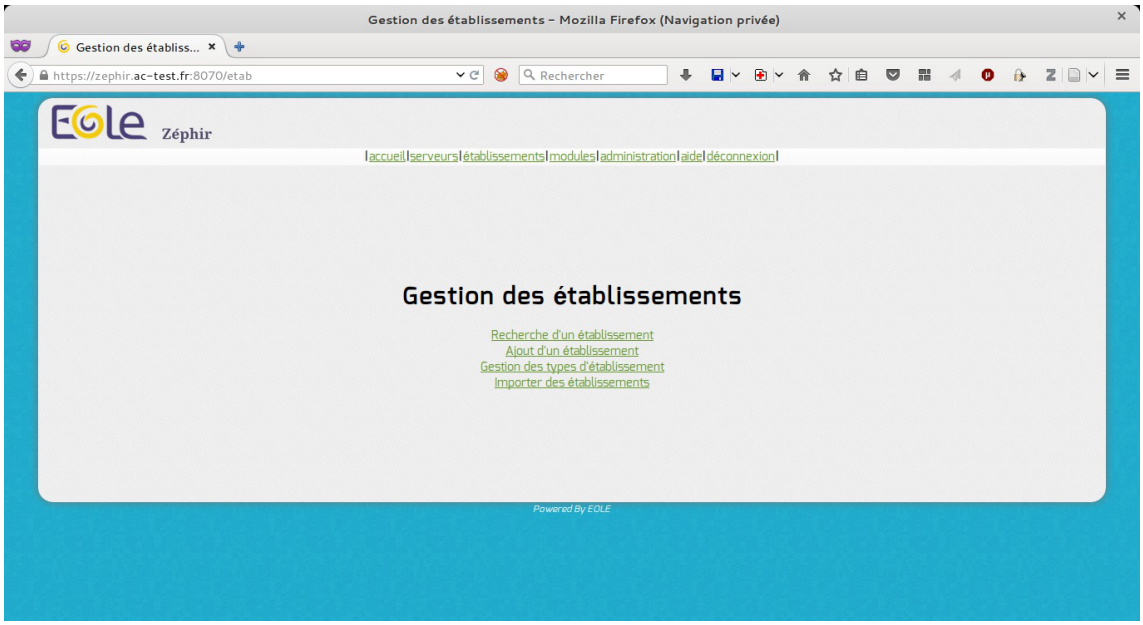
L'établissement d'appartenance du serveur doit déjà exister dans la base des serveurs.



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`.



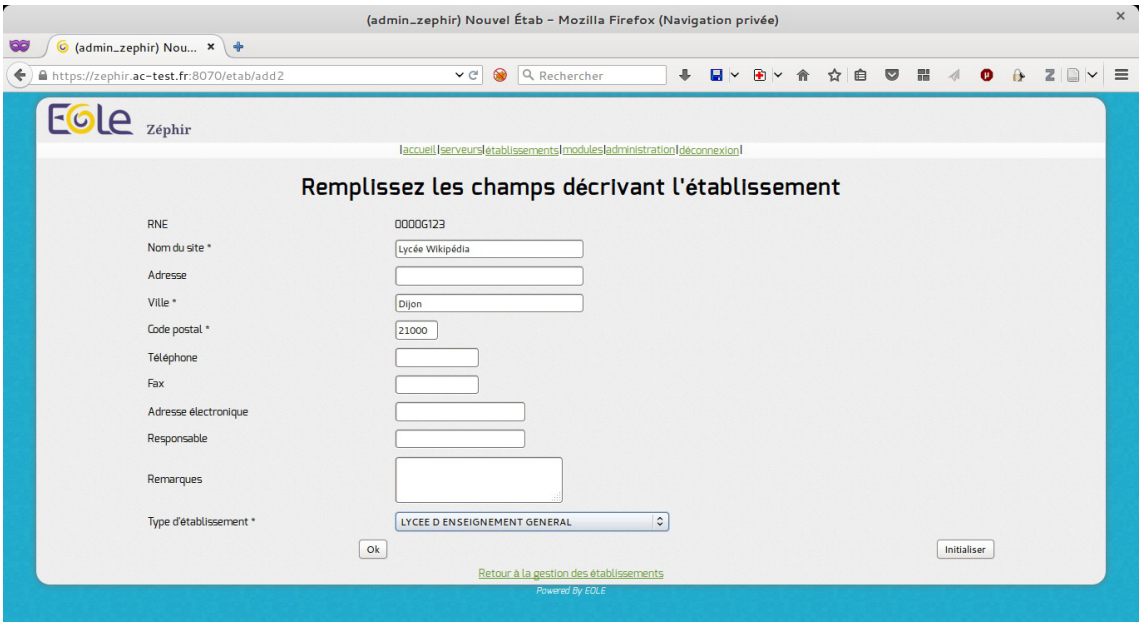
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.776]) CSV[p.758] avec comme séparateur un "|".

Les champs suivants sont attendus :

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

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

Après l'importation un rapport est affiché.



L'enregistrement d'un serveur

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

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

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



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

Configuration minimale du réseau

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

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



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

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

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

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



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

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

Déroulement de l'enregistrement

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

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

- saisir l'adresse du serveur Zéphir, ainsi qu'un nom d'utilisateur et un mot de passe autorisé en écriture dans l'application web Zéphir ;
- dans le cas d'utilisation de certificats non reconnus par une autorité de certification, il faut, pour procéder à l'enregistrement d'un serveur, copier le certificat de la CA locale du serveur Zéphir `/etc/ssl/certs/ca_local.crt` sur la machine à enregistrer dans le répertoire `/usr/local/share/ca-certificates/` et mettre à jour les certificats sur la machine locale à l'aide de la commande `update-ca-certificates` ;
- relancer la procédure d'enregistrement avec la commande `enregistrement_zephir` ;
- si le serveur n'a pas été pré-créé sur le serveur Zéphir, répondre `oui` à la question `Créer le serveur dans la base Zéphir ?` ;
- saisir le numéro RNE qui doit au préalable exister dans l'application Zéphir ;
- saisir le libellé du serveur ;
- répondre aux diverses questions sur le matériel ;
- répondre aux diverses questions sur l'installateur ;
- choisir un module et une variante dans les listes proposées ;
- synchronisation de la configuration :
  - si la configuration a été faite en mode autonome sur le module à enregistrer choisir `Sauver la configuration actuelle sur Zephir`
  - si la configuration a été réalisé sur le serveur Zéphir choisir `Récupérer les fichiers de variante sur Zéphir`
- un message indiquera que la configuration est bien sauvegardée et que les communications avec Zéphir sont configurées. Dans le cas où des paramètres du serveur ne seraient pas renseignés (paramètres provenant d'une variante), un message vous préviendra que ceux-ci doivent être saisis.

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

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

```
root@eolebase:~# enregistrement_zephir

 Procédure d'enregistrement sur le serveur Zéphir

Entrez l'adresse du serveur Zéphir : 192.168.240.254
Entrez votre login pour l'application Zéphir (rien pour sortir) : admin_zephir
Mot de passe pour l'application Zéphir pour admin_zephir :

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

Certificat de Zéphir non validé !

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


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

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

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

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

root@eolebase:~# enregistrement_zephir

 Procédure d'enregistrement sur le serveur Zéphir

Entrez l'adresse du serveur Zéphir : 192.168.240.254
Entrez votre login pour l'application Zéphir (rien pour sortir) :
admin_zephir
Mot de passe pour l'application Zéphir pour admin_zephir :

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

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

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

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

** liste des modules disponibles **

47 amon-2.4
46 eolebase-2.4
42 horus-2.4
45 scribe-2.4
43 sentinelle-2.4
44 sphynx-2.4
```


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

```
48 thot-2.4

module (eolebase-2.4 par défaut):

** liste des variantes de ce module **

45 * standard

variante (45 par défaut):

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

** Configuration des communications vers le serveur Zéphir **

1 -> Ne rien faire
2 -> Récupérer les fichiers de variante sur le serveur Zéphir
3 -> Sauver la configuration actuelle sur le serveur Zéphir
4 -> Modifier la variante du serveur

Entrez le numéro de votre choix : 3
Pour l'enregistrement il faut choisir l'option 3.

-- sauvegarde en cours (veuillez patienter) --
-- OK --

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

Le module est correctement enregistré sur le serveur Zéphir.

Lancement de l'interface de configuration

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

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

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



Désinscription d'un serveur

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

```
root@eolebase:~# enregistrement_zephir

  Procédure d'enregistrement sur le serveur Zéphir


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

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

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

  Entrez le numéro de votre choix : 1

Désinscription auprès du serveur Zéphir terminée

root@eolebase:~#
```

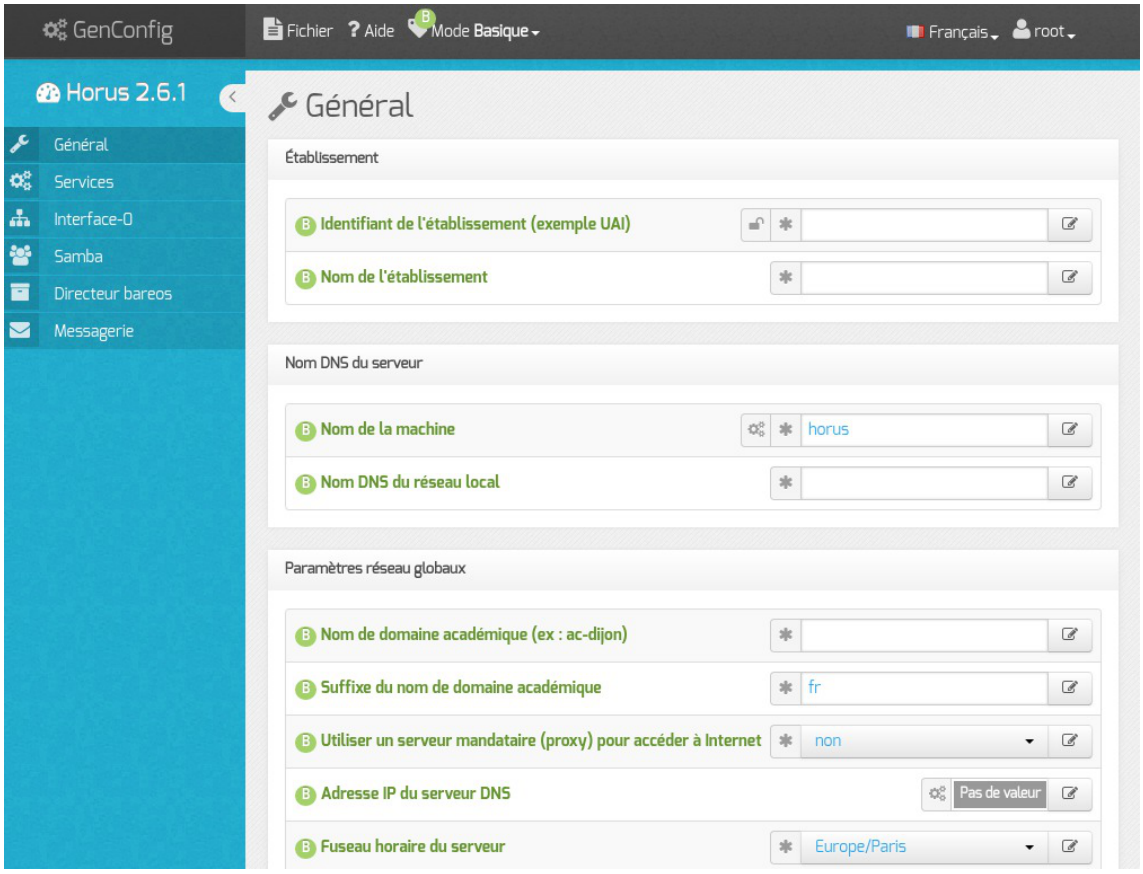

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Configuration en mode basique

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

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

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



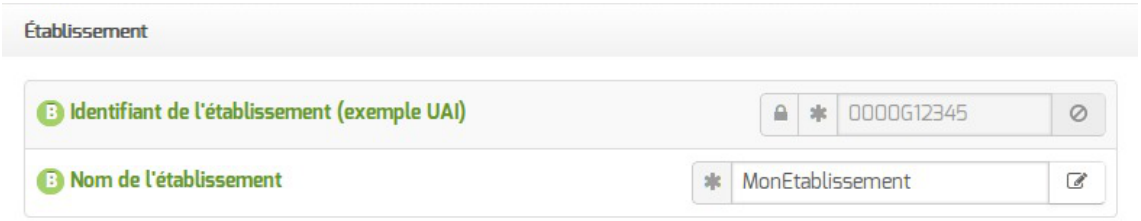
Vue générale de l'interface de configuration du module

2.1. Onglet Général

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

Informations sur l'établissement

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`.

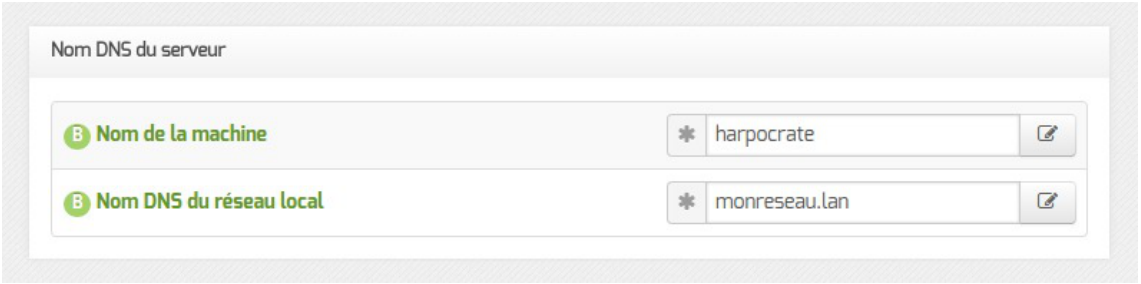
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.766] 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.

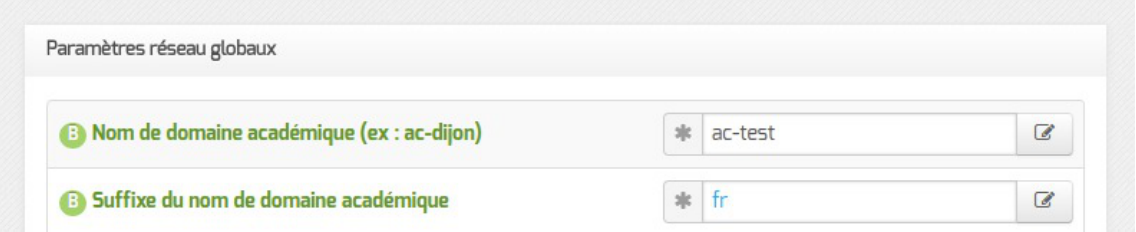
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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

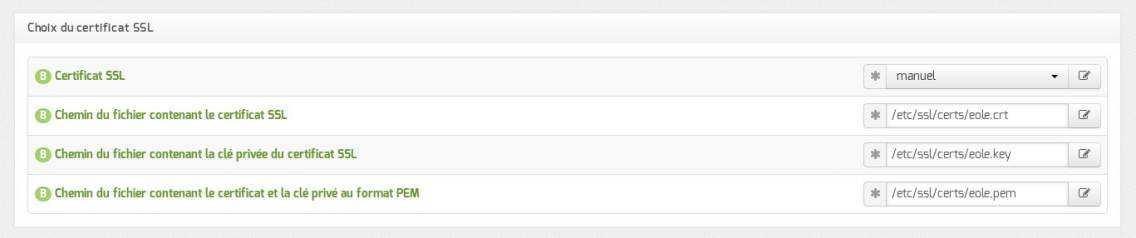
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

IP du ou des serveur(s) de noms DNS[p.759].

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.781] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.753] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.767] ;
- `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.

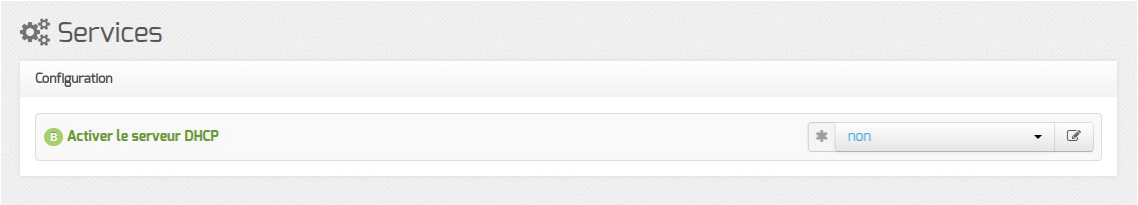
2.2. Onglet Services

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

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

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

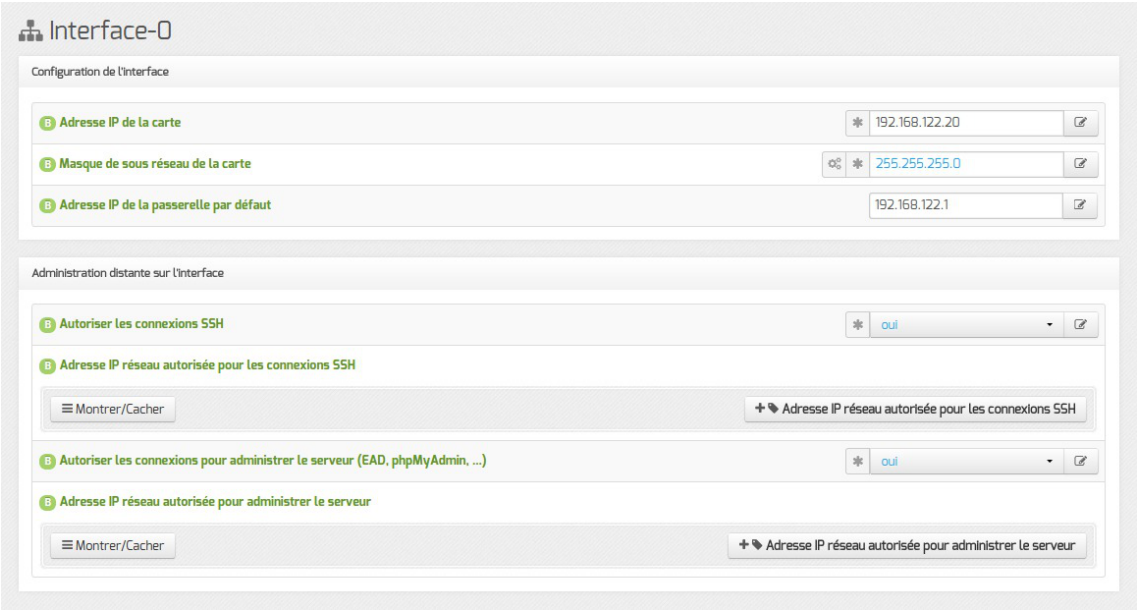
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



En mode basique seul le service DHCP est activable.

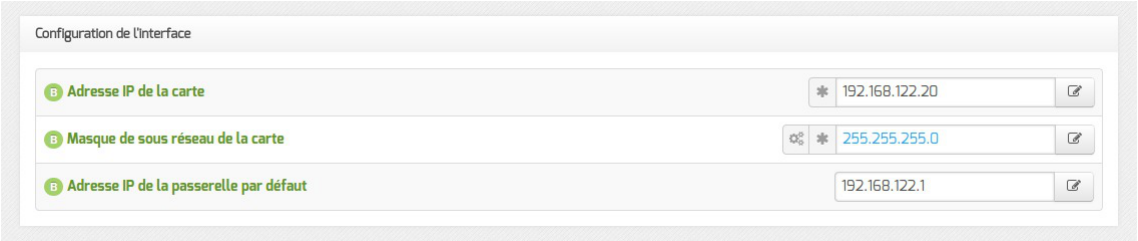
2.3. Onglet Interface-0

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



Vue de l'onglet Interface-n

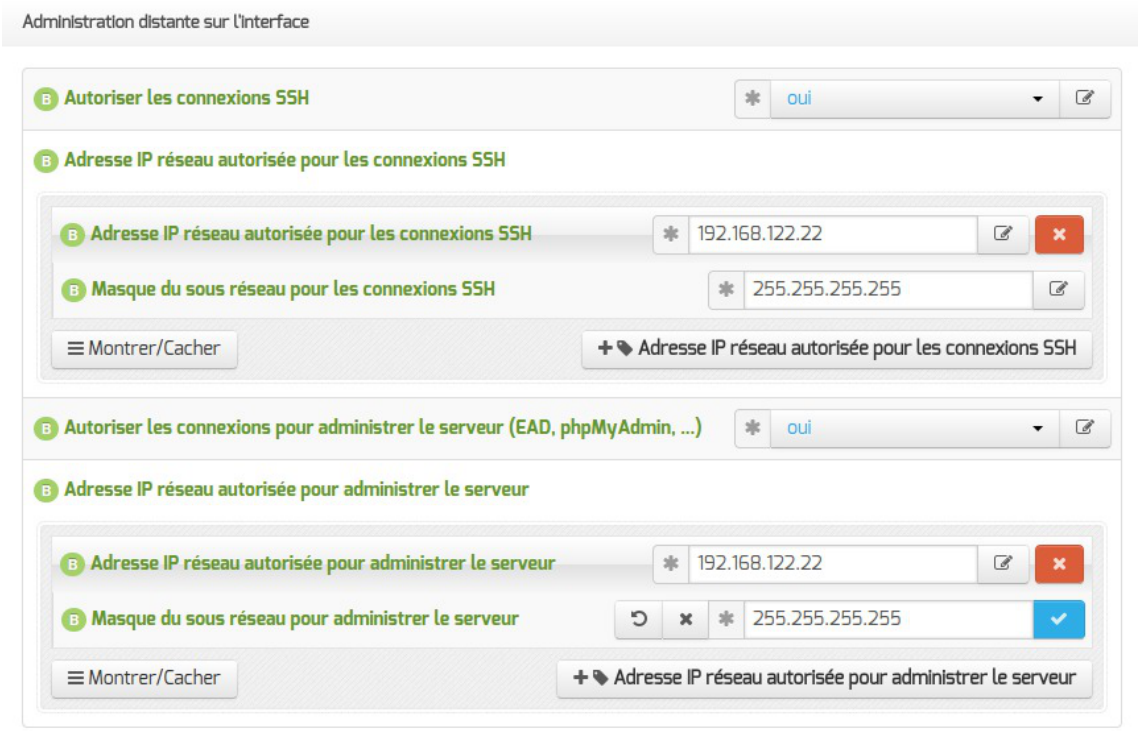
Configuration de l'interface



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)

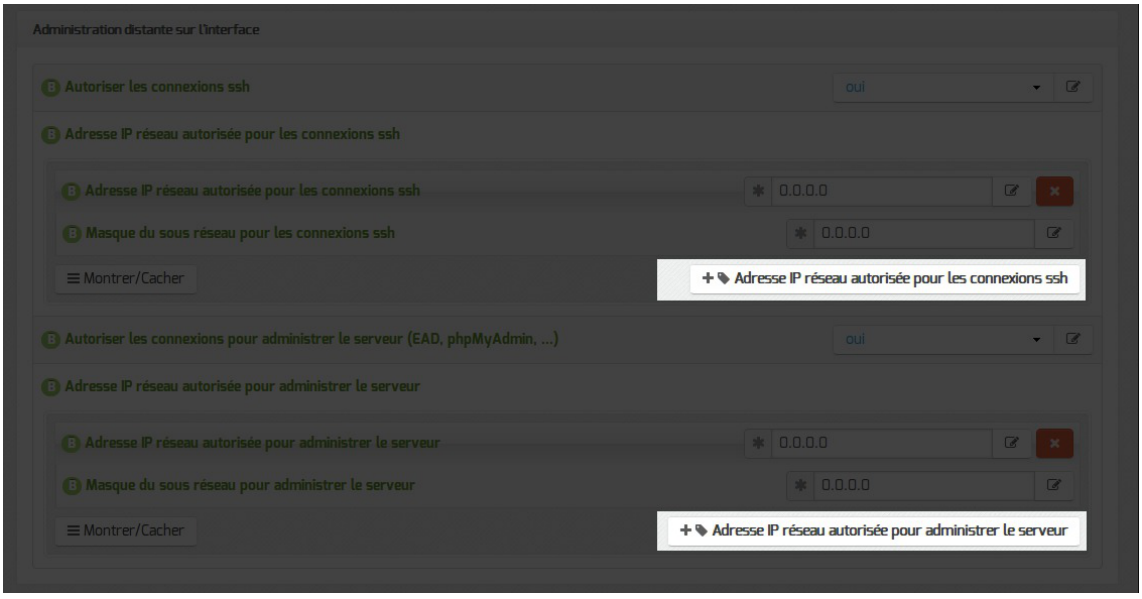


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.779] 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.758] 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.

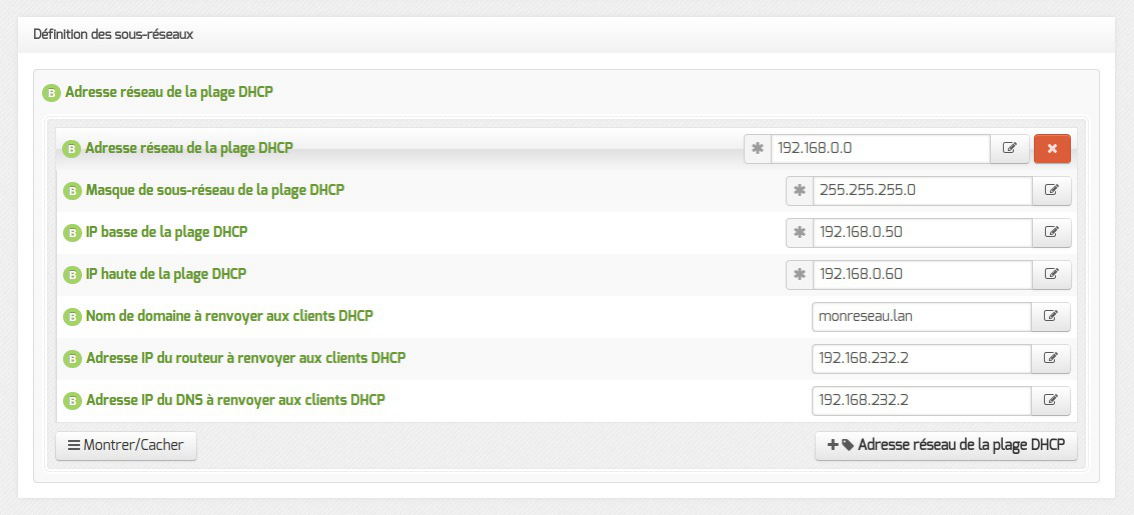
Sur les modules Seth, Horus, Scribe et Eclair (mode une carte), les adresses servies doivent généralement être sur le réseau local (interface 0).

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.776] 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`.



La plage DHCP doit contenir au moins autant d'adresses que le nombre de stations susceptibles d'être

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

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.761] 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.759], 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.

2.5. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.774]) de type Windows NT.

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

Cela signifie qu'il permet une authentification centralisée des ouvertures de session sur les postes clients et qu'il fournit un ensemble de partages aux utilisateurs (dossier personnel, dossier de groupes, partages communs, d'icônes, etc.).

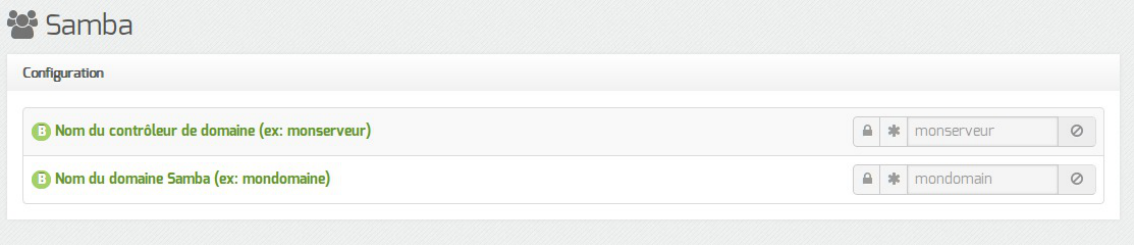
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

Sur le module Scribe, un professeur aura globalement plus de droits qu'un élève. Il a également à sa disposition des outils lui permettant d'interagir avec les élèves (observation, blocage, distribution de documents, etc.).

Seules deux variables sont à remplir avec attention pour obtenir un contrôleur fonctionnel.

Elles se trouvent dans l'onglet `Samba` de l'interface de configuration du module.

Domaine Samba



Configuration Samba

Le champ `Nom du contrôleur de domaine` (nom d'ordinateur NetBIOS[p.770][p.770]) est le nom qui sera utilisé pour accéder aux fichiers avec la syntaxe `\\machine`.

Sa taille maximale est fixée à 15 caractères et il ne doit pas être modifié une fois le module instancié.

En mode conteneur (sur les modules AmonEcole et ses variantes), il doit impérativement être différent du `Nom de la machine`.

Le champ `Nom du domaine Samba`, aussi appelé groupe de travail (workgroup) est le nom qui sera utilisé lors de l'intégration d'une station au domaine.

Sa taille maximale est également fixée à 15 caractères et il ne doit pas être modifié une fois que le module instancié.

Il doit impérativement être différent du `Nom du contrôleur de domaine`.

Caractères autorisés et non autorisés

Noms d'ordinateur NetBIOS peuvent contenir tous les caractères alphanumériques à l'exception des caractères étendus suivants :

- la barre oblique inverse (\) ;
- marque de barre oblique (/) ;
- signe deux-points (:) ;
- astérisque (*) ;

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

- point d'interrogation (?) ;
- guillemet (") ;
- inférieur à (<) signe ;
- signe supérieur à (>) ;
- barre verticale (|).

Attention, les noms peuvent contenir un point, mais ne peuvent pas commencer par un point.

Pour en savoir plus sur les conventions de nommage dans un domaine, vous pouvez consulter la page :

http://support.microsoft.com/kb/909264/fr

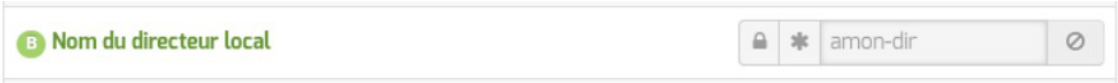
Fichiers invisibles sur les partages

Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- desktop.ini : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`). En mode expert, la liste des fichiers cachés peut être personnalisée grâce à la variable `Fichiers à masquer dans le partage` ;
- $recycle.bin : les fichiers `$recycle.bin` générés par le fonctionnement de Windows sont cachés et inaccessibles par l'utilisateur (`veto files = /$RECYCLE.BIN/` dans le fichier `smb.conf`).

2.6. 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.

2.7. 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)

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



Les paramètres communs à renseigner sont les suivants :

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



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

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

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

Relai des messages



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

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

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

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

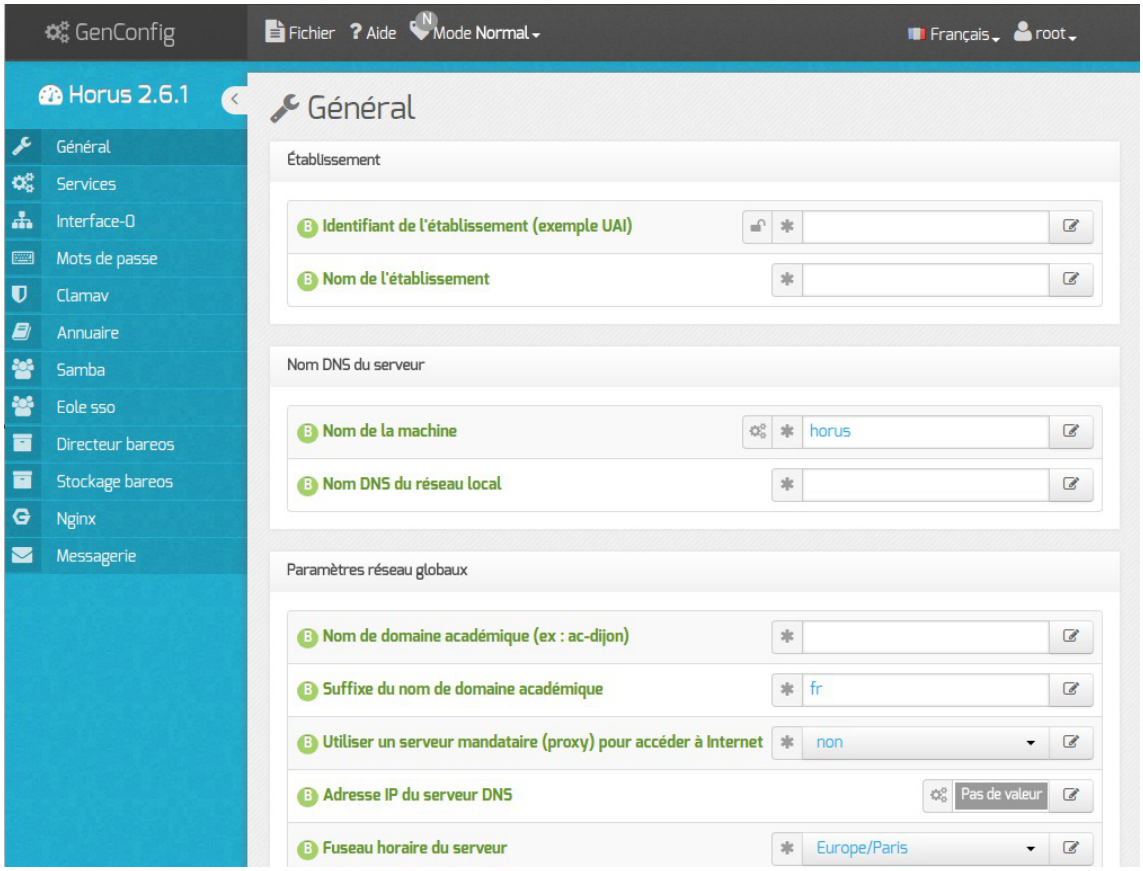
3. Configuration en mode normal

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

- `Général` ;
- `Services` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Mots de passe` ;
- `Clamav` (configuration de l'anti-virus) ;
- `Annuaire` ;
- `Dhcp` * ;
- `Esu` * ;
- `Samba` ;
- `Onduleur` * ;
- `Applications web` * ;
- `Eole sso` ;
- `Directeur bareos` ;
- `Stockage bareos` ;
- `Nginx` ;
- `Reverse proxy` * ;
- `Messagerie`.

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

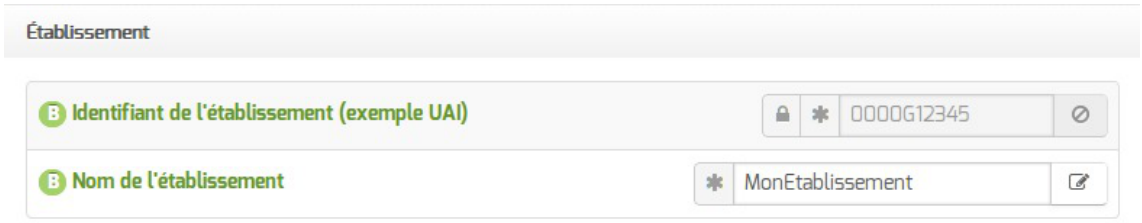
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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, ...

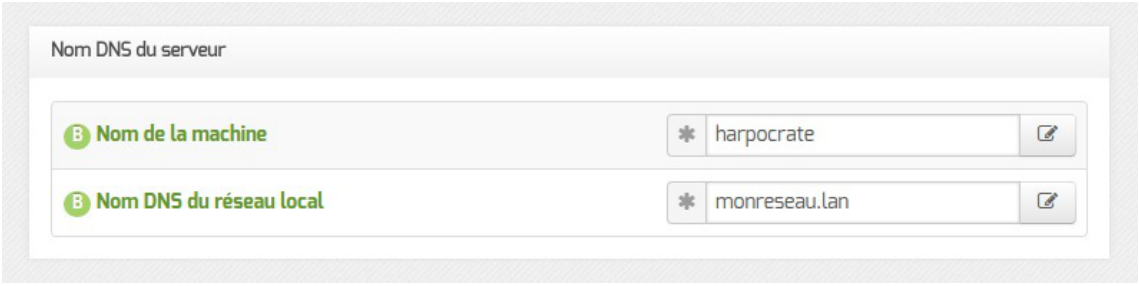
Sur les modules fournissant un annuaire LDAP[p.766] local, ces variables sont utilisées pour créer l'arborescence.



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

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

Nom DNS du serveur



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

Cette information est découpée en 2 champs :

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

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

Le `Nom DNS du serveur` utilise fréquemment des domaines de premier niveau du type `.lan` ou `.local`.

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

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

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

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

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

Paramètres réseau globaux



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

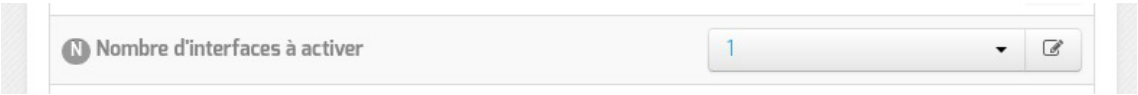
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette information est découpée en plusieurs champs :

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

Nombre d'interfaces

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



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



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

Proxy

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



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

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



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

DNS et fuseau horaire

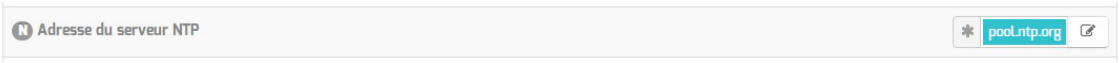


La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.759].

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

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

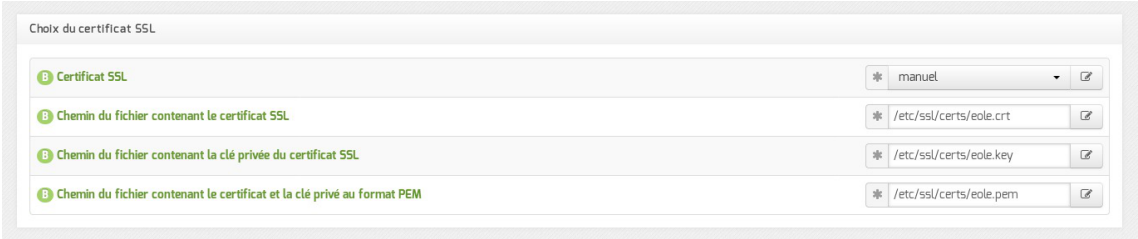
NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.771]. 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.781] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.753] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.767] ;
- `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...

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

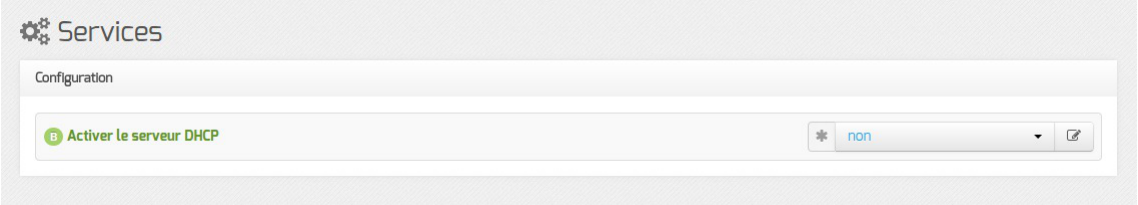
Les différents types de mises à jour [p.430]

3.2. Onglet Services

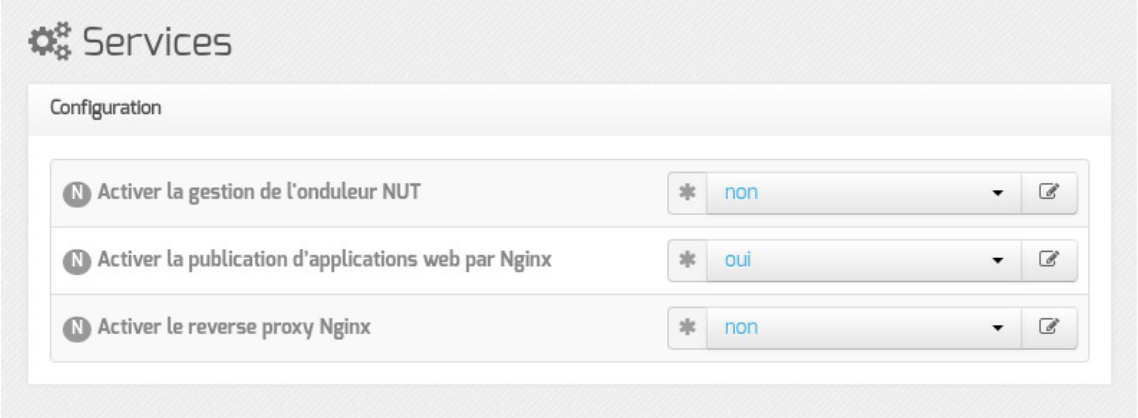
L'onglet Services permet d'activer et de désactiver une partie des services proposés par le module.

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

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



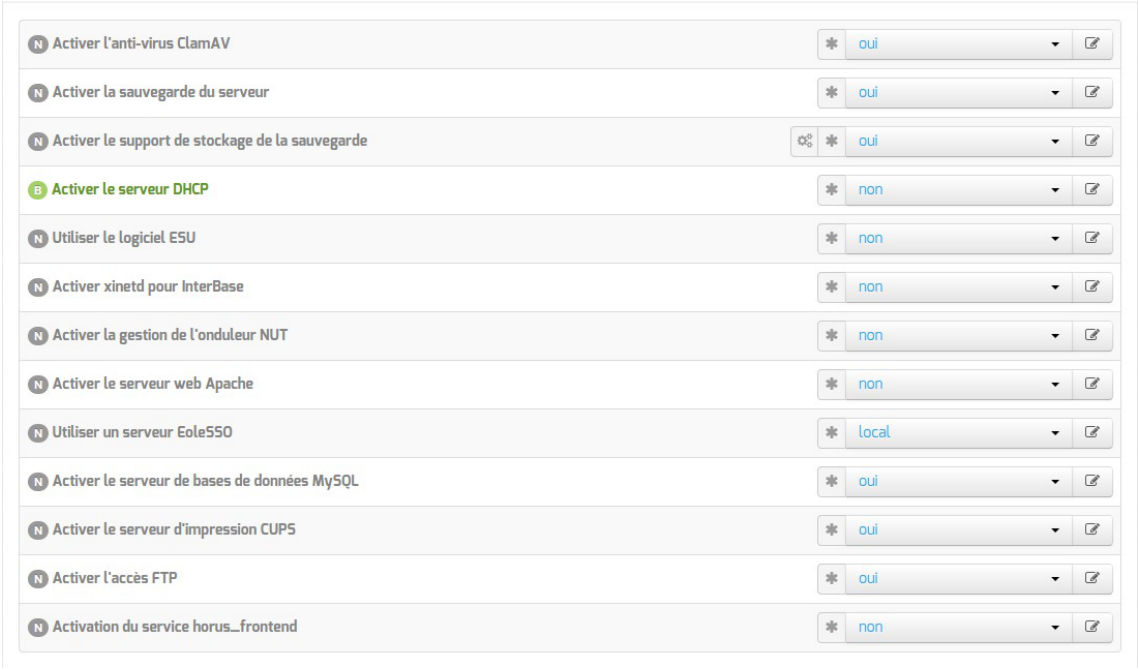
En mode basique seul le service DHCP est activable.



Vue de l'onglet Services en mode normal

Les services de base communs à tous les modules sont la gestion de l'onduleur NUT[p.771], l'activation d'applications web par Nginx et l'activation du proxy inverse.

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



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

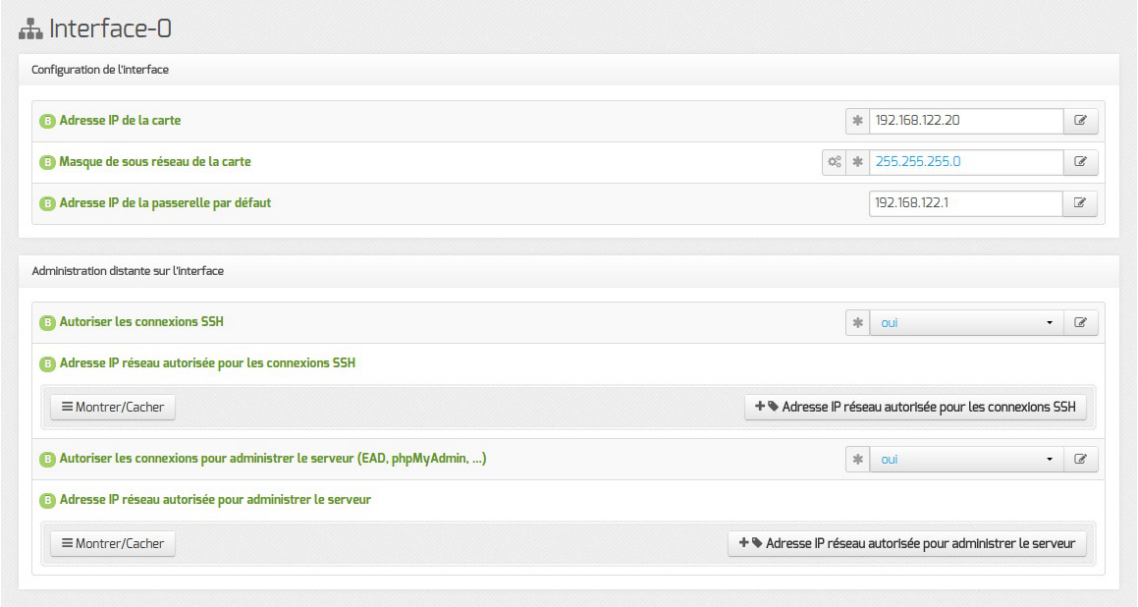
Les services disponibles propres au module Horus en mode normal sont les suivants :

- l'anti-virus ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le logiciel ESU[p.761] ;
- Interbase[p.765] ;
- le serveurs web ;
- l'authentification unique SSO[p.779] ;
- les bases de données MySQL ;
- le serveur d'impression avec CUPS ;
- l'accès FTP ;
- l'interface de gestion des utilisateurs Horus.

3.3. Onglet Interface-0

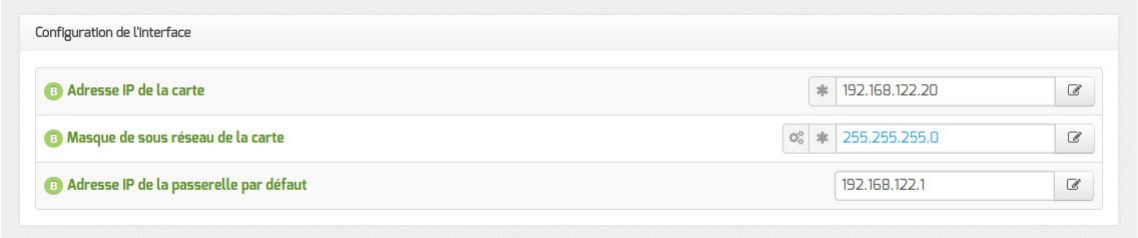
Présentation des différents paramètres de l'onglet `Interface-0`.

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



Vue de l'onglet Interface-n

Configuration de l'interface



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

Administration à distance



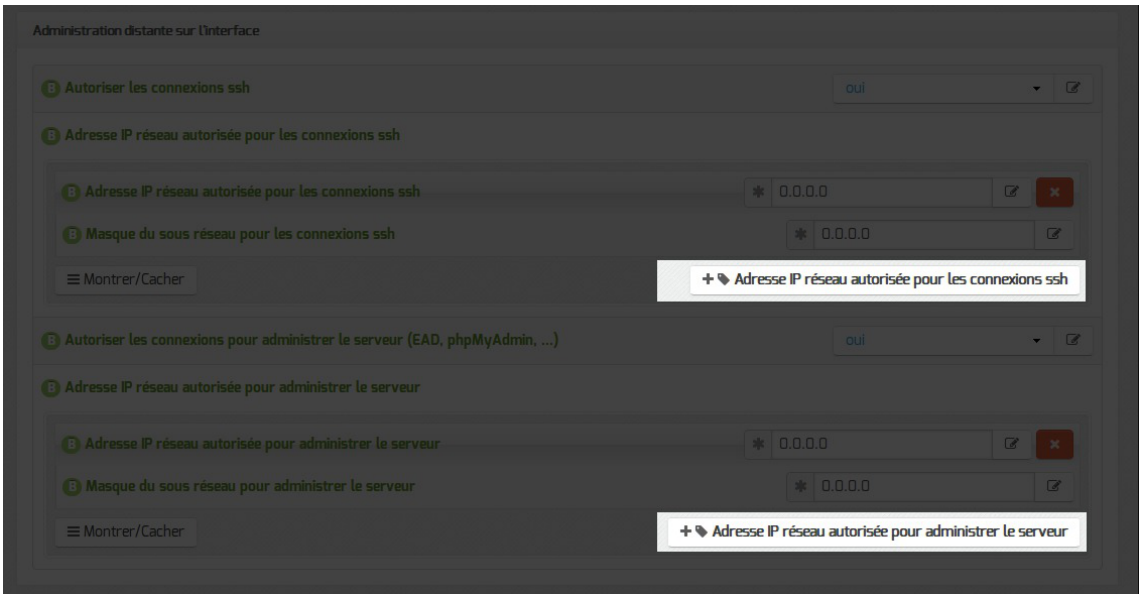
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.779] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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

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

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

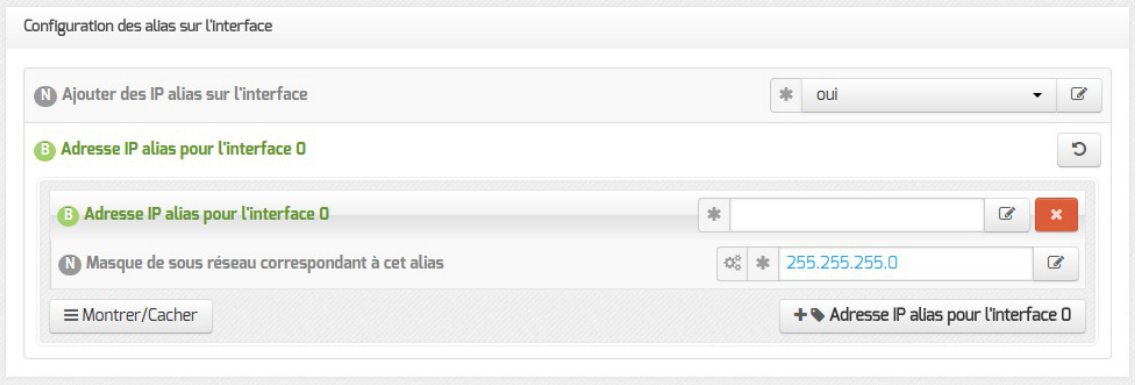
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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

Configuration des alias sur l'interface

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

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

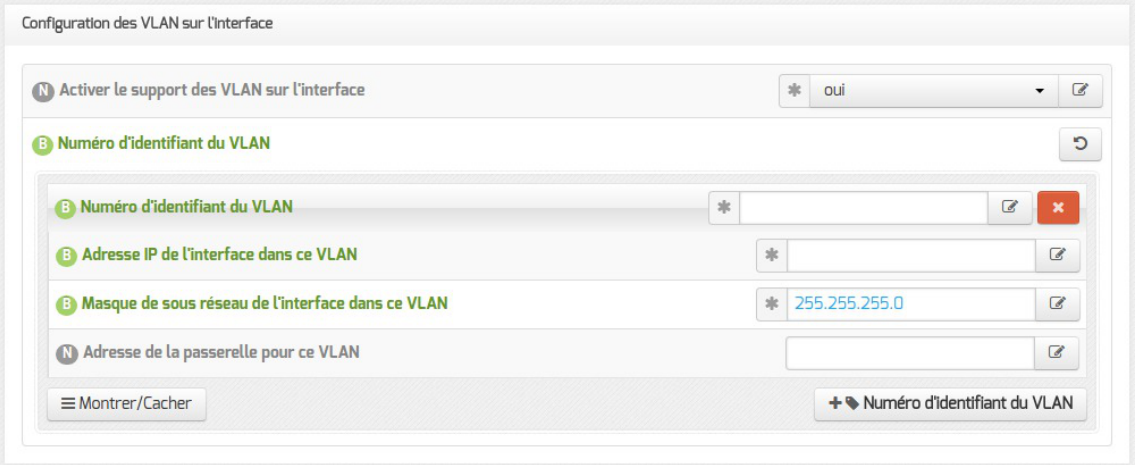


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

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

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.783] (réseau local virtuel) sur une interface déterminée du module.



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

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

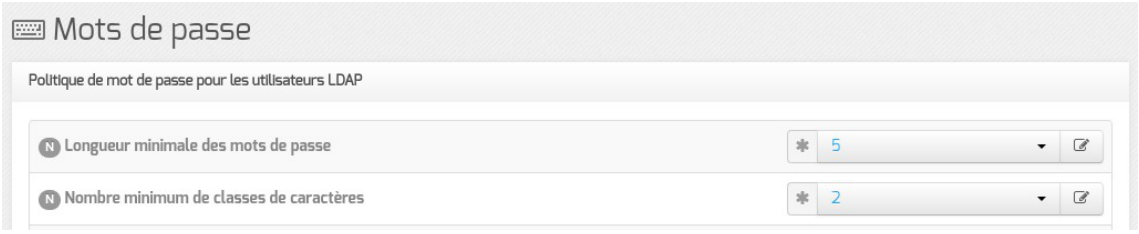
Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.

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

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

3.4. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs

Cet onglet permet de modifier la politique des mots de passe des utilisateurs LDAP et Samba.



Longueur minimale des mots de passe

Cette variable permet de définir la longueur minimale requise pour un mot de passe lors de son changement par l'utilisateur dans sa session Windows (ctrl+alt+suppr).

Cette contrainte s'applique également à toutes les interfaces EOLE permettant de changer des mots de passe (EAD, EOP, EOE, ...).

La longueur minimale est paramétrable de 3 à 12 caractères.

Nombre minimum de classes de caractères

Cette variable permet de choisir le nombre minimum de classes de caractères[p.755] imposées pour le mot de passe d'un compte utilisateur.

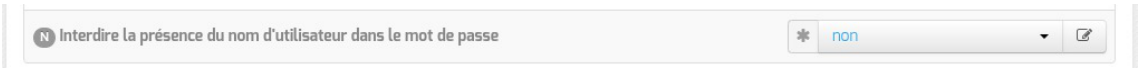
Il est possible d'imposer l'utilisation de 1 à 4 classes différentes parmi :

- caractères minuscules ;
- caractères majuscules ;
- caractères numériques ;
- autres caractères (spéciaux et accentués).



Attention, un mot de passe sécurisé doit avoir une longueur de 8 caractères et doit contenir au minimum 3 classes différentes de caractères.

À partir de la version EOLE 2.6.2, une nouvelle contrainte est disponible pour permettre forcer l'utilisation d'un mot de passe plus fort.



Interdire la présence du nom d'utilisateur dans le mot de passe

La présence du nom d'utilisateur dans le mot de passe affaiblit le mot de passe en permettant qu'une partie des caractères utilisés pour le mot de passe soient prévisibles.

Interdire la présence du nom d'utilisateur dans le mot de passe permet de rejeter un mot de passe lors de son changement si celui-ci contient le nom de l'utilisateur concerné.

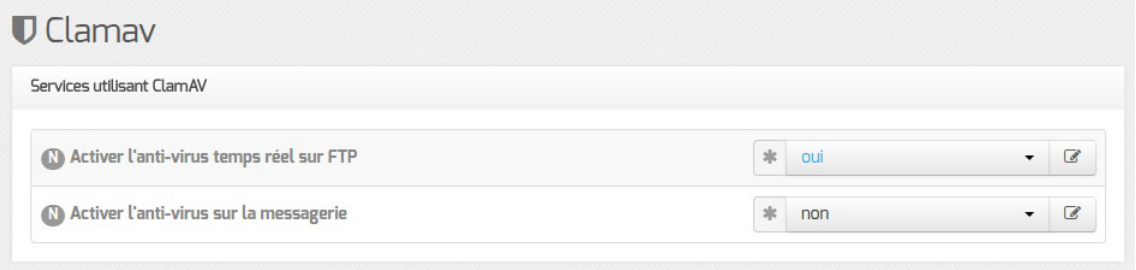
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Dans le cadre de l'utilisation d'un serveur Active Directory distant, la politique de sécurité définie dans l'onglet `Mots de passe` doit être en accord avec celle du serveur AD.

3.5. 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



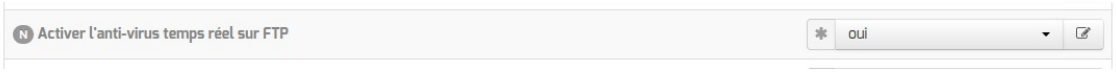
Par défaut, le service est activé sur le module et l'anti-virus est actif uniquement sur le service FTP.
Sur le module Horus il est possible d'activer l'anti-virus sur :

- le service SMB ;
- 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.

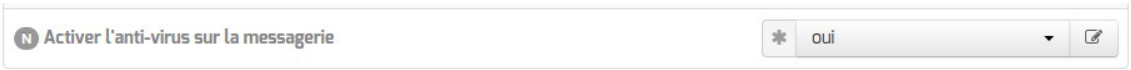
Activation de l'anti-virus sur FTP

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

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`.



Contribuer

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

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).

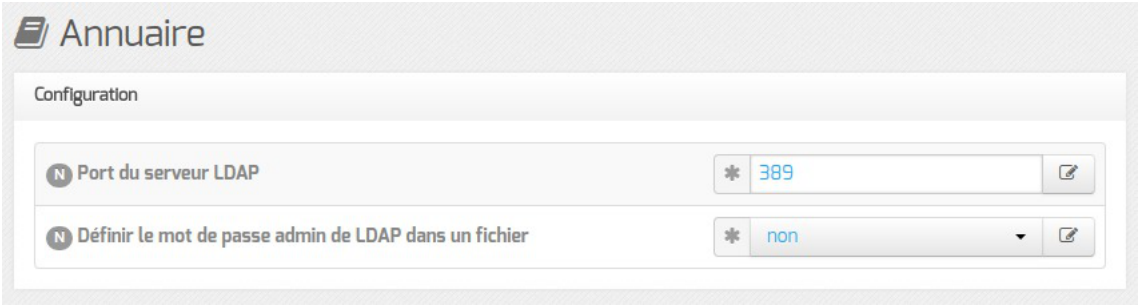
Pour cela il faut utiliser le formulaire suivant (en) : http://www.clamav.net/contact#reports
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.
En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.



Il ne faut pas signaler des PUA[p.775] comme étant des faux positifs.

3.6. Onglet Annuaire

Sur les modules Horus, Scribe et AmonEcole l'annuaire OpenLDAP est local.



Lorsque l'annuaire est configuré comme étant local, l'onglet propose 2 paramètres :

- `Port du serveur LDAP` : permet de changer le port d'écoute du serveur LDAP ;
- `Définir le mot de passe admin de LDAP dans un fichier` : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire dans le fichier `/root/.writer`.

3.7. Onglet Dhcp : Configuration du serveur DHCP

Le serveur DHCP[p.758] 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.

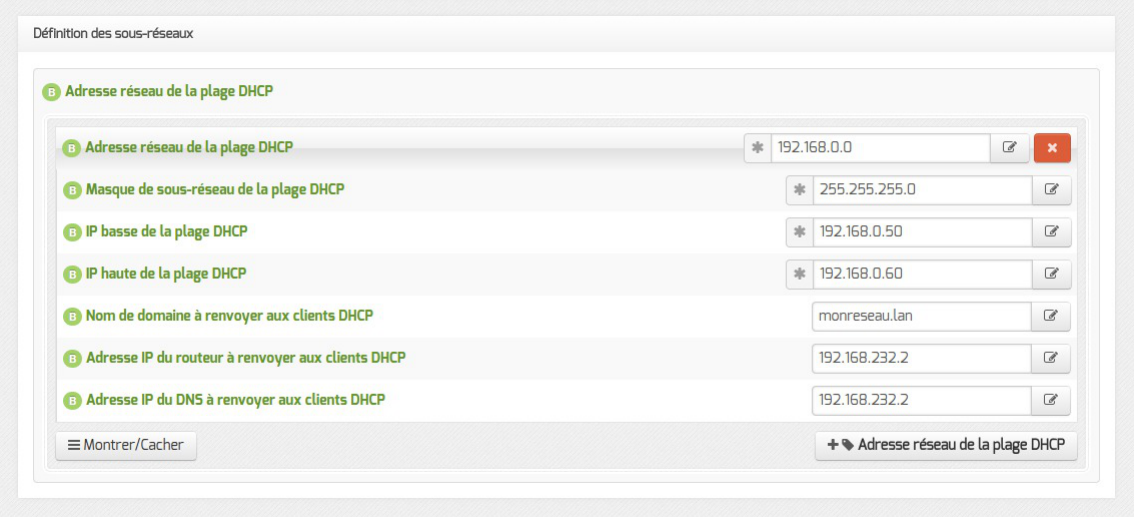
Sur les modules Seth, Horus, Scribe et Eclair (mode une carte), les adresses servies doivent généralement être sur le réseau local (interface 0).
Sur les modules AmonEcole et AmonEcole-Eclair, les adresses servies sont celles du réseau interne (interface 1).

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.776] 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.761] 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.759], 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

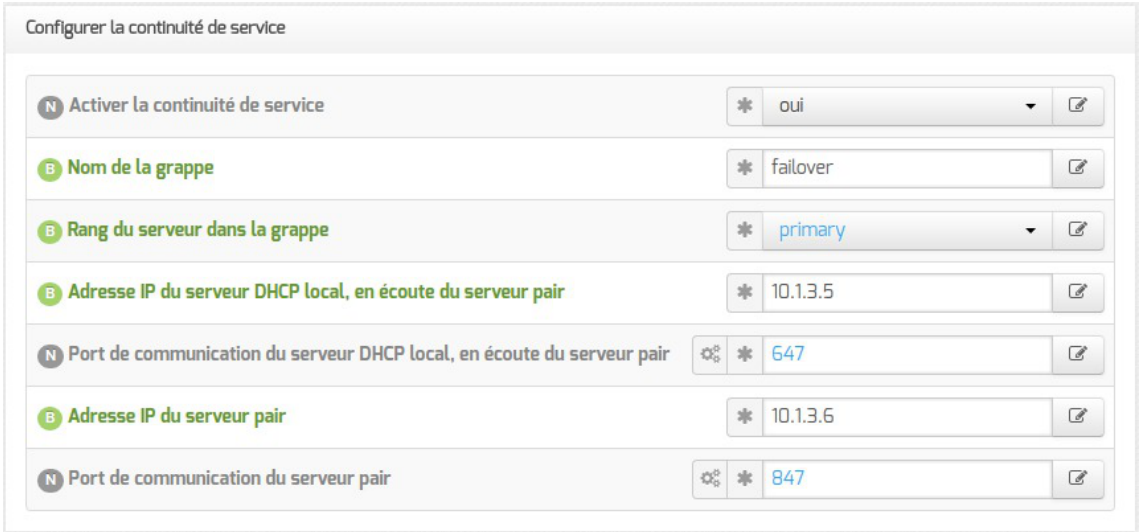
À partir de la version 2.6.2, il est possible de mettre en place de la continuité de service pour le DHCP.

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

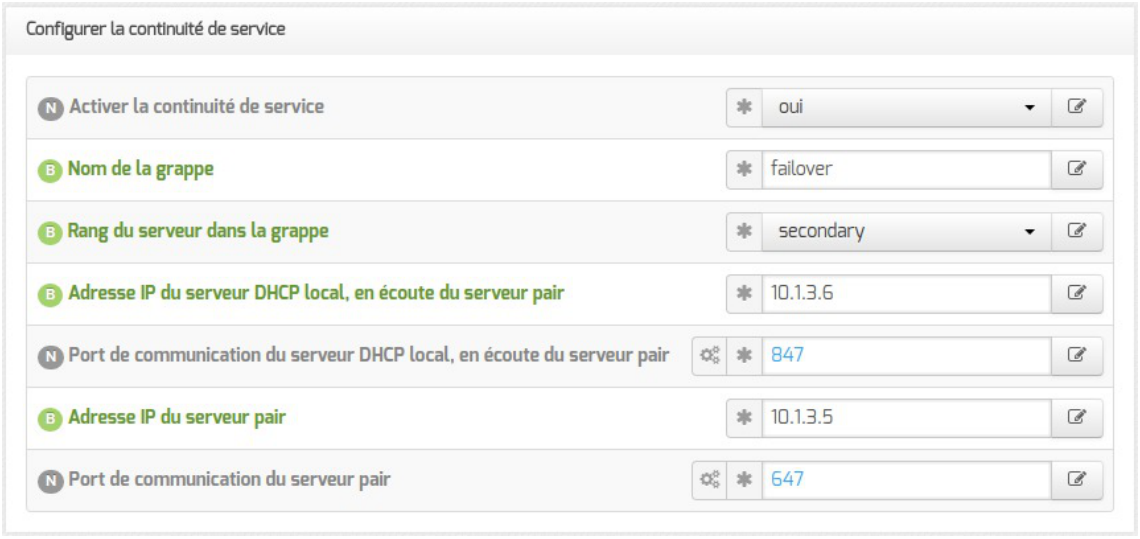


- `Nom de la grappe` : le nom de la grappe devra être le même sur le serveur primaire (local) et sur le serveur secondaire (pair) ;
- `Rang du serveur dans la grappe` : choisir `primary` pour le serveur primaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de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

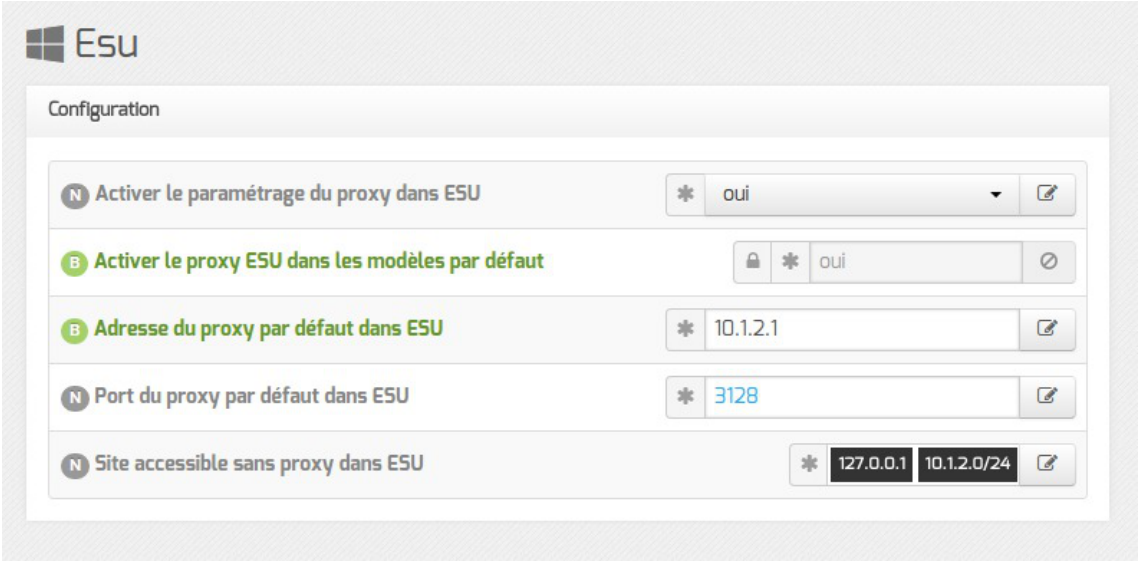
- `Nom de la grappe` : le nom de la grappe doit être le même que pour le serveur primaire (local) ;
- `Rang du serveur dans la grappe` : choisir `secondary` pour le serveur secondaire ;
- `Adresse IP du serveur DHCP local, en écoute du serveur pair` : saisir l'adresse IP de l'interface sur laquelle écoute 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`.

3.8. Onglet Esu : Configuration du proxy ESU

Sur les modules Scribe et AmonEcole, l'utilisation du couple ESU / ClientScribe est obligatoire pour les stations Windows Microsoft rattachées au domaine et l'onglet `Esu` est d'emblée visible.

Sur le module Horus, l'onglet `Esu` n'est visible qu'après activation du service dans l'onglet `Services` en passant l'option : `Utiliser le logiciel ESU` à `oui`. Ce mode de fonctionnement nécessite l'installation du logiciel ClientHorus sur les stations clientes.

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



La configuration du proxy pour des stations clientes gérées par ESU s'effectue au niveau de l'interface de configuration du module dans l'onglet `Esu`.

Après avoir passé la variable `Activer le paramétrage du proxy dans ESU` à `oui` il est possible de paramétrer le proxy ESU.

La variable `Activer le proxy ESU dans les modèles par défaut` permet de définir le comportement du proxy ESU dans les modèles par défaut. Ce choix par défaut sera appliqué dans les modèles à l'instance et ne pourra plus être modifié par l'interface de configuration du module.

Si, à l'avenir, l'utilisateur souhaite changer le comportement du proxy il devra le faire au travers de l'interface ESU.

> Les paramètres suivants `Adresse du proxy par défaut dans ESU`, `Port du proxy par défaut dans ESU` et `Réseau par défaut sans proxy dans ESU` sont modifiables à souhait et sont appliqués dans les variables ESU à chaque reconfiguration du module.

Saisir l'adresse IP ou le nom du proxy ESU dans le champ `Adresse du proxy par défaut dans ESU` et si besoin changer le port `3128` proposé par défaut.

Le champ `Site accessible sans proxy dans ESU` (nommé `Réseau par défaut sans proxy dans ESU` dans les versions antérieures à EOLE 2.5.2) permet d'ajouter plusieurs adresses IP, réseaux, noms de domaine et noms de machines pour lesquels le proxy ESU ne sera pas utilisé (exemple de valeurs : `mozilla.org`, `asso.fr`, `192.168.1.0/24`).

> Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet `Interface-1` (variable : `adresse ip eth1 proxy link`).

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

L'utilisation du logiciel ESU modifie profondément la configuration des stations clientes (emplacement des icônes, ...) et sa désactivation ne restaure pas leur configuration d'origine.

Pour récupérer une station utilisable hors du domaine, vous pouvez :

- ré-activer ESU, renseigner les options telles qu'elles sont sur un Windows par défaut (cases décochées), ouvrir une session et désactiver ESU ;
- restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que celui fourni par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

3.9. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.774]) de type Windows NT.

Cela signifie qu'il permet une authentification centralisée des ouvertures de session sur les postes clients et qu'il fournit un ensemble de partages aux utilisateurs (dossier personnel, dossier de groupes, partages communs, d'icônes, etc.).

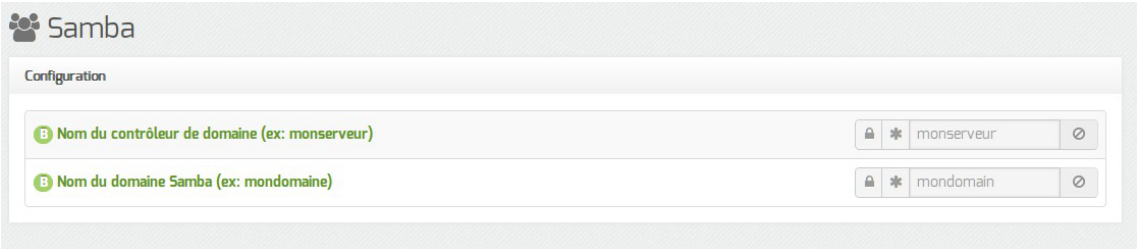
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

Sur le module Scribe, un professeur aura globalement plus de droits qu'un élève. Il a également à sa disposition des outils lui permettant d'interagir avec les élèves (observation, blocage, distribution de documents, etc.).

Seules deux variables sont à remplir avec attention pour obtenir un contrôleur fonctionnel.

Elles se trouvent dans l'onglet `Samba` de l'interface de configuration du module.

Domaine Samba



Configuration Samba

Le champ `Nom du contrôleur de domaine` (nom d'ordinateur NetBIOS[p.770][p.770]) est le nom qui sera utilisé pour accéder aux fichiers avec la syntaxe `\\machine`.

Sa taille maximale est fixée à 15 caractères et il ne doit pas être modifié une fois le module instancié.

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

> En mode conteneur (sur les modules AmonEcole et ses variantes), il doit impérativement être différent du `Nom de la machine`.

Le champ `Nom du domaine Samba`, aussi appelé groupe de travail (workgroup) est le nom qui sera utilisé lors de l'intégration d'une station au domaine.

> Sa taille maximale est également fixée à 15 caractères et il ne doit pas être modifié une fois que le module instancié.
>
> Il doit impérativement être différent du `Nom du contrôleur de domaine`.

> **Caractères autorisés et non autorisés**
>
> Noms d'ordinateur NetBIOS peuvent contenir tous les caractères alphanumériques à l'exception des caractères étendus suivants :
>
> - la barre oblique inverse (\) ;
> - marque de barre oblique (/) ;
> - signe deux-points (:) ;
> - astérisque (*) ;
> - point d'interrogation (?) ;
> - guillemet (") ;
> - inférieur à (<) signe ;
> - signe supérieur à (>) ;
> - barre verticale (|).
>
> Attention, les noms peuvent contenir un point, mais ne peuvent pas commencer par un point.
>
> Pour en savoir plus sur les conventions de nommage dans un domaine, vous pouvez consulter la page :
>
> http://support.microsoft.com/kb/909264/fr

Fichiers invisibles sur les partages

Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

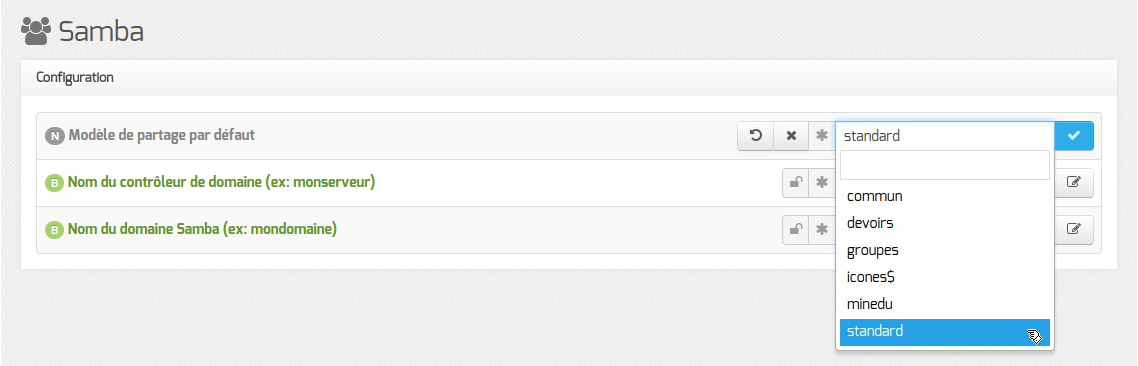
Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- desktop.ini : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`). En mode expert, la liste des fichiers cachés peut être personnalisée grâce à la variable `Fichiers à masquer dans le partage` ;
- $recycle.bin : les fichiers `$recycle.bin` générés par le fonctionnement de Windows sont cachés et inaccessibles par l'utilisateur (`veto files = /$RECYCLE.BIN/` dans le fichier `smb.conf`).

Modèle de partage par défaut

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

En mode normal il est possible de choisir le modèle de partage par défaut.



Le fichier de configuration Samba (`/etc/samba/smb.conf`) est généré à partir des informations contenues dans l'annuaire.

Par défaut, les partages utilisent le template python : `/usr/share/eole/fichier/models/standard.tmpl`

Il est possible d'utiliser un autre modèle de partage par défaut pour les nouveaux partages en renseignant son nom (sans l'extension `.tmpl`) au niveau de l'option `Modèle de partage par défaut`.

Il existe déjà plusieurs modèles à disposition :

- `standard`
  héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe
- `commun`
  héritage des permissions, accès en écriture, accessible à tous en lecture et en écriture, accès anonyme (guest)
- `devoirs`
  héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `groupes`
  héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `icones$`
  caché dans le voisinage réseau, accès anonyme (guest)
- `minedu`
  héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe, nom de fichier et répertoire en minuscules

3.10. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.771]. 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)

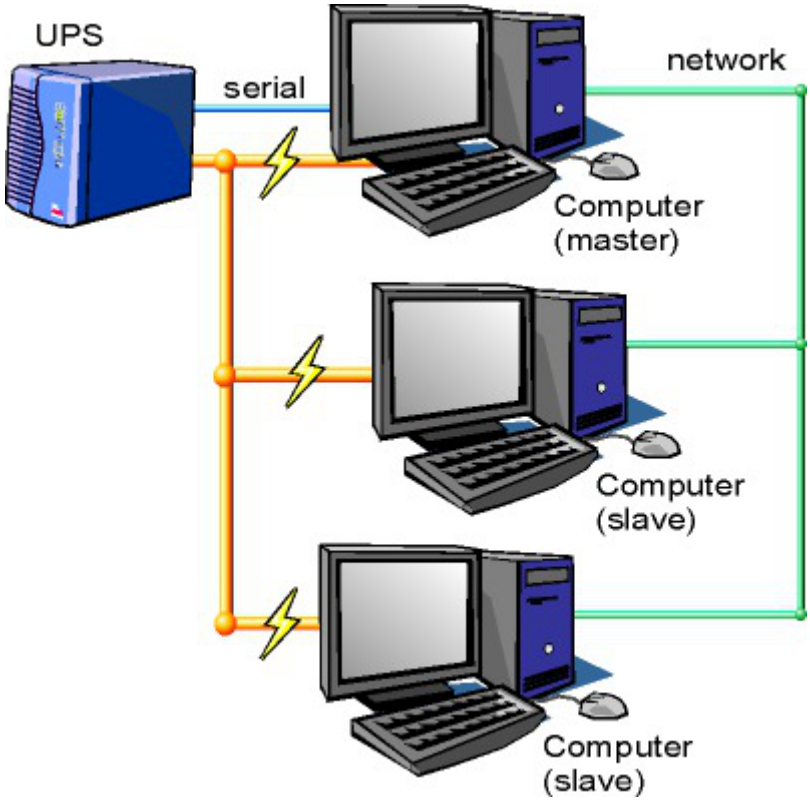


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

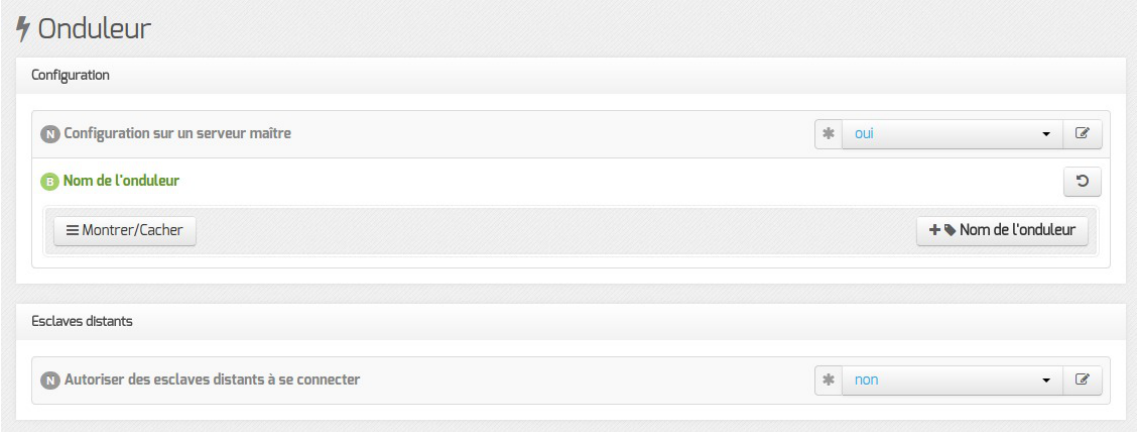
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

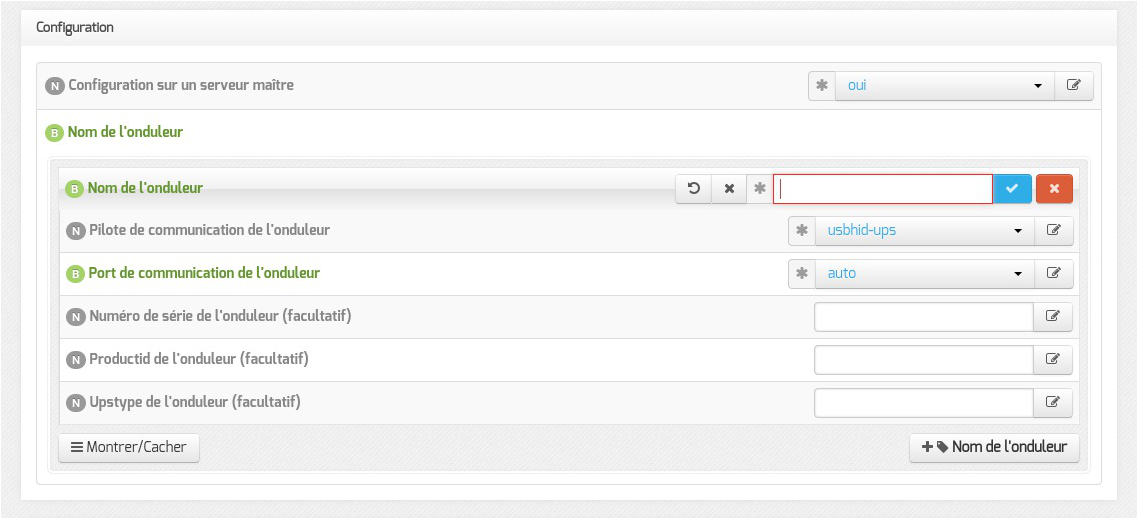
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

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)

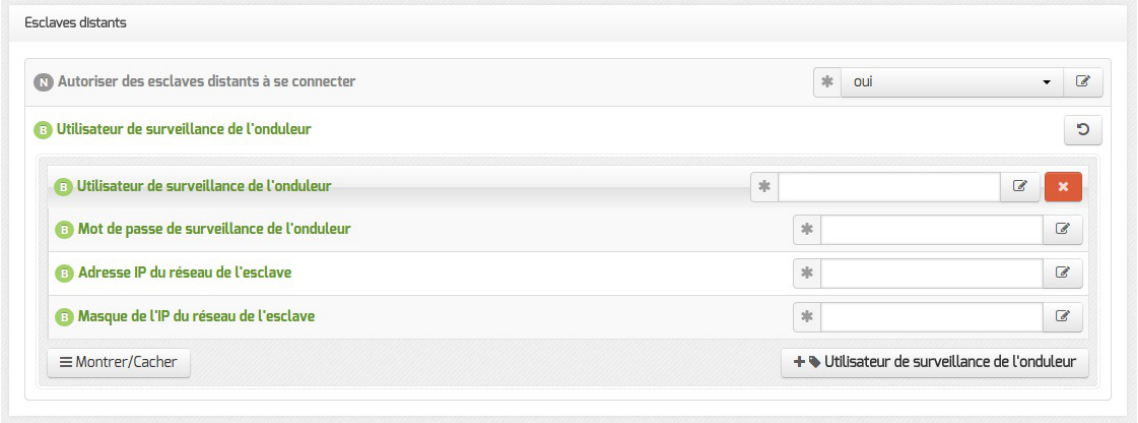
- Port de communication de l'onduleur : `auto`.

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`.

3.11. Onglet Applications web : Configuration des applications web

Les onglets `Applications web` et `Apache` ne sont disponibles qu'après activation du service, `Activer le serveur web Apache` à `oui`, dans l'onglet `Services`.



L'onglet `Applications web` permet un réglage minimum pour le fonctionnement des applications web. Il permet aussi d'activer/désactiver toutes les applications web EOLE installées sur le module.

Nom de domaine des applications web

Le choix du `Nom de domaine des applications web` est essentiel.

Pour un bon fonctionnement de toutes les applications, il est impératif d'utiliser un nom de domaine.

Dans la mesure du possible, il faut que celui-ci soit résolvable sur Internet. Si ce n'est pas le cas, il est possible d'utiliser un nom de domaine local diffusé par le serveur DNS[p.759] de l'établissement.

Ce paramètre ne doit pas être précédé du nom du protocole.



À partir de la version EOLE 2.6.1, les adresses IP ne sont plus autorisées pour cette variable.

Cette restriction est notamment due au durcissement du support du protocole HTTPS[p.764] par les navigateurs.

Application web par défaut

L'application web par défaut sera celle renseignée dans la variable : `Application web par défaut (redirection)`.



Si la variable `Application web par défaut` vaut `/webmail`, alors l'adresse `http://<adresse serveur>/` pointera vers `http://<adresse_serveur>/webmail/`

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

Serveur web et proxy inverse

Lorsque le serveur web est derrière un proxy inverse, c'est l'adresse IP du proxy inverse et non celle de l'utilisateur qui est enregistrée dans les fichiers de journalisation. Pour éviter cela, il est possible de passer la variable `Le serveur web est derrière un reverse proxy` à `oui` et de déclarer son adresse (généralement l'adresse IP du module Amon sur la zone) dans `Adresse IP du serveur reverse proxy`.

Sur le module AmonEcole, si le proxy inverse est activé, les variables sont calculées et masquées : `Le serveur web est derrière un reverse proxy` est à `oui` et l'`Adresse IP du serveur reverse proxy` est celle du bridge interne : `192.0.2.1`.



La déclaration du proxy inverse ajoute une entête qui contient une adresse IP qui peut potentiellement être falsifiée depuis la machine source.

En cas d'utilisation d'un proxy, la récupération de l'adresse IP des stations du réseau local n'est pas garantie.



Sur EOLE 2.6.0 et inférieur, cette fonctionnalité était implémentée via le module Apache additionnel RPAF : https://github.com/gnif/mod_rpaf.

Sur EOLE 2.6.1 et supérieur, cette fonctionnalité est implémentée via le module Apache natif RemoteIP : https://httpd.apache.org/docs/current/fr/mod/mod_remoteip.html

Activer Bareos WebUI (gestion de la sauvegarde)

Bareos WebUI est une application web permettant de surveiller et gérer les sauvegardes Bareos.

Activer phpMyAdmin (administration des bases MySQL)

phpMyAdmin permet de gérer les bases de données MySQL hébergées par le module.

Pour activer/désactiver l'application web phpMyAdmin il faut passer la variable `Activer phpMyAdmin (administration des bases MySQL)` à `oui`.

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

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

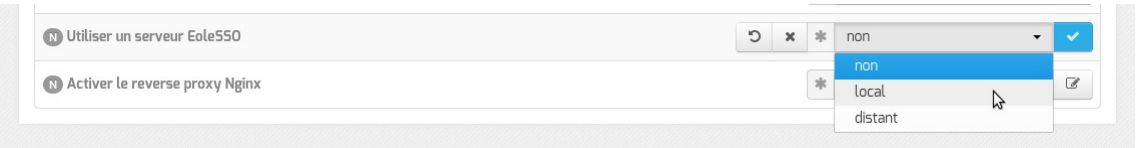
Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

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

Serveur local ou distant

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

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

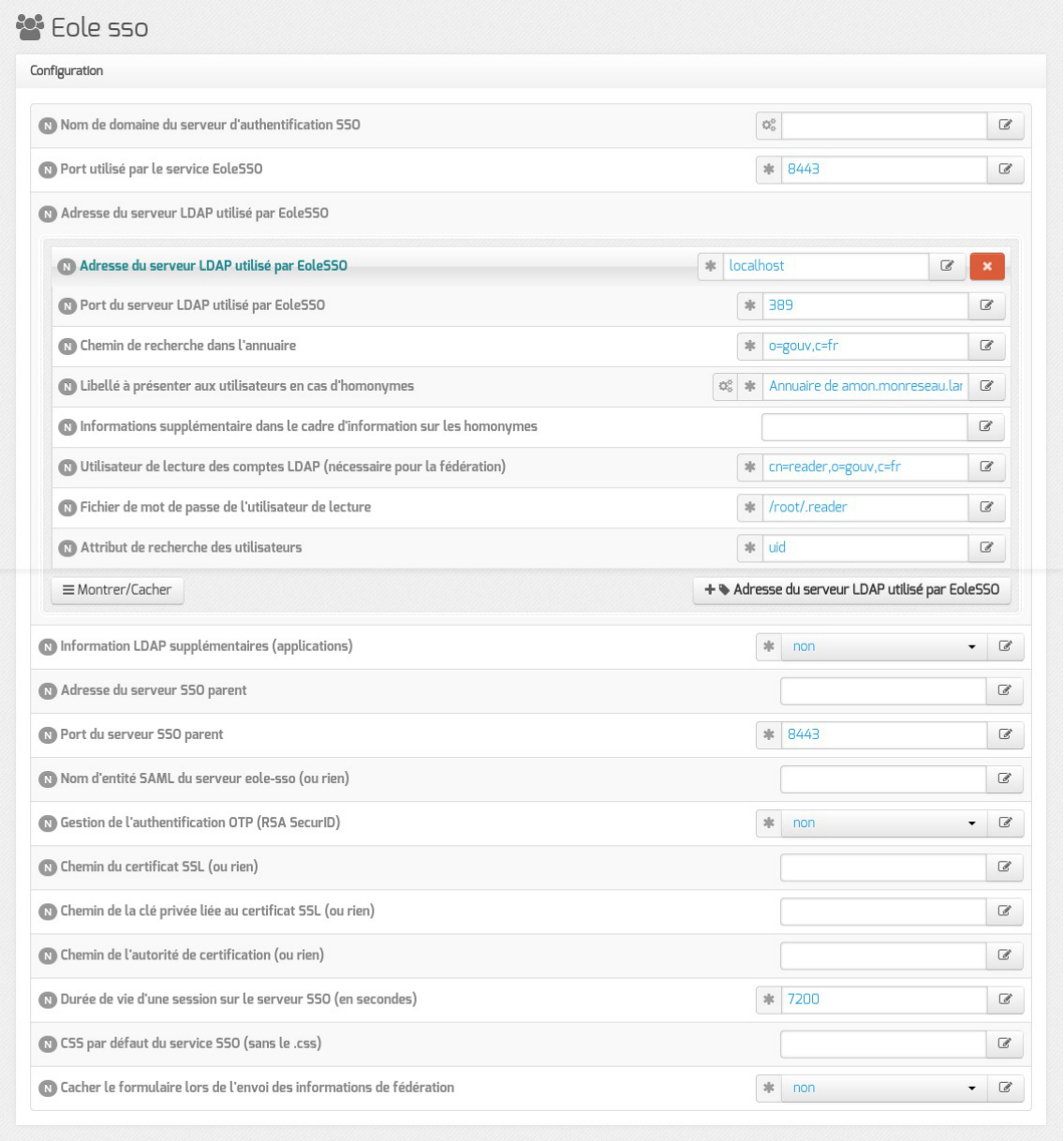


La variable `Utiliser un serveur EoleSSO` permet :

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

Adresse et port d'écoute

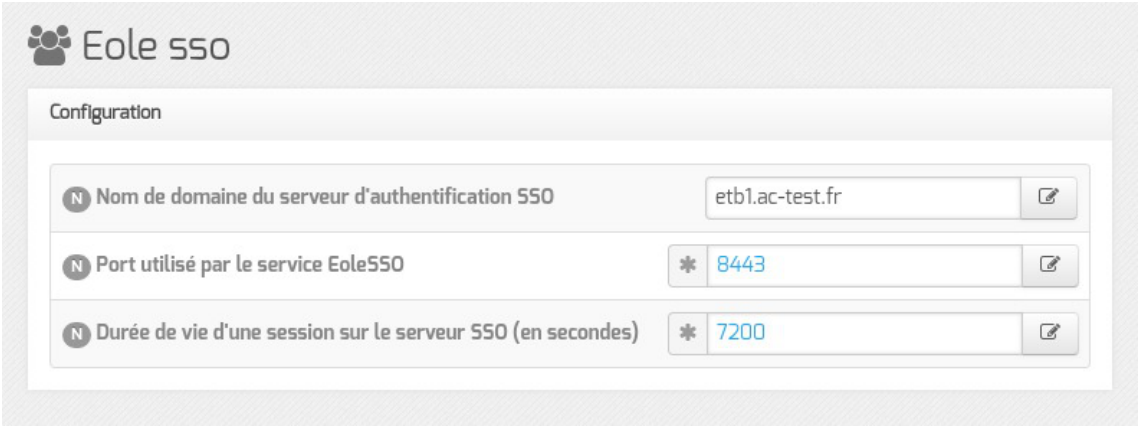
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

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

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



Configuration d'un serveur EoleSSO distant

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

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

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

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.766] pour authentifier les utilisateurs et récupérer leurs attributs.

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs (basedn) ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN[p.758] et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.773] si disponible *(voir plus loin)*.

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



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

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

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

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

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

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

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.784] en HTTPS, sur le port défini pour le serveur EoleSSO).

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



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

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole

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

securID[p.778] de la société EMC (précédemment RSA).

Pour cela il faut :

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

Des champs supplémentaires apparaissent :

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

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.765] du serveur et sont utilisés par défaut.

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

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.777] (version 2).

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

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

Autres options

`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra

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

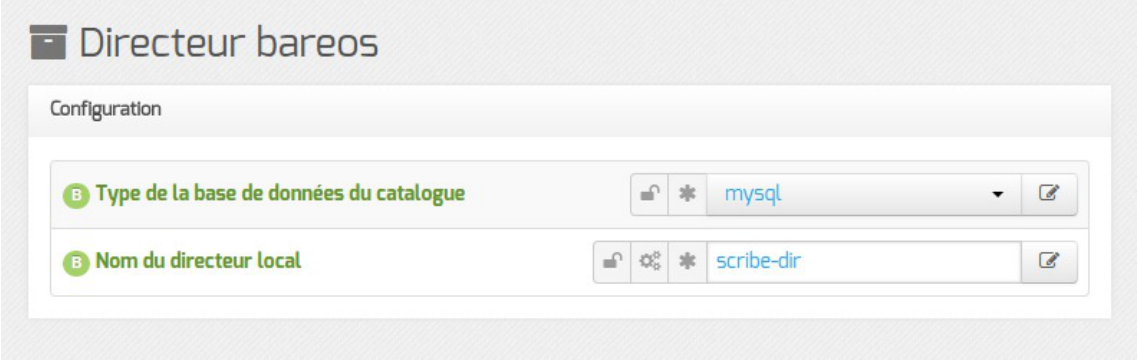
obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

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

Voir aussi...

Gestion des sources d'authentification multiples [p.288]

3.13. Onglet Directeur bareos



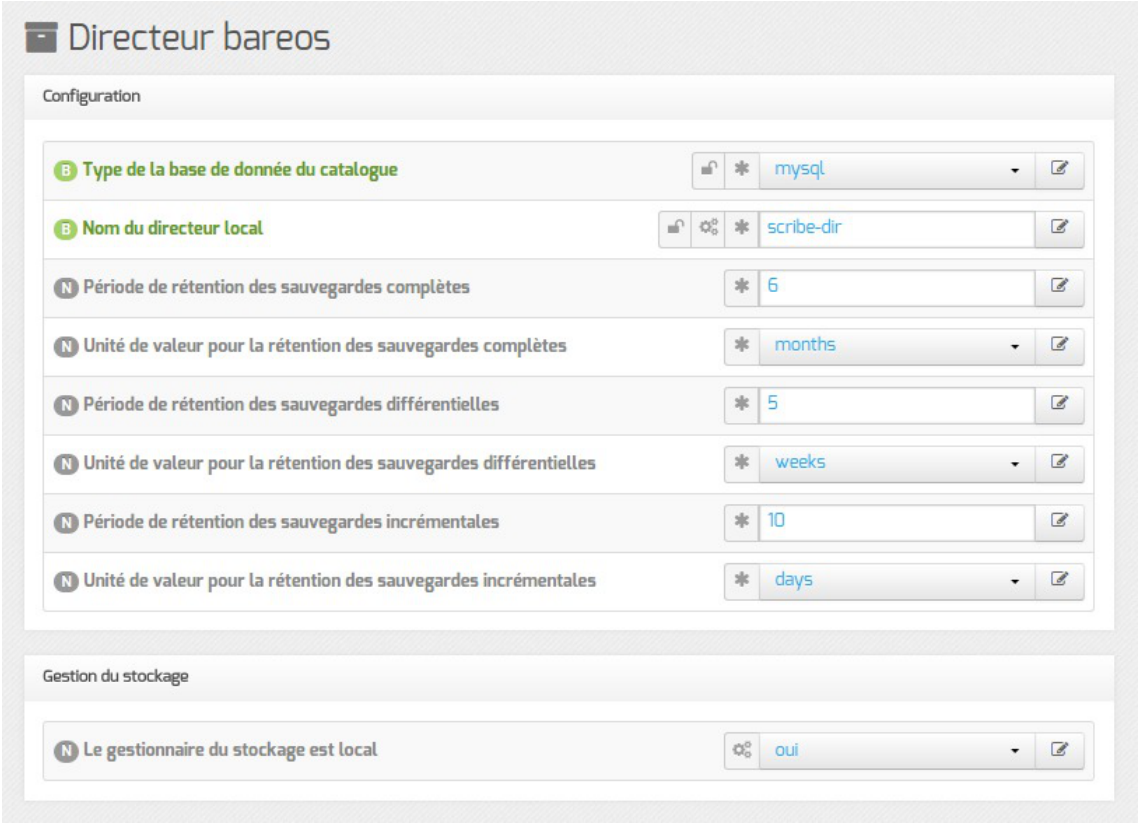
Le type de base de données permet de choisir si l'enregistrement du catalogue se fait dans MySQL ou dans SQLite. Il ne sera plus possible de modifier ce paramètre après l'enregistrement de la configuration.

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.759] 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.

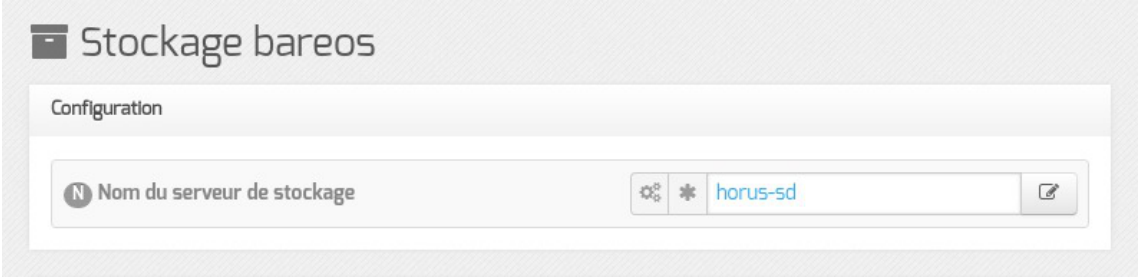
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

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)

3.14. Onglet Stockage bareos

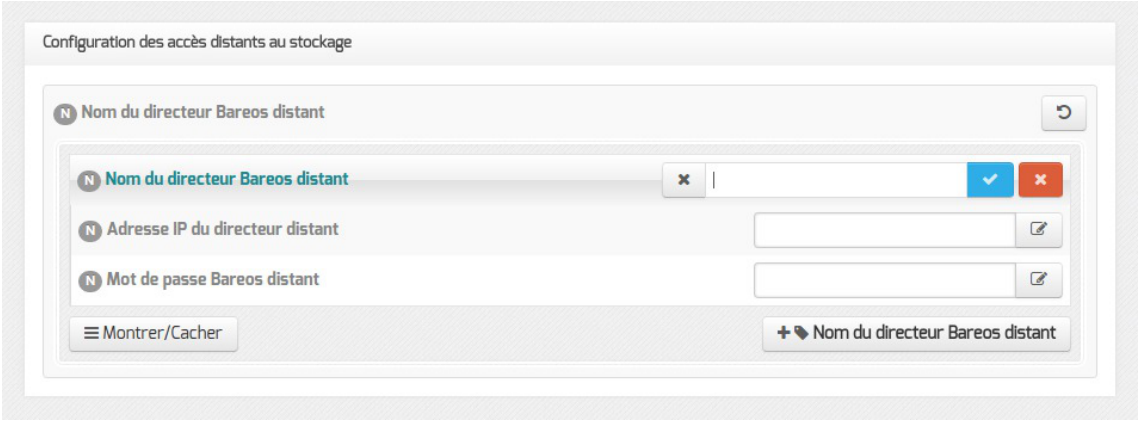
Dans l'onglet Stockage bareos il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



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.344]

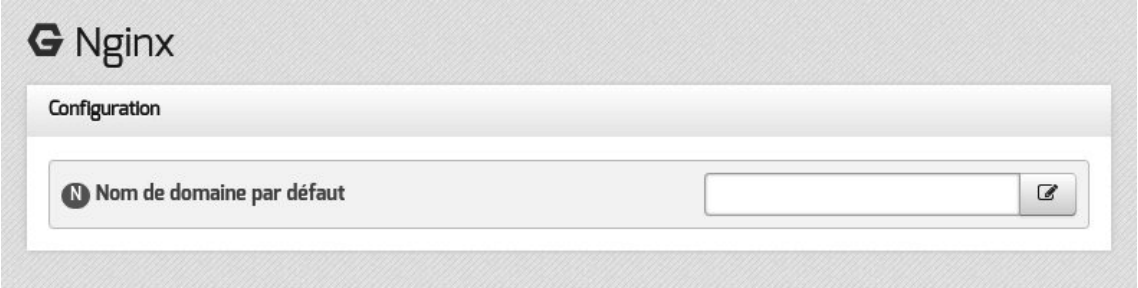
3.15. Onglet Nginx

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.

3.16. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.771].

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.758] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.779].

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.765]*/DNAT*.

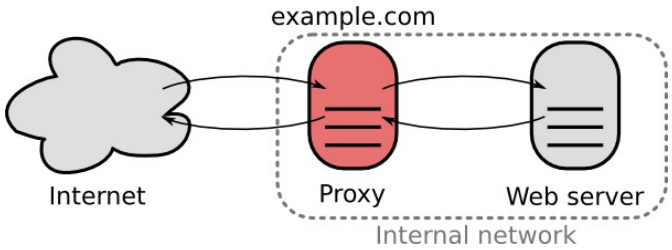
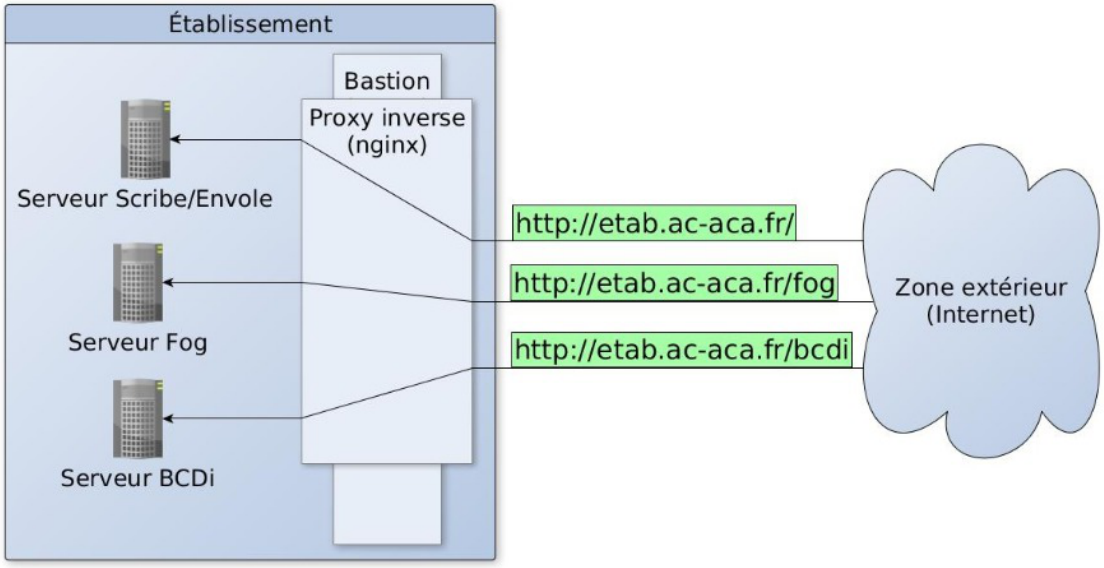


Diagramme d'un proxy inverse - Licence CC0

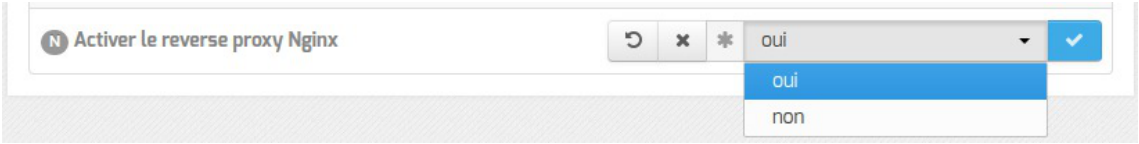
Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD[p.759] ;
- application EOP ;
- protocole HTTP[p.764] ;
- protocole HTTPS[p.764].

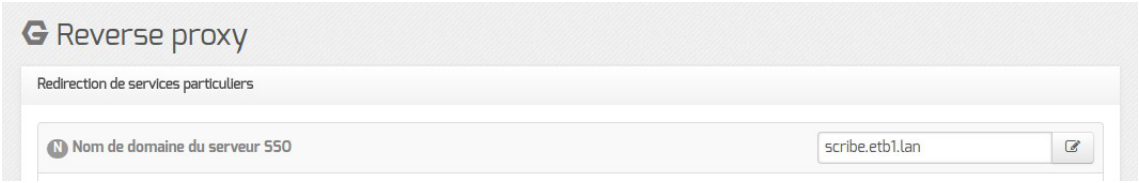
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

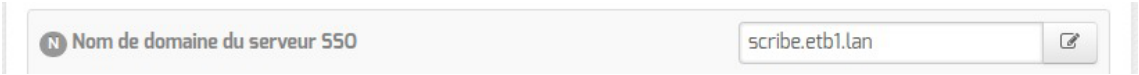


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

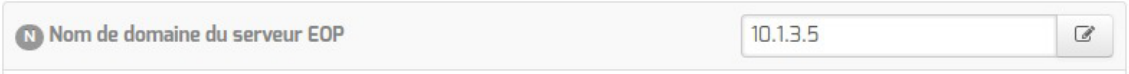
Redirection du service EoleSSO



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

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

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.783]).

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).

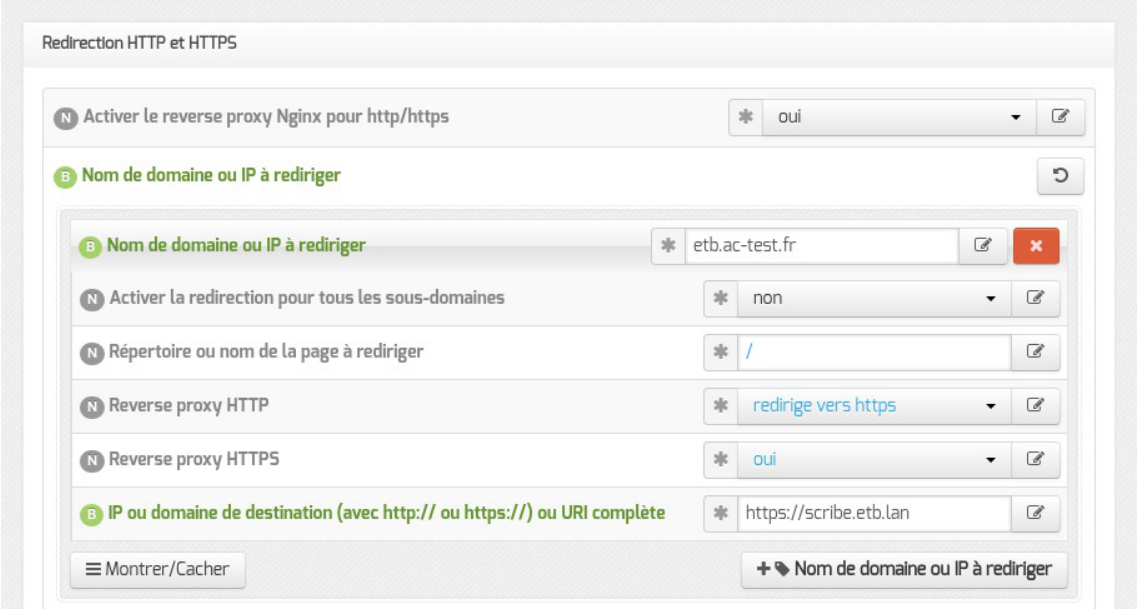
Redirection de l'interface d'administration EAD



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



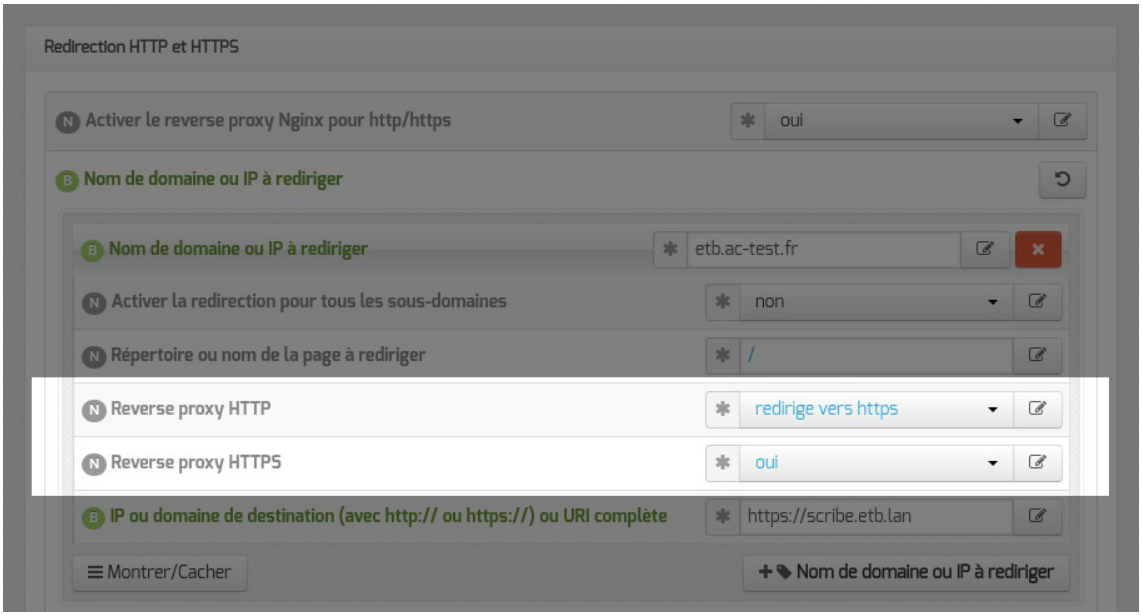
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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.783] (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.).

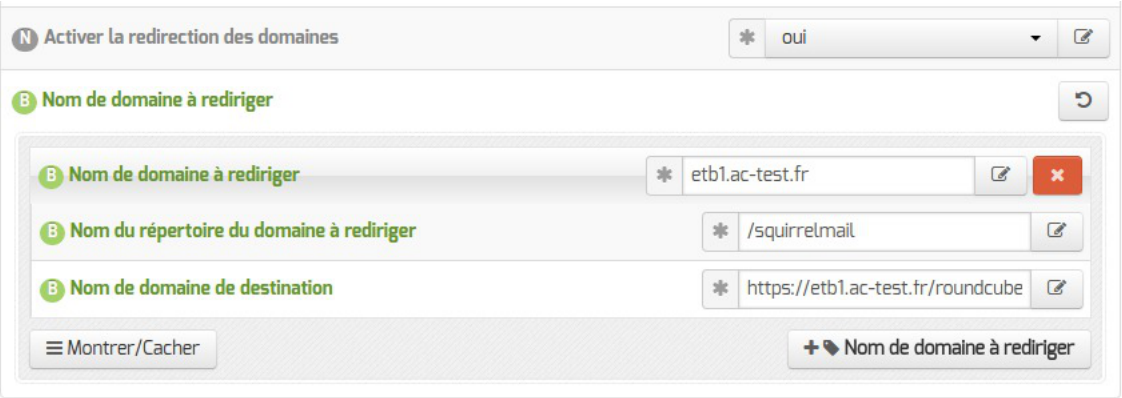
Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

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.775], `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/`.

3.17. Onglet Messagerie

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

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

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

Serveur d'envoi/réception (SMTP)



Les paramètres communs à renseigner sont les suivants :

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



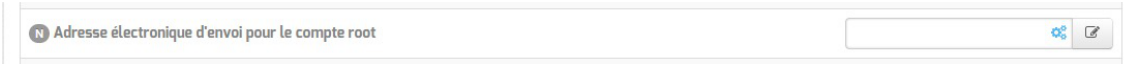
Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine

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

(onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

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

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



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

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

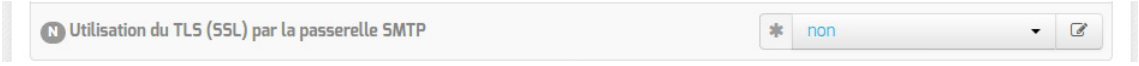
Relai des messages



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

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

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



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.781] pour l'envoi de message. Si la passerelle SMTP[p.778] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.779] (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.

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 Horus :

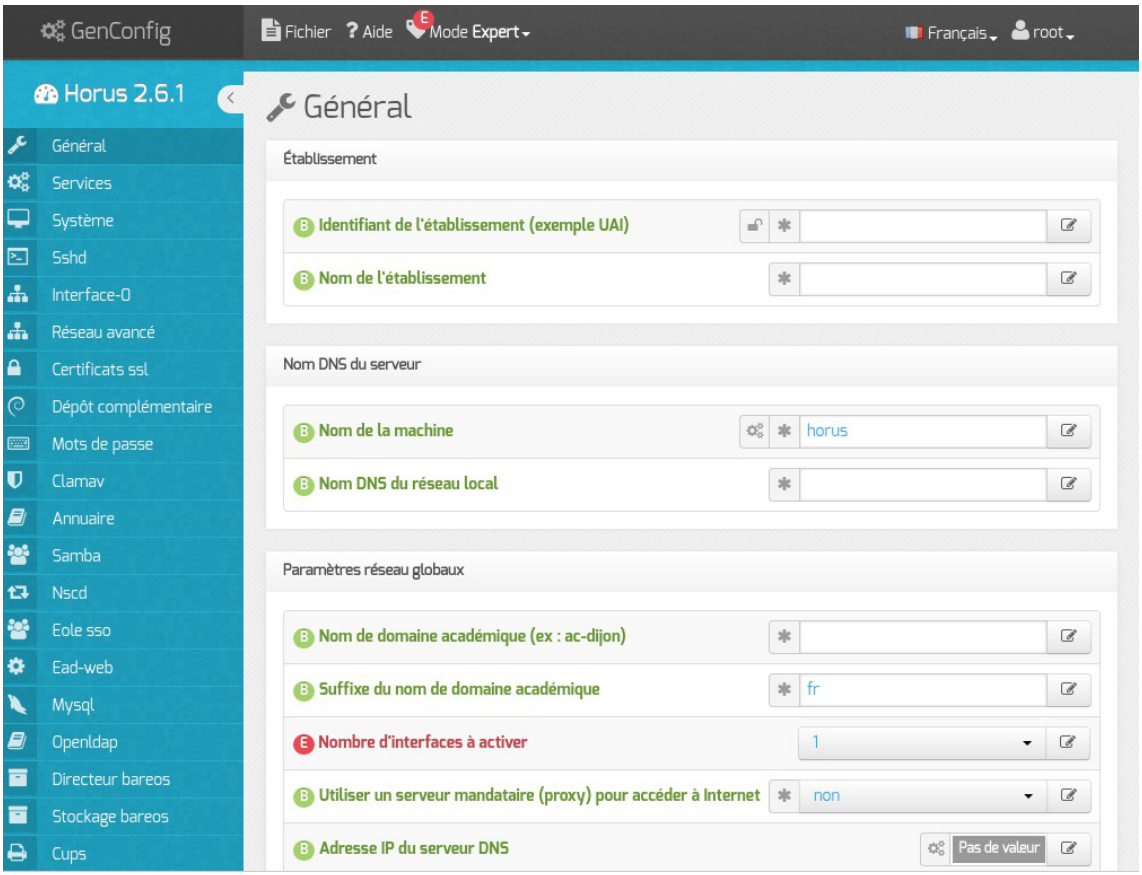
- Général ;
- Services ;
- Système ;
- Sshd ;
- Ntp ;
- Logs * ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-n (configuration de l'interface réseau) ;
- Réseau avancé ;
- Certificat ssl ;
- Dépôt tiers ;
- Eoledb ** ;
- Mots de passe ;
- Clamav (configuration de l'anti-virus) ;
- Annuaire ;
- Dhcp * ;
- Tftp * ;
- Esu * ;
- Samba ;
- Nscd ;
- Onduleur * ;
- Saltstack * ;
- Applications web * ;
- Apache * ;
- Eole sso ;
- Ead-web ;
- Mysql ;
- Openldap ;
- Directeur bareos ;
- Stockage bareos ;
- Cups ;
- Nginx ;
- Applications web nginx * ;
- Reverse proxy * ;

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

- Proftpd ;
- Messagerie ;
- Eoleflask.

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

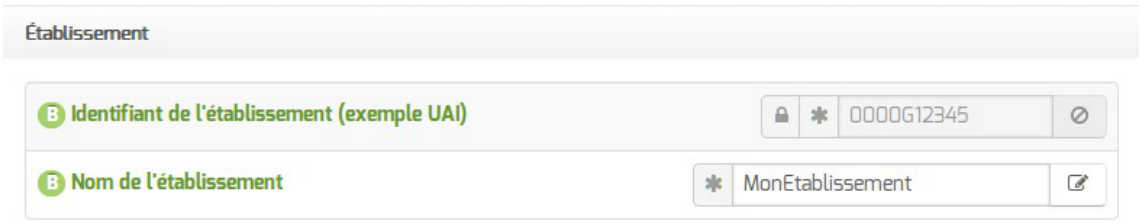
** Certains onglets ne sont disponibles qu'après installation manuelle d'un paquet.



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, ...

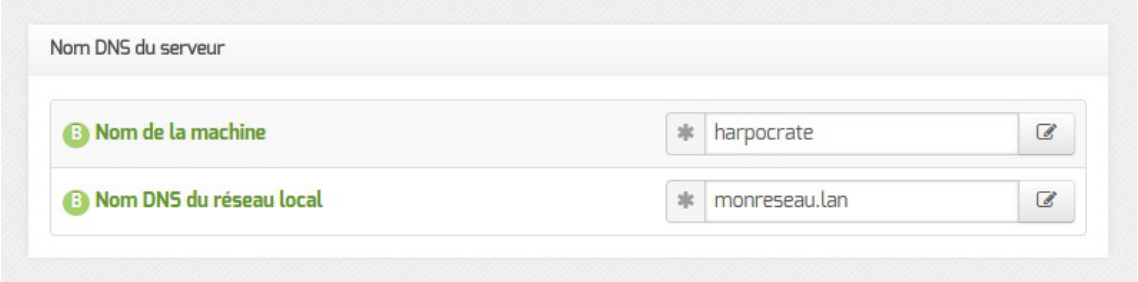
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sur les modules fournissant un annuaire LDAP[p.766] 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.

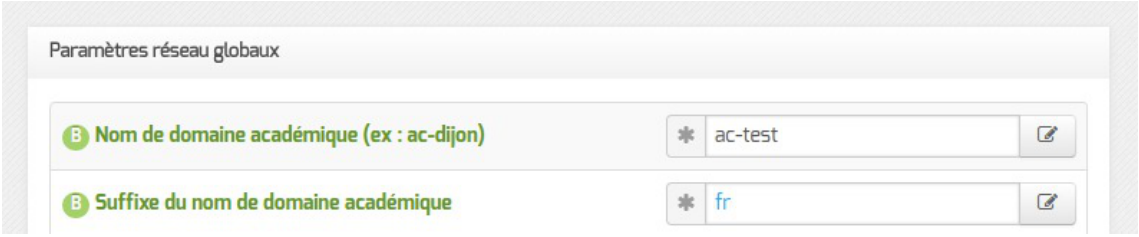
Les informations sur les noms de domaine sont importantes car elles sont notamment utilisées pour l'envoi des courriels et pour la création de l'arborescence de l'annuaire LDAP.



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)



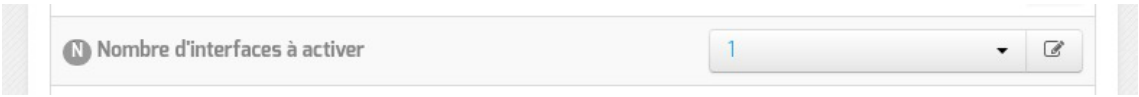
En deuxième lieu, il convient de configurer les noms de domaine de la machine.

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 :

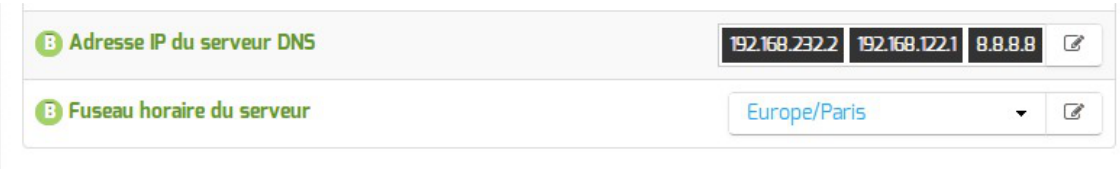
- nom de domaine ou adresse IP du serveur proxy ;
- le port du proxy.



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

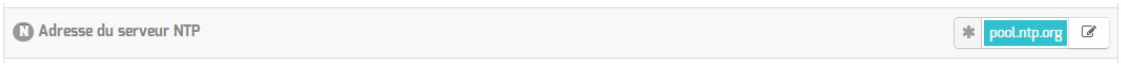
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.759].

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

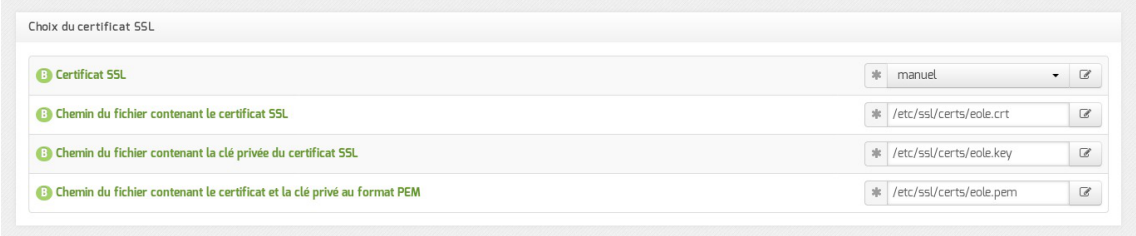
NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.771]. 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.



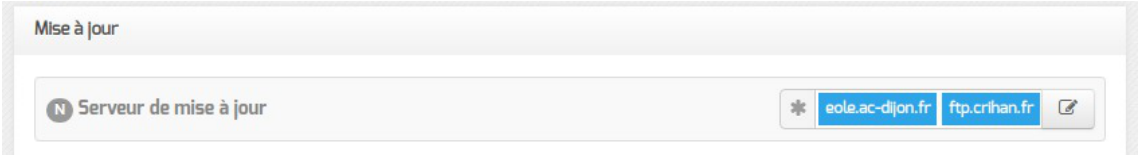
Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.781] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.753] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.767] ;
- `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...

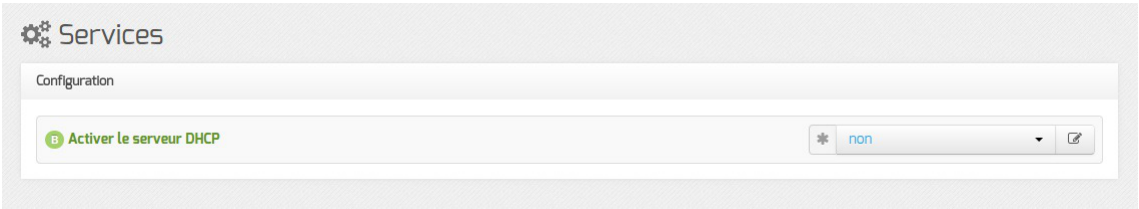
Les différents types de mises à jour [p.430]

4.2. Onglet Services

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

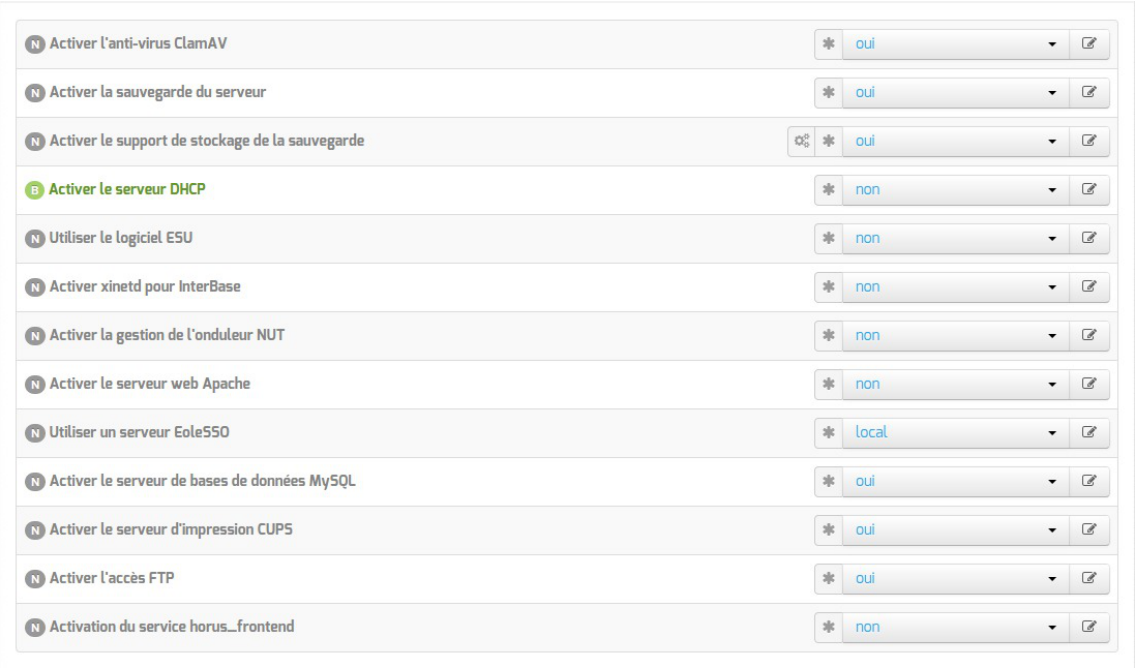
Suivant le module installé et le mode utilisé pour la configuration la liste des services activables ou désactivables est très différente.

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



En mode basique seul le service DHCP est activable.

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



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

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

- l'anti-virus ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le logiciel ESU[p.761] ;
- Interbase[p.765] ;
- le serveurs web ;
- l'authentification unique SSO[p.779] ;
- les bases de données MySQL ;
- le serveur d'impression avec CUPS ;
- l'accès FTP ;
- l'interface de gestion des utilisateurs Horus.

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

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

Le seul service propre au module Horus est le service PXE/TFTP, il est désactivé par défaut.

4.3. Onglet Système

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

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

Paramétrage de la console



- `Activer l'auto-complétion étendue sur la console` : l'auto-complétion facilite l'utilisation de la ligne de commande mais peut ralentir son affichage, elle est activée par défaut ;
- `Temps d'inactivité avant déconnexion bash` : si aucune activité n'est constatée sur la console utilisateur pendant cette durée (en secondes), sa session est automatiquement coupée, avec le message : `attente de données expirée : déconnexion automatique`. La valeur `0` permet de désactiver cette fonctionnalité.
- `Activer le reboot sur ctrl-alt-suppr` : si cette variable est passée à `non`, la séquence ctrl - alt - suppr est désactivée.
- `Nuance du fond d'écran dans VIM` : l'éditeur VIM peut utiliser différents thèmes pour la coloration syntaxique et adapter ceux-ci en fonction de la valeur de la couleur d'arrière-plan pour en améliorer la lisibilité. La variable prend une valeur parmi dark et light, permettant d'adapter la coloration syntaxique à un arrière-plan sombre et clair respectivement.

Optimisations système



- `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.so` et `pam unix.so`.

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

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

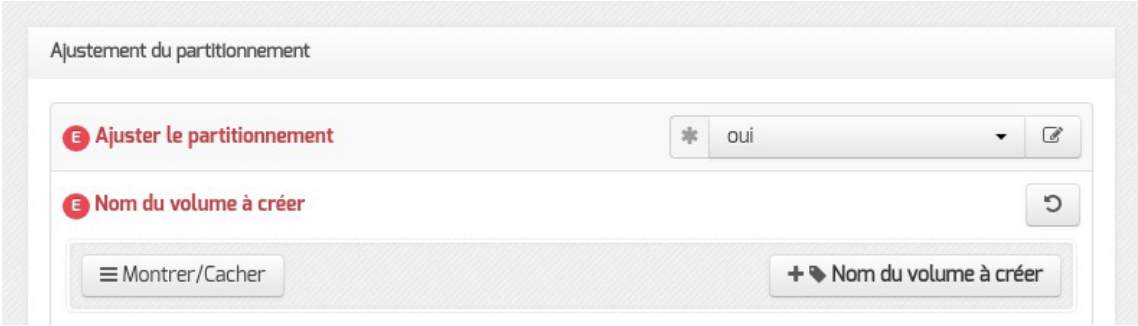
```
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-10-05 18:37:11 +0200
  LV Status              available
  # open                 1
  LV Size                8,94 GiB
  Current LE             2288
  Segments               1
  Allocation             inherit
  Read ahead sectors     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`.

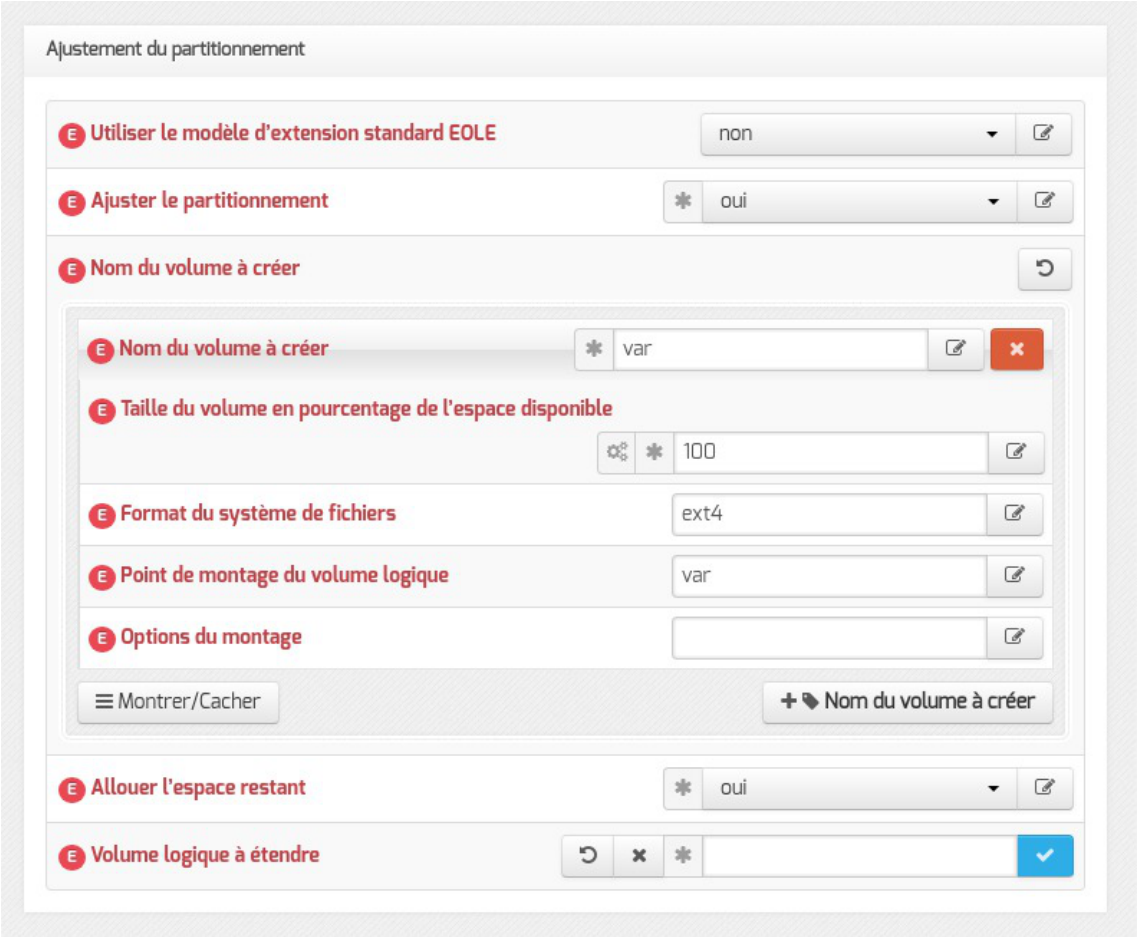


Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

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).

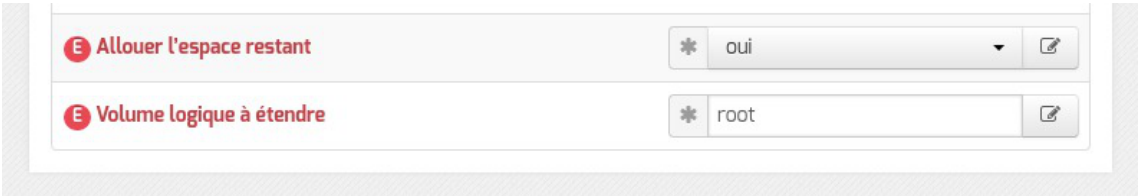
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



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.344]

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`).

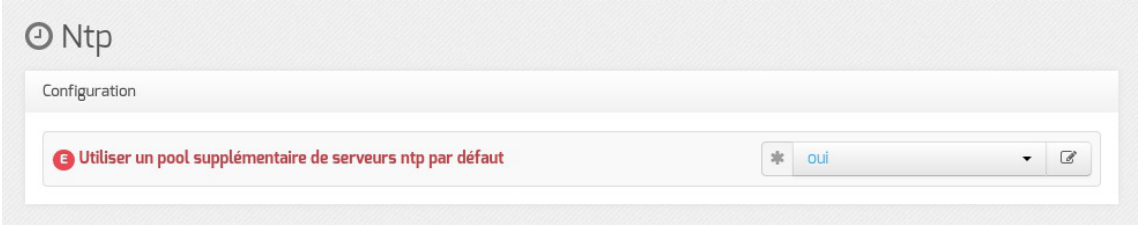
Par défaut, les groupes Unix autorisés sont `root` et `adm`.

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`).

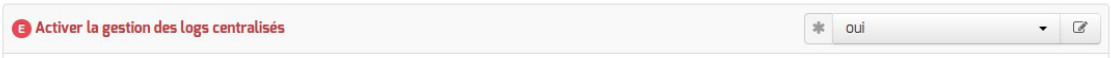
Par défaut, l'utilisation du pool est activée.

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

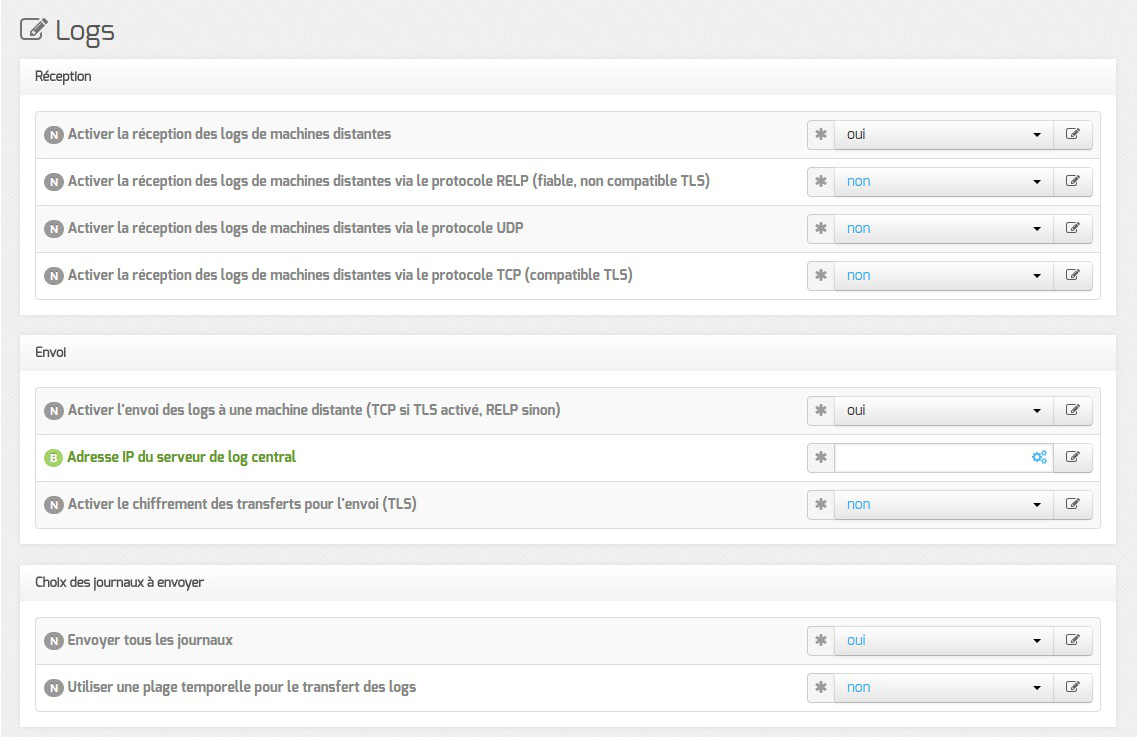
La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.785]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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)



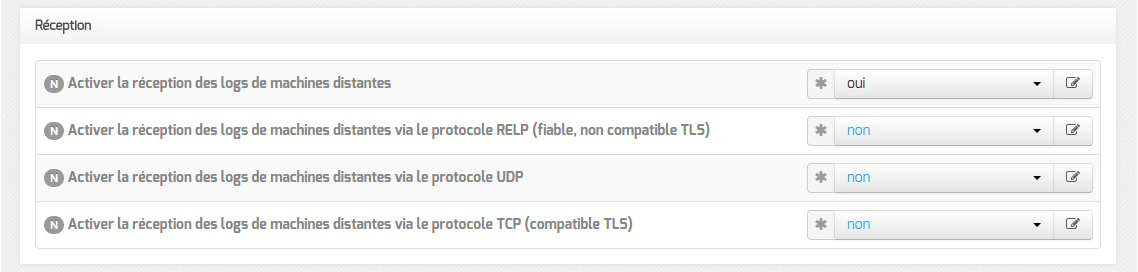
Vue de l'onglet Logs

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.780] ou RELP[p.776]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.781]) ;
- 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.753].

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.

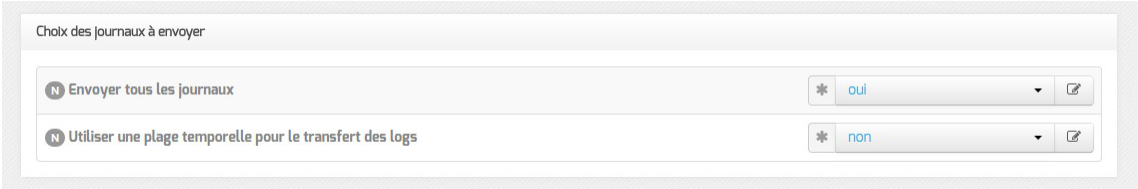


Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).

Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.753].

Choix des journaux à envoyer

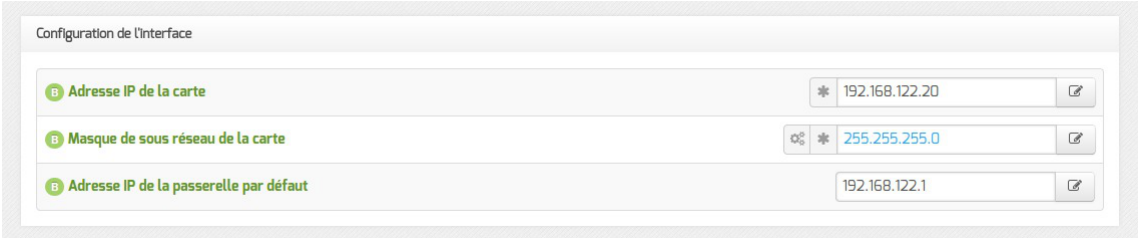
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



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

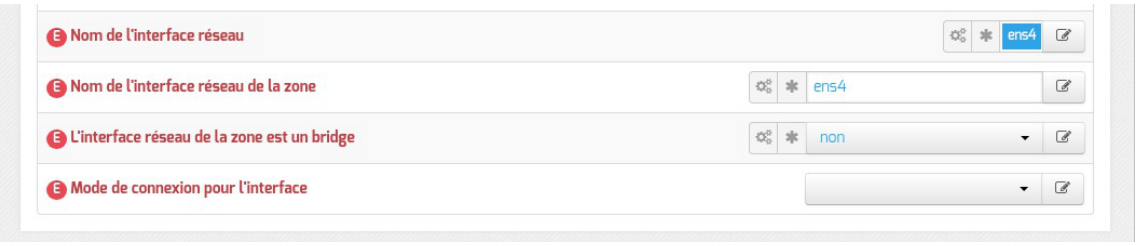
Configuration de l'interface



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)

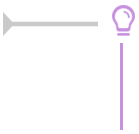


Nom de l'interface réseau

À partir de la version EOLE 2.6, afin de respecter la convention Consistent Network Device Naming[p.755], 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.752] 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.752].

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.

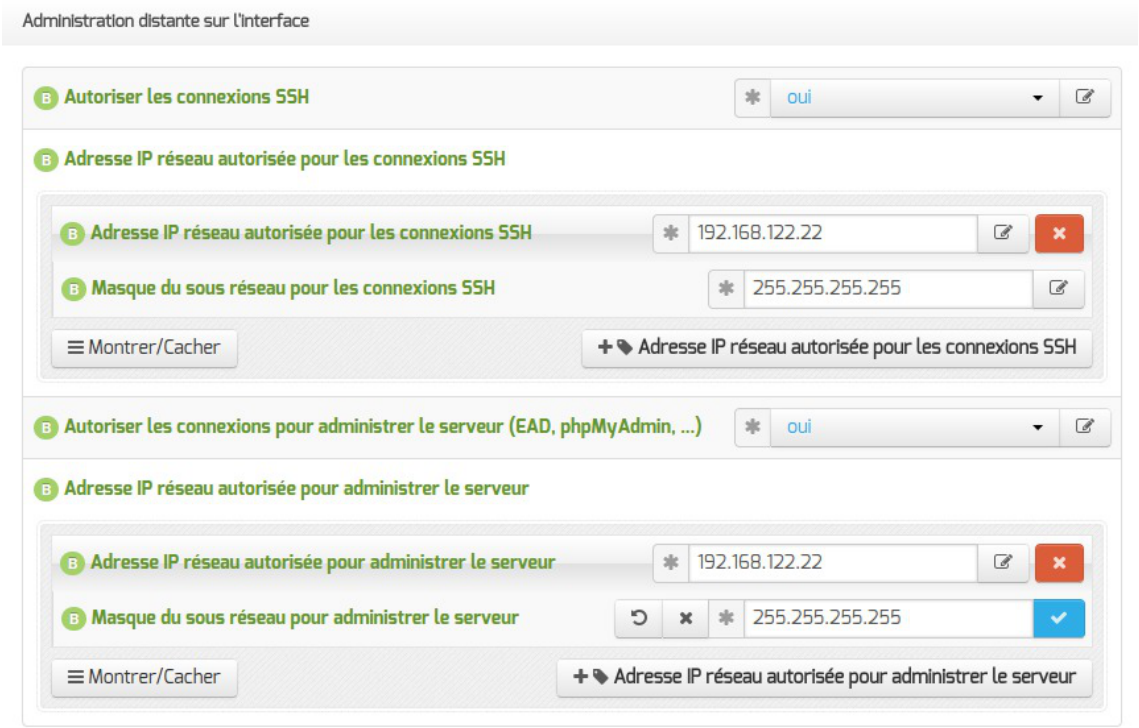
Liste des valeurs possibles :

- `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



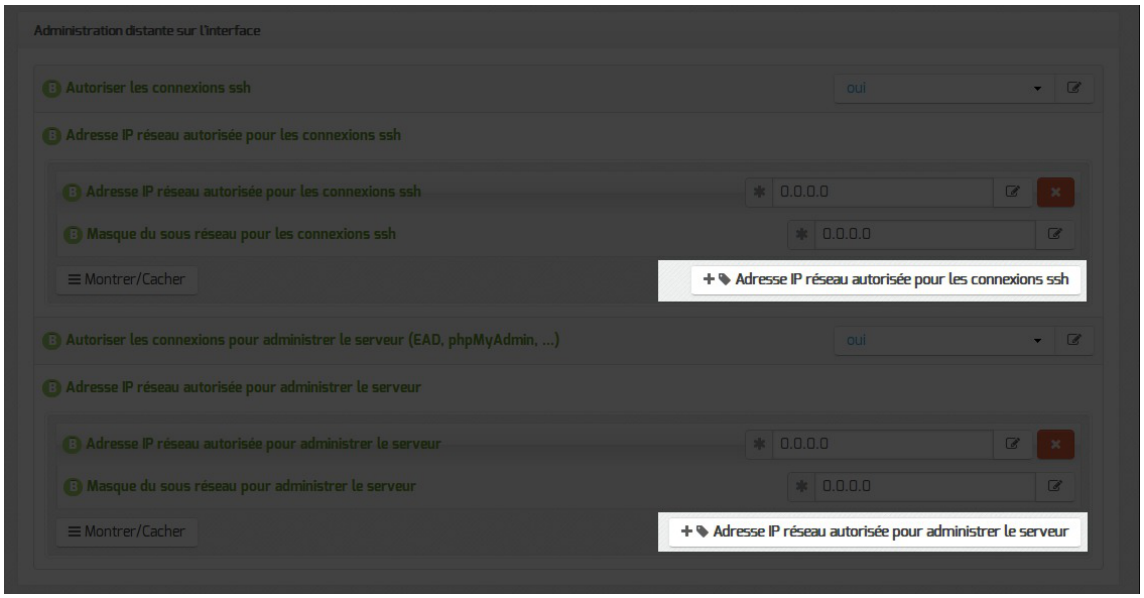
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.779] 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.

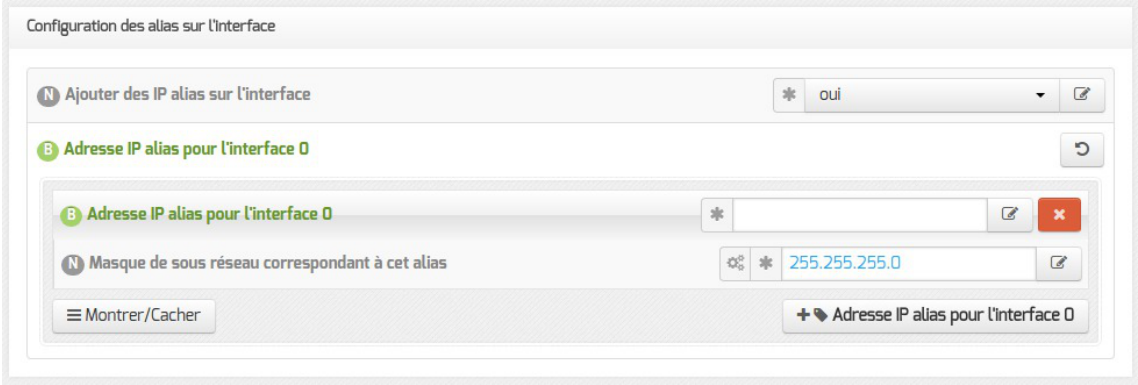
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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)

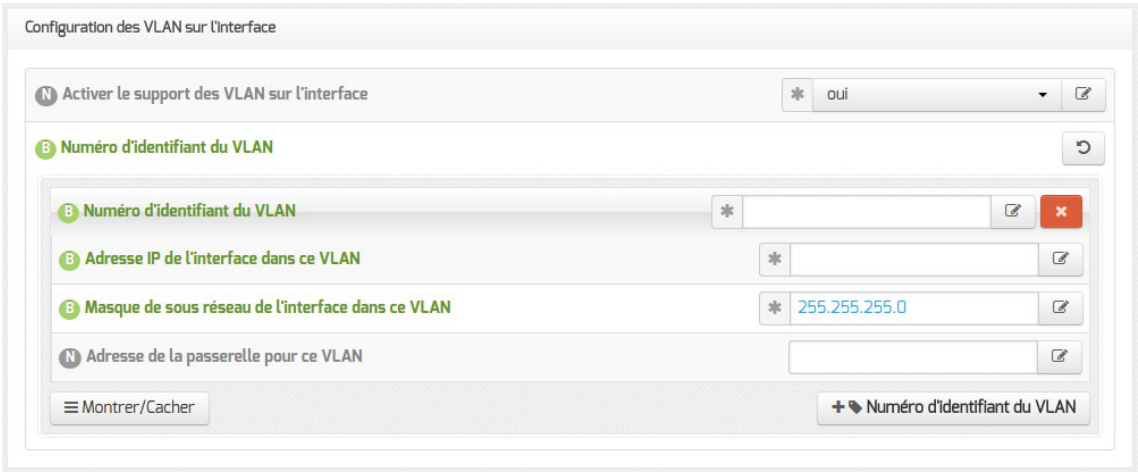


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

> 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.783] (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 :

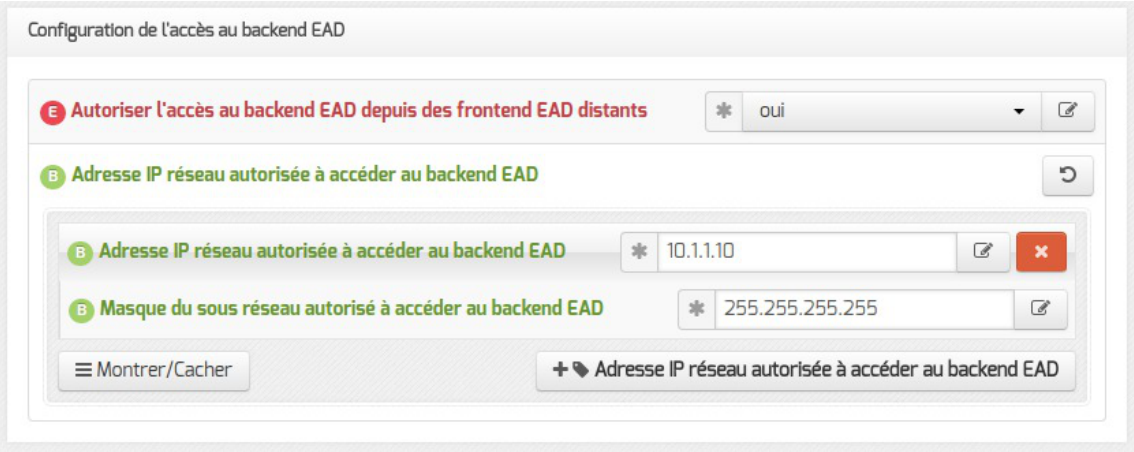
- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

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.759] 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.340]

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.

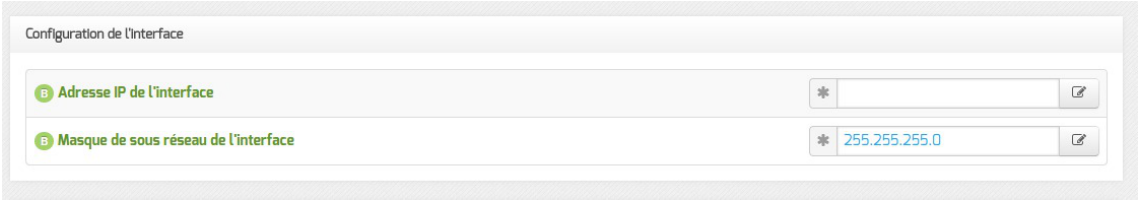


Cela ajoute autant d'onglet `Interface-n` que le nombre d'interfaces à activer choisi.

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

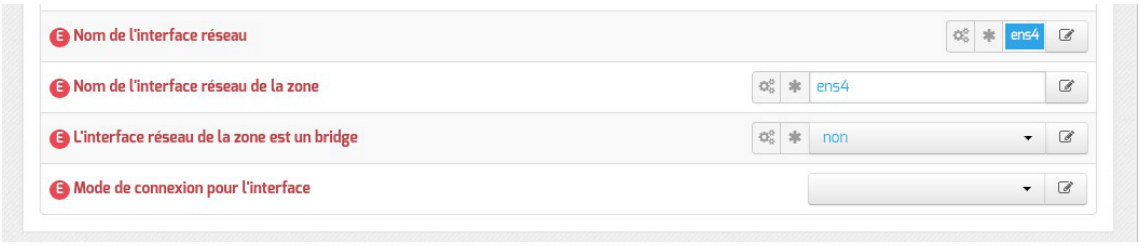
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.755], 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.752] 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.752].

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 :

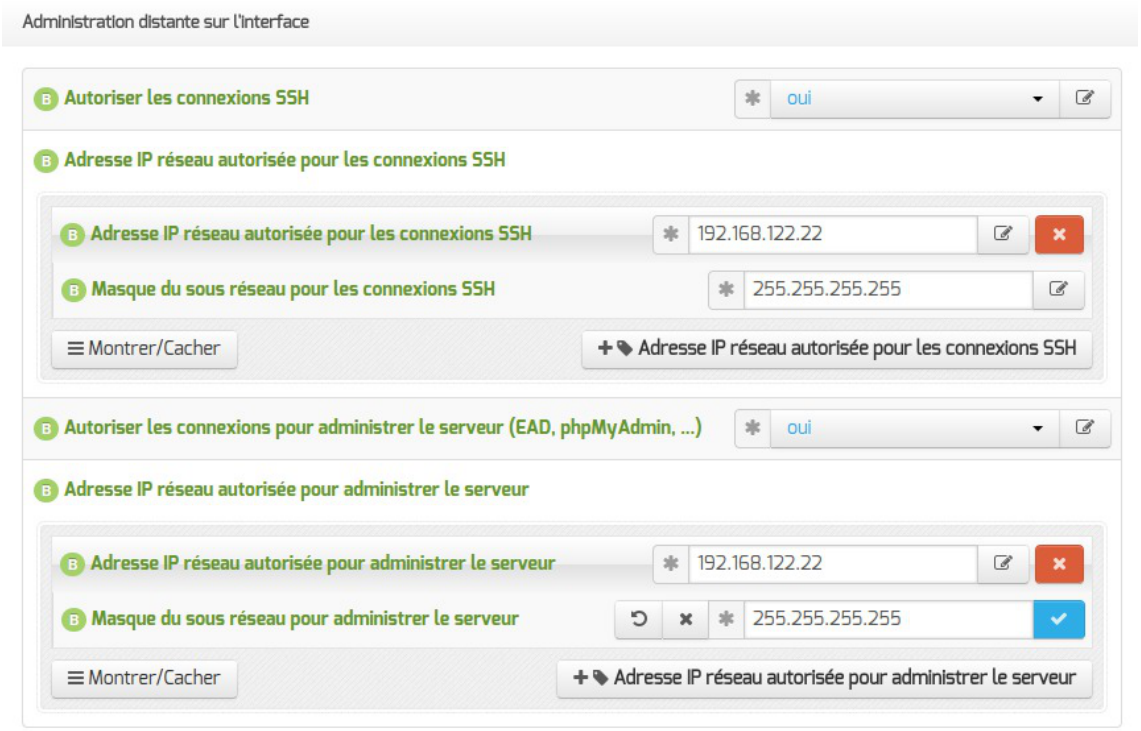
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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

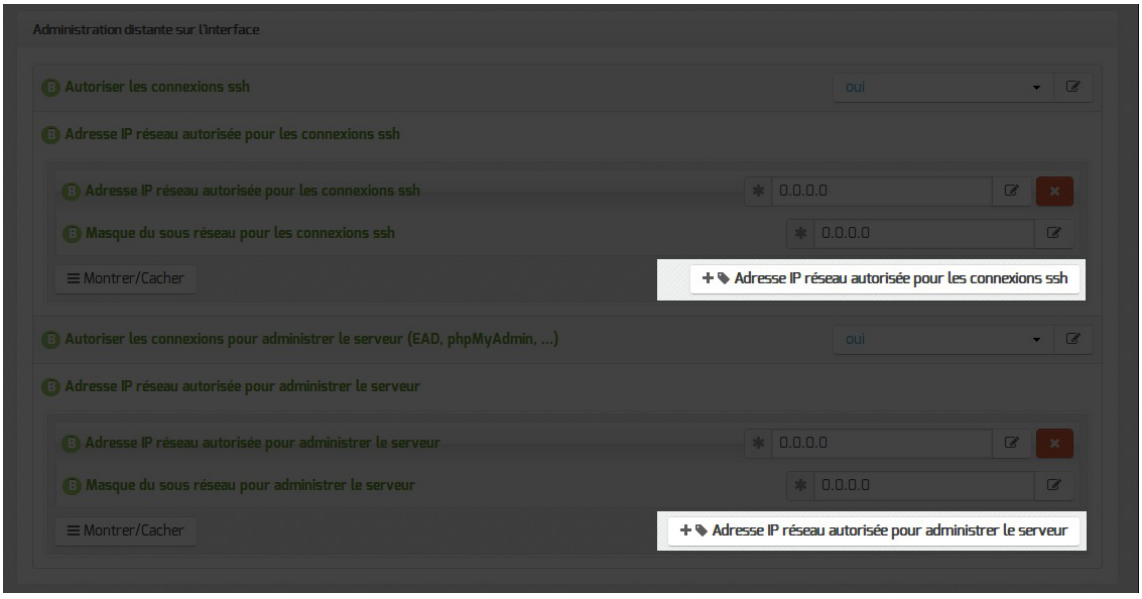


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.779] 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)

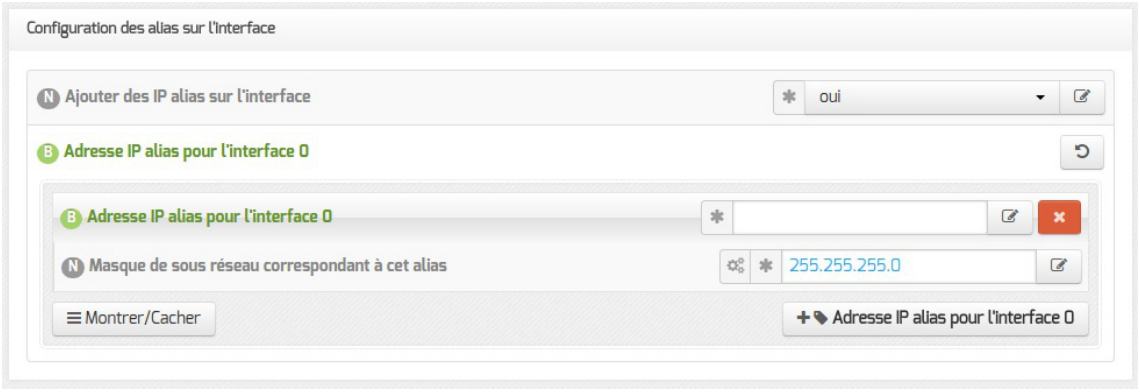
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

> 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.

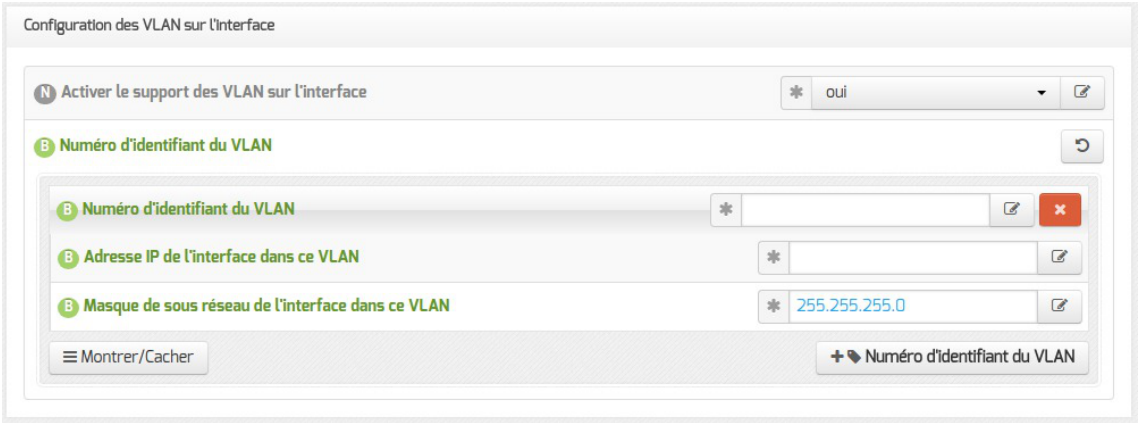


Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

> 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.783] (réseau local virtuel) sur une interface déterminée du module.



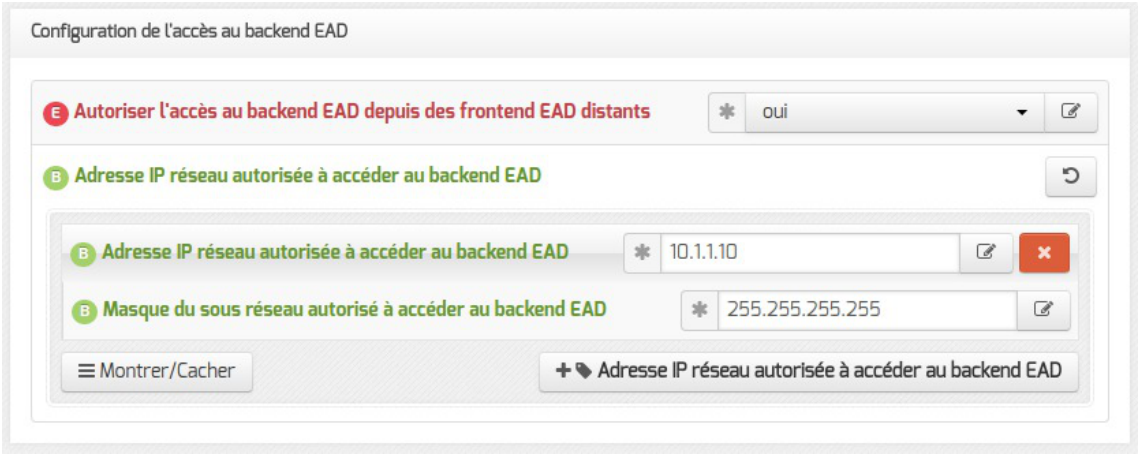
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.759] 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...

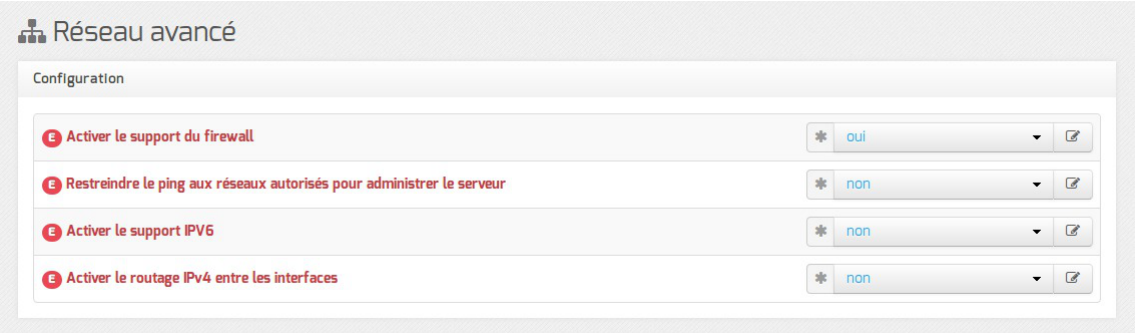
Mise en place de l'agrégation de liens Ethernet (bonding) [p.340]

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.765] 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`).

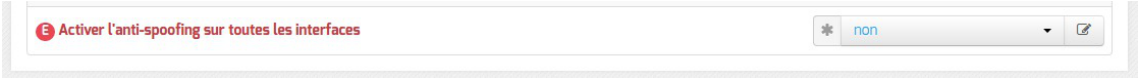
Sécurité



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)

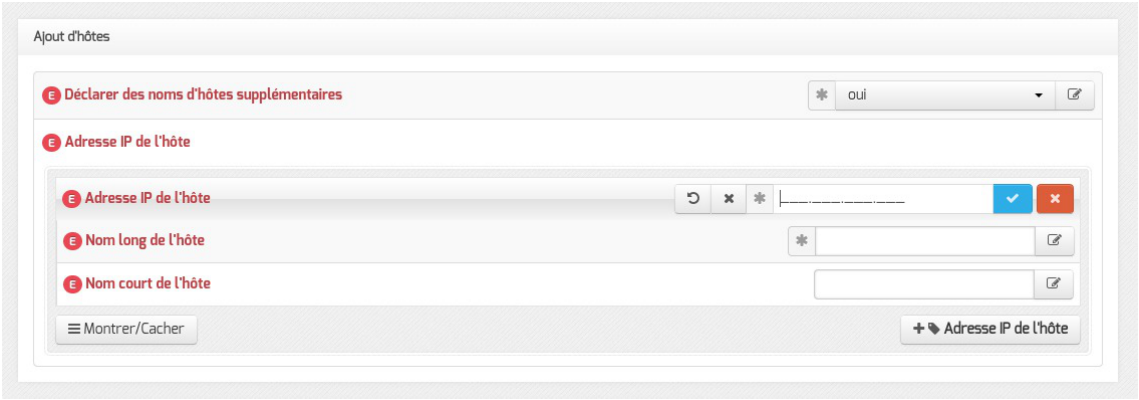
utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.753] 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`.

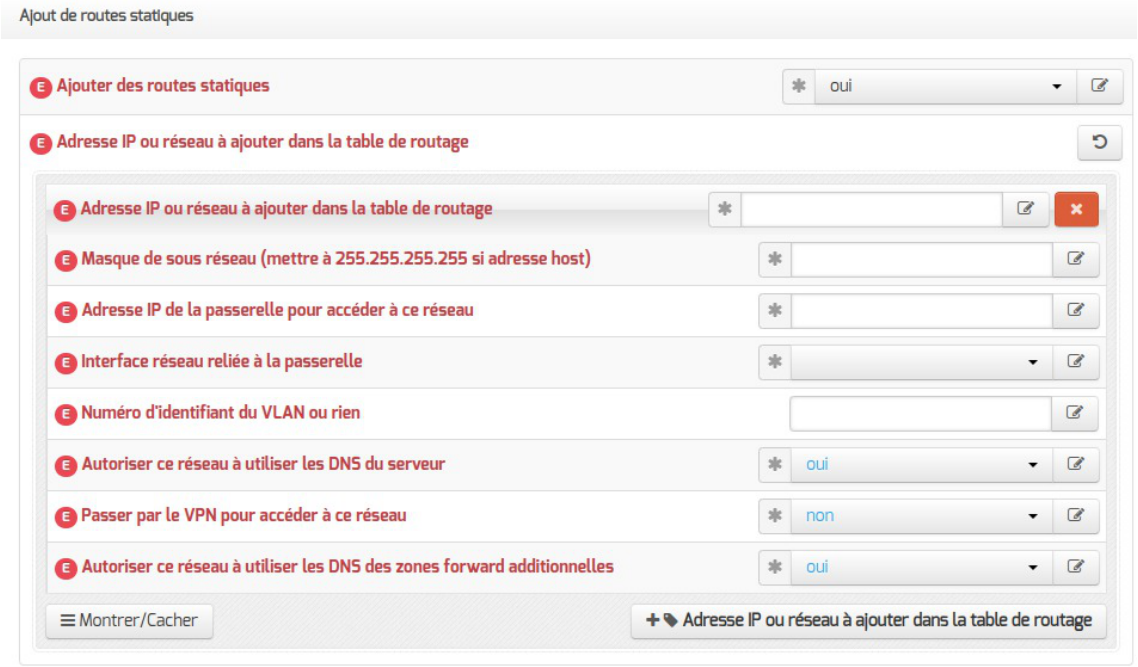
Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte` .

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.754] 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 :

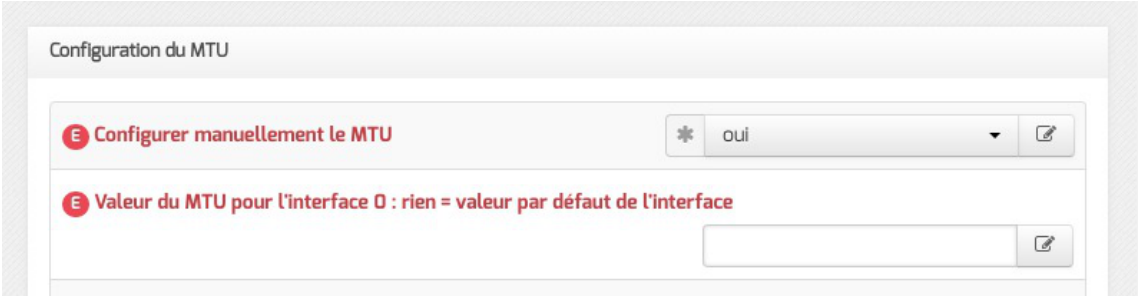
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

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.770] (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.764] 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.770] 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).

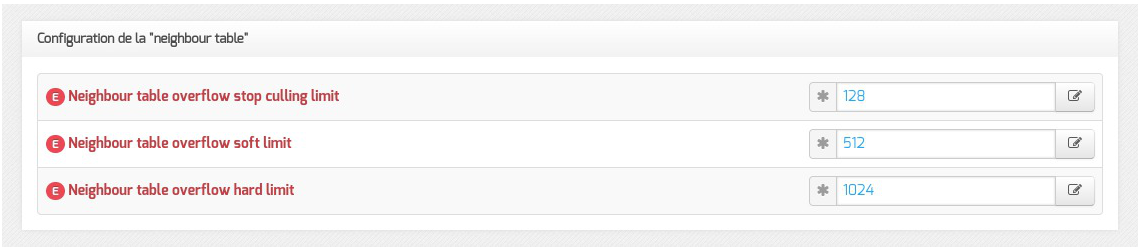
Si l'interface externe est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le champ : `Valeur du MTU pour l'interface 0`.



Si l'interface externe d'un module Amon ou AmonEcole est de type PPPoE[p.775] 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"

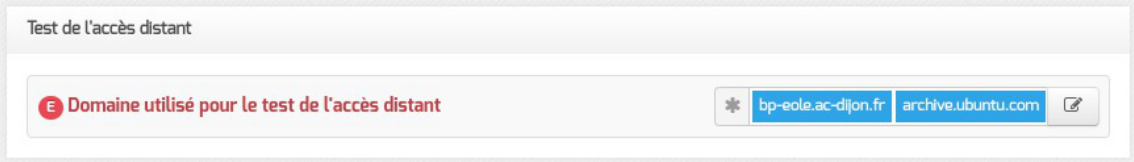


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

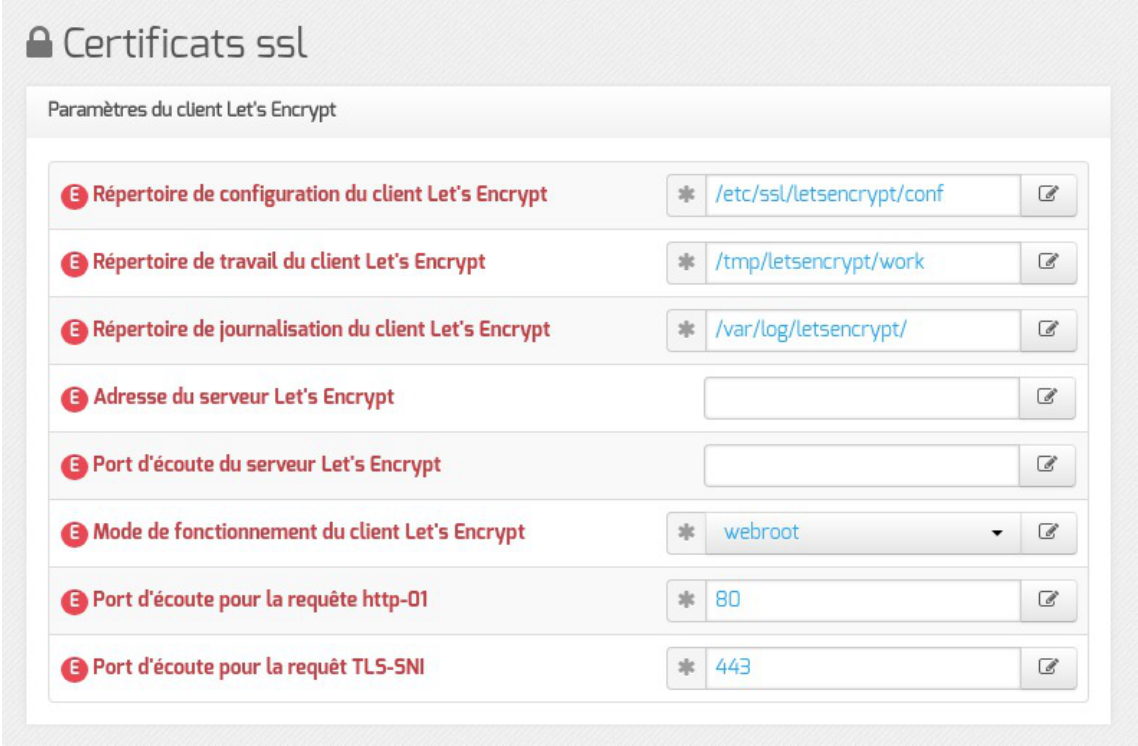
Vous pouvez à présent gérer des certificats Let's Encrypt pour des serveurs accessibles depuis Internet ou au travers d'un proxy inverse.

Serveurs accessibles depuis Internet ou au travers d'un proxy inverse

L'utilisation de certificats Let's Encrypt requiert l'utilisation de noms DNS connus d'Internet.

Le certificat sera fait au nom résultant de la concaténation du nom de la machine et du nom de DNS local.

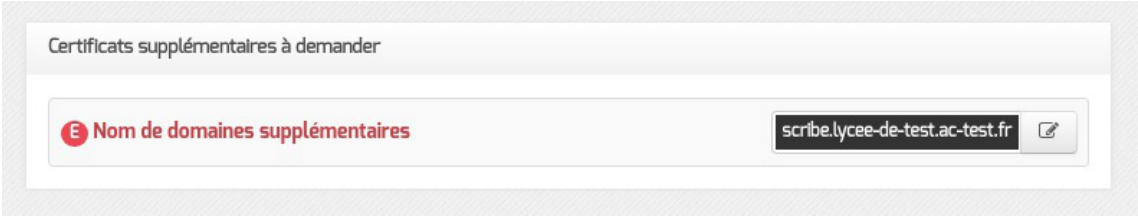
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Seule la variable `Mode de fonctionnement du client Let's Encrypt` nécessite un paramétrage en fonction de l'accessibilité du serveur :

- accessible depuis Internet → utiliser la valeur `standalone` ;
- accessible au travers d'un proxy inverse → utiliser la valeur `webroot`.

Nom DNS supplémentaires



Il est possible de faire des requêtes supplémentaires pour d'autres noms DNS connus d'Internet en renseignant la variable `Nom de domaines supplémentaires`.

> Il y aura autant de certificats supplémentaires que de noms DNS déclarés dans la variable `Nom de domaines supplémentaires`.

Certificat de type autosigné et manuel

Certificats par défaut

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

- `/etc/ssl/certs/ca_local.crt` : autorité de certification propre au serveur (certificats auto-signés) ;
- `/etc/ssl/private/ca.key` : clef privée de la CA ci-dessus ;

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

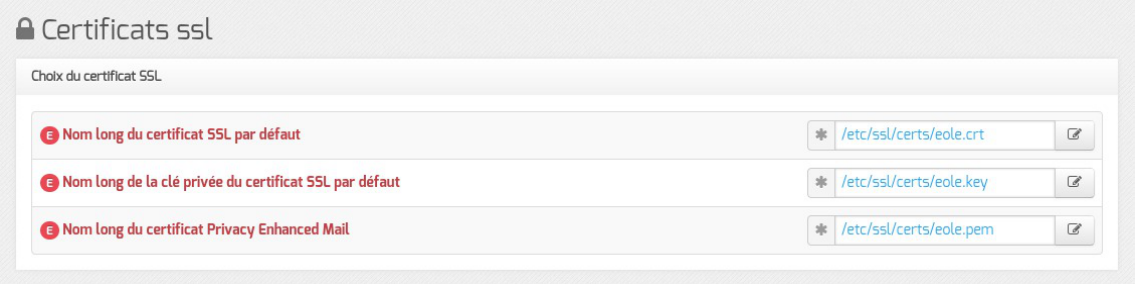
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un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

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

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

Mise en place d'un certificat particulier

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



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

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

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

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

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

Sur un module dont la version est supérieure ou égale à 2.6.2, la configuration des chemins est proposée dans l'onglet `Général`.

Le répertoire `/etc/ssl/local_ca/` accueille uniquement des certificats CA.

Paramètres SSL

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

Les variables de la section `Paramètres SSL` permettent de personnaliser la configuration OpenSSL[p.773] 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.758]) 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.782] 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.755] 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.759] 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`

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

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...

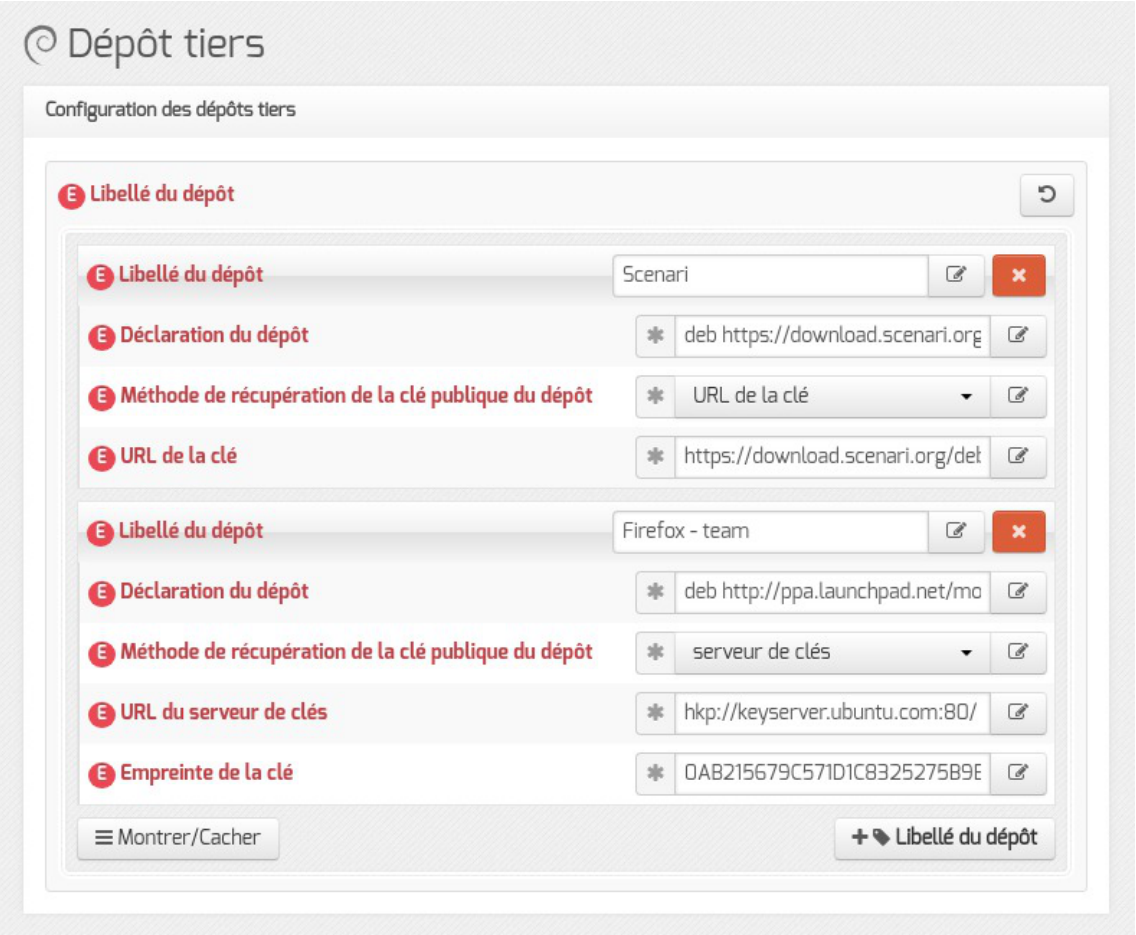
Intégration d'un certificat et d'une chaîne d'authentification

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 Eoledb : Gestion des bases de données

EoleDB est disponible depuis la version 2.5.2 d'EOLE. C'est une re-implémentation de l'ancien gestionnaire des bases de données EOLE (eole-sql) dont les objectifs principaux sont :

- n'utiliser qu'un seul fichier de configuration ;
- supporter nativement plusieurs types de bases de données (MySQL, PostgreSQL, SQLite, ...) ;
- supporter nativement l'externalisation des bases de données sur d'autres serveurs ;
- ne plus avoir à fournir des scripts python dans les paquets d'application web du projet EOLE pour pouvoir générer ou mettre à jour des bases de données (cf eole-sql : `/usr/share/eole/applications/gen/` , `/usr/share/eole/applications/passwords/` , `/usr/share/eole/applications/updates/`).

EoleDB rend possible l'externalisation des bases de données d'un module EOLE.



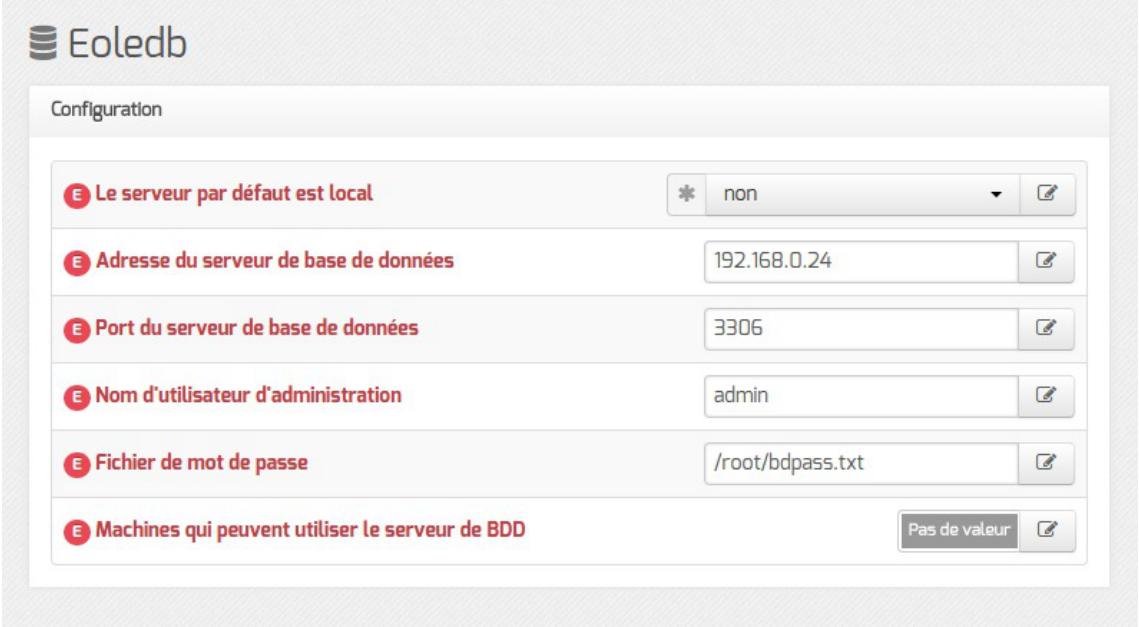
Pour le moment, la version publiée d'EoleDB gère uniquement les bases de données MySQL et PostgreSQL.

Cet onglet est disponible en mode expert après l'installation manuelle du paquet `eole-db` :

```
# apt-eole install eole-db
```

Par défaut le serveur est paramétré comme étant local. Dans le cas où le serveur est distant quelques variables sont à renseigner.

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



- `Adresse du serveur de base de données` : adresse IP, nom de machine ou nom de domaine du serveur de base de données distant. Cette valeur est utilisée pour toutes les applications web qui ne définiront pas elles-mêmes un serveur de base de données.
- `Port du serveur de base de données` : port du serveur de base de données utilisé, par exemple `3306` pour le serveur MySQL fourni par EOLE.
- `Nom d'utilisateur d'administration` : identifiant du gestionnaire de la base de données distante.
- `Fichier de mot de passe` : chemin d'accès vers le fichier qui contient le mot de passe du gestionnaire, par exemple `/root/bdpass.txt`. Ce fichier doit être accessible par EoleDB, idéalement le fichier doit avoir les droits 600.
- `Machines qui peuvent utiliser le serveur de BDD` : permet d'autoriser des machines à accéder à l'administration des bases distantes #fixme [https://dev-eole.ac-dijon.fr/issues/15456] , si rien n'est renseigné l'adresse IP du serveur utilisant EoleDB est ajoutée automatiquement dans le fichier de configuration.

Voir aussi...

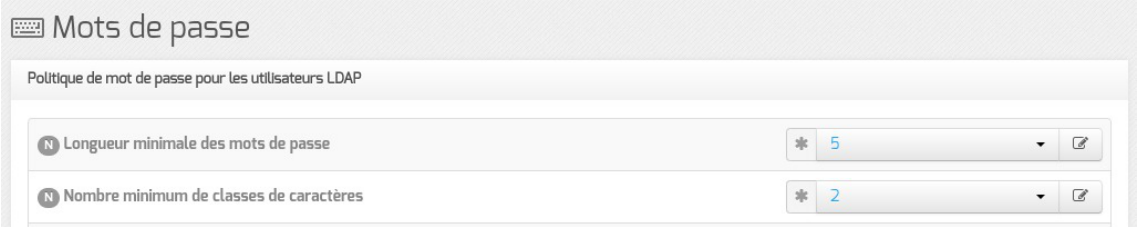
Gestion des bases de données avec EoleDB [p.330]

Externalisation des bases de données MySQL avec EoleDB

4.13. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs

Cet onglet permet de modifier la politique des mots de passe des utilisateurs LDAP et Samba.

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



Longueur minimale des mots de passe

Cette variable permet de définir la longueur minimale requise pour un mot de passe lors de son changement par l'utilisateur dans sa session Windows (ctrl+alt+suppr).

Cette contrainte s'applique également à toutes les interfaces EOLE permettant de changer des mots de passe (EAD, EOP, EOE, ...).

La longueur minimale est paramétrable de 3 à 12 caractères.

Nombre minimum de classes de caractères

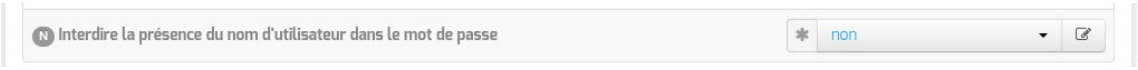
Cette variable permet de choisir le nombre minimum de classes de caractères[p.755] imposées pour le mot de passe d'un compte utilisateur.

Il est possible d'imposer l'utilisation de 1 à 4 classes différentes parmi :

- caractères minuscules ;
- caractères majuscules ;
- caractères numériques ;
- autres caractères (spéciaux et accentués).

Attention, un mot de passe sécurisé doit avoir une longueur de 8 caractères et doit contenir au minimum 3 classes différentes de caractères.

À partir de la version EOLE 2.6.2, une nouvelle contrainte est disponible pour permettre forcer l'utilisation d'un mot de passe plus fort.



Interdire la présence du nom d'utilisateur dans le mot de passe

La présence du nom d'utilisateur dans le mot de passe affaiblit le mot de passe en permettant qu'une partie des caractères utilisés pour le mot de passe soient prévisibles.

Interdire la présence du nom d'utilisateur dans le mot de passe permet de rejeter un mot de passe lors de son changement si celui-ci contient le nom de l'utilisateur concerné.

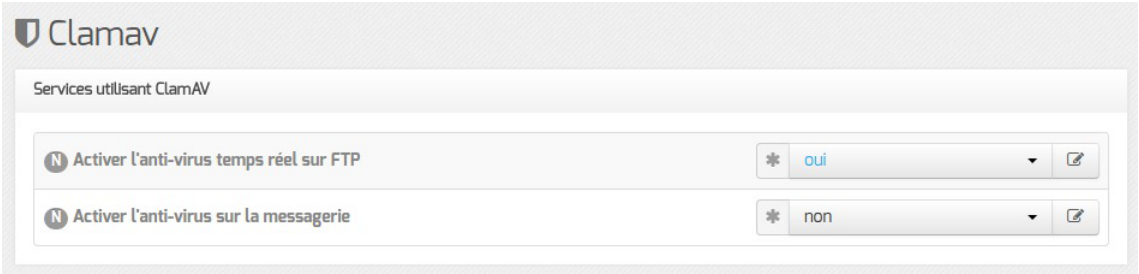
Dans le cadre de l'utilisation d'un serveur Active Directory distant, la politique de sécurité définie dans l'onglet Mots de passe doit être en accord avec celle du serveur AD.

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

4.14. 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 uniquement sur le service FTP.
Sur le module Horus il est possible d'activer l'anti-virus sur :

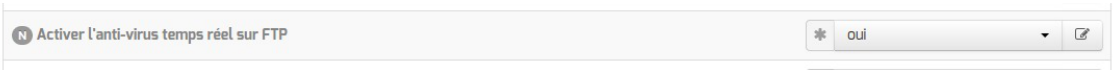
- le service SMB ;
- le service de messagerie.



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.

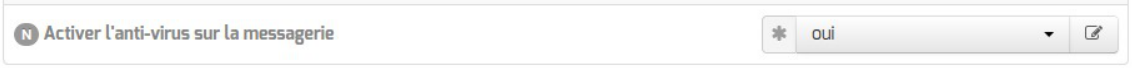
Activation de l'anti-virus sur FTP

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

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

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

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)` ;
- `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.760] ;
- `Scan du contenu des fichiers PDF` ;
- `Scan des fichiers courriels` ;
- `Détection des fichiers exécutables corrompus`.

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

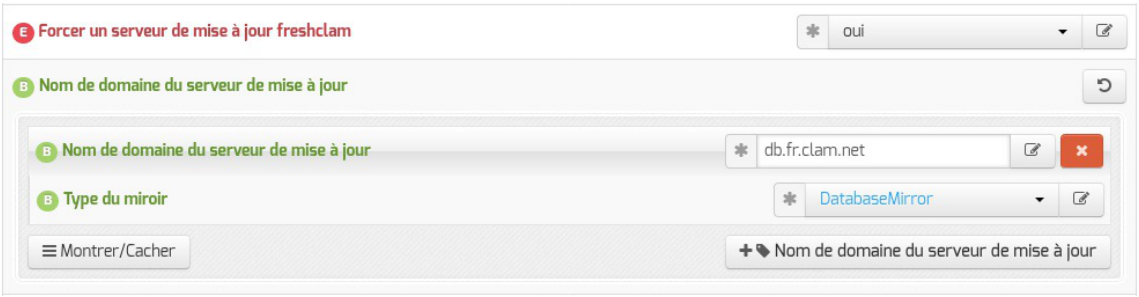
Configuration avancée du service de mise à jour de l'anti-virus

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.



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

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

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).

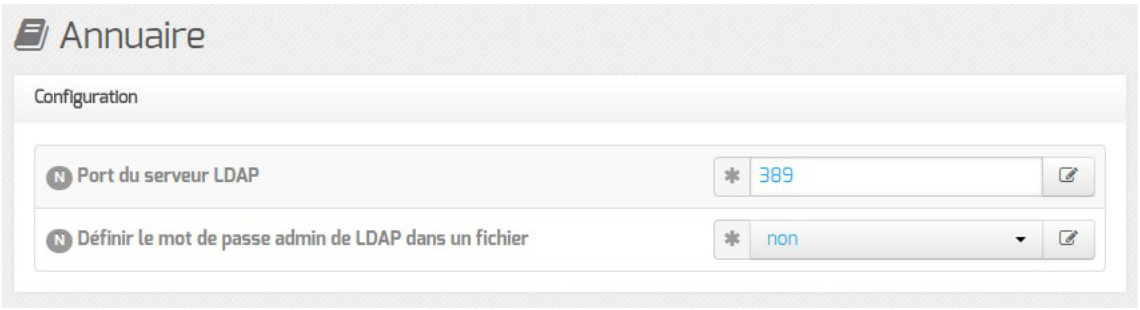
Pour cela il faut utiliser le formulaire suivant (en) : http://www.clamav.net/contact#reports
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.
En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.



Il ne faut pas signaler des PUA[p.775] comme étant des faux positifs.

4.15. Onglet Annuaire

Sur les modules Horus, Scribe et AmonEcole l'annuaire OpenLDAP est local.

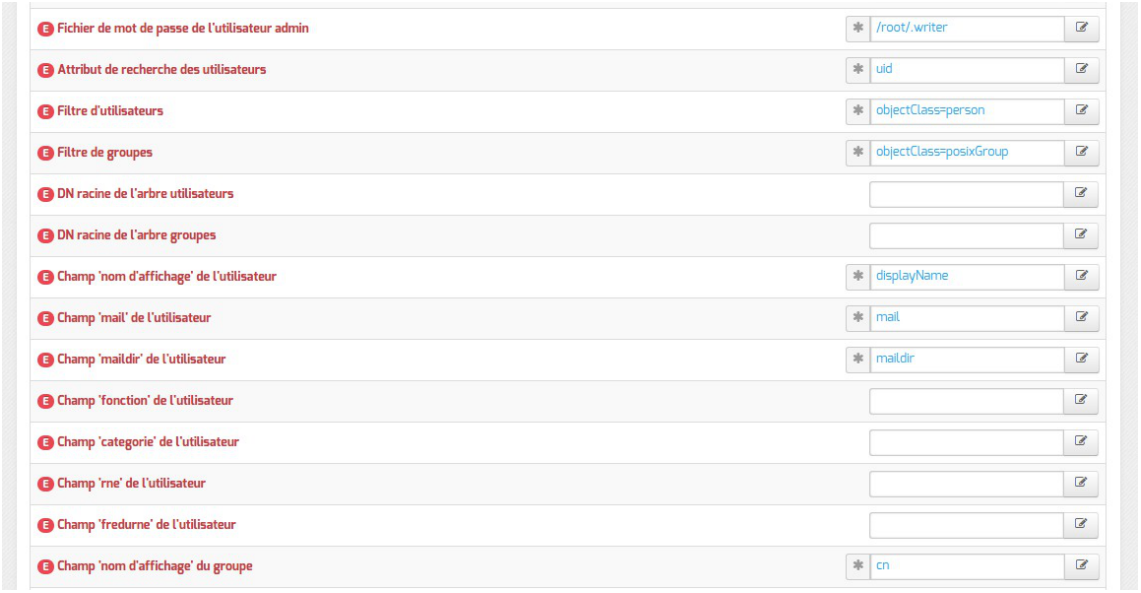


Lorsque l'annuaire est configuré comme étant local, l'onglet propose 2 paramètres :

- `Port du serveur LDAP` : permet de changer le port d'écoute du serveur LDAP ;
- `Définir le mot de passe admin de LDAP dans un fichier` : permet de stocker et de réutiliser par ailleurs le mot de passe administrateur de l'annuaire dans le fichier `/root/.writer`.

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

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



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

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

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



Le paramétrage d'un serveur LDAP local s'effectue dans l'onglet `Openldap`.

Voir aussi...

Onglet Openldap : Configuration du serveur LDAP local [p.226]

4.16. Onglet Dhcp : Configuration du serveur DHCP

Le serveur DHCP[p.758] 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).

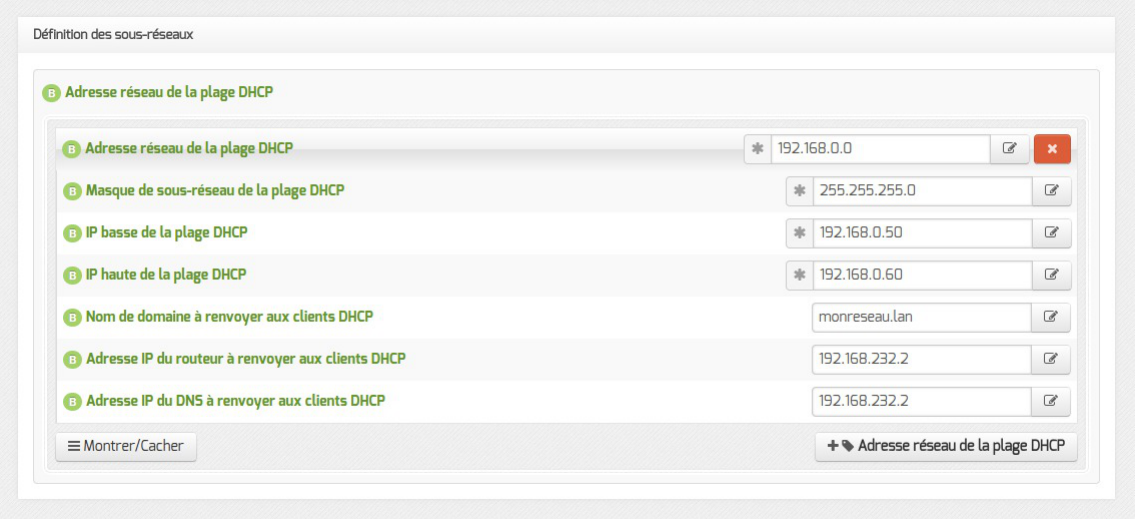
Sur les modules AmonEcole et AmonEcole-Eclair, les adresses servies sont celles du réseau interne (interface 1).

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.776] 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.761] pour une utilisation sans le module Amon. Il est également possible d'utiliser des serveurs DNS disponibles sur Internet.

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

Si vous disposez d'un module Amon ou d'un module AmonEcole, il est conseillé d'utiliser le module comme relais DNS[p.759], 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.



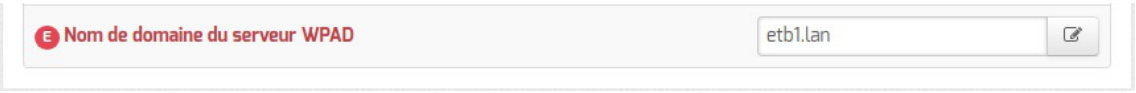
Il est possible de spécifier les adresses IP de Wins primaire et secondaire à renvoyer aux clients.

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).

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

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



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

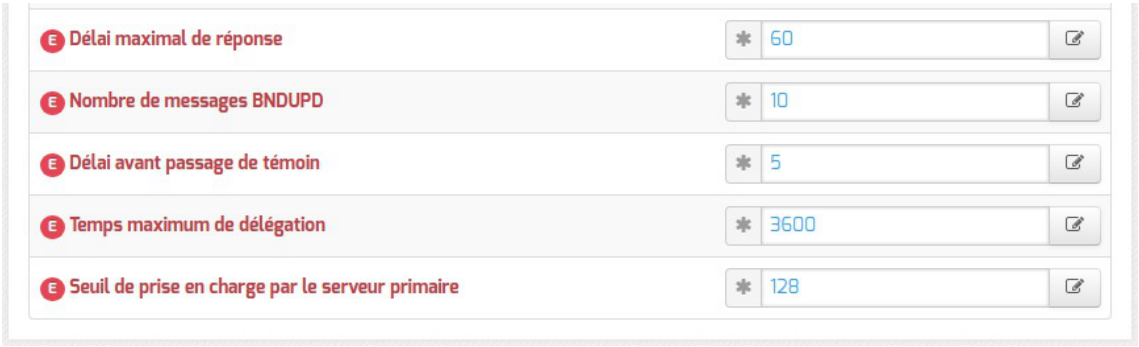


- `Nom de la grappe` : le nom de la grappe devra être le même sur le serveur primaire (local) et sur le serveur secondaire (pair) ;
- `Rang du serveur dans la grappe` : choisir `primary` pour le serveur primaire ;

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

- `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

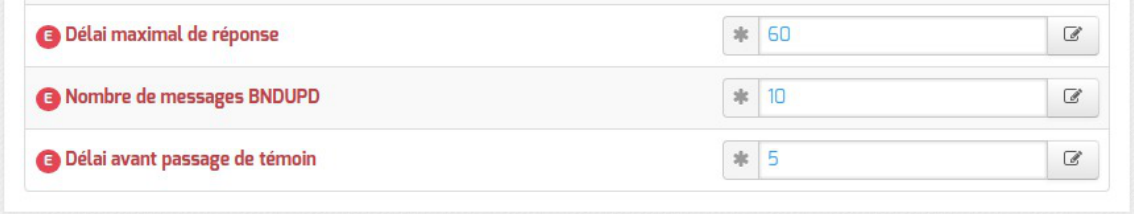


Pour un serveur secondaire, les variables à paramétrer sont :

- `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` ;
- `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`.

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

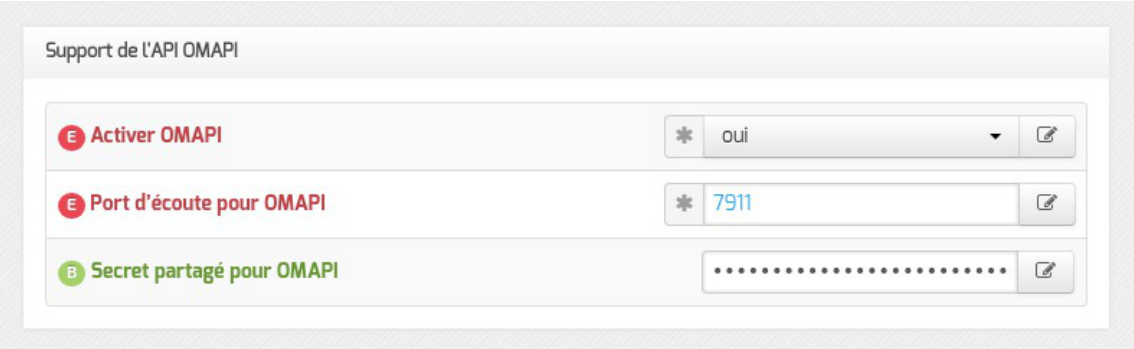
En mode expert, un certain nombre de variables permettent d'ajuster finement la configuration du failover.



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.772], 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.754].

La clé secrète sera à utiliser pour que les clients du service s'authentifient.

Voir aussi...

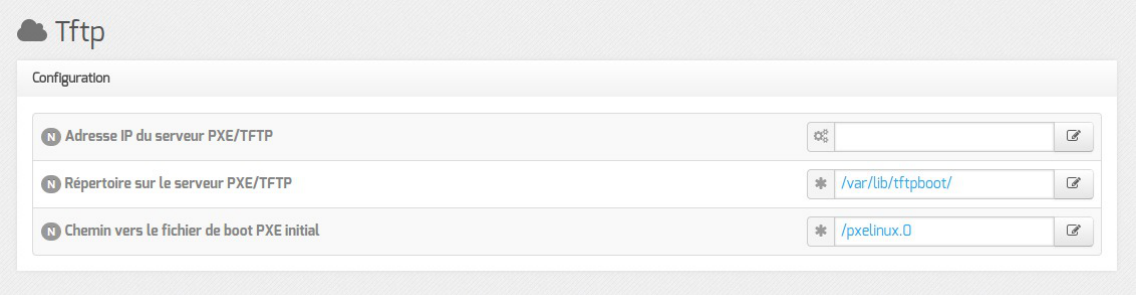
> Configurer la découverte automatique du proxy avec WPAD

4.17. 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.773], outil de clonage édité par le CRDP de Lyon (http://oscar.crdp-lyon.fr) :

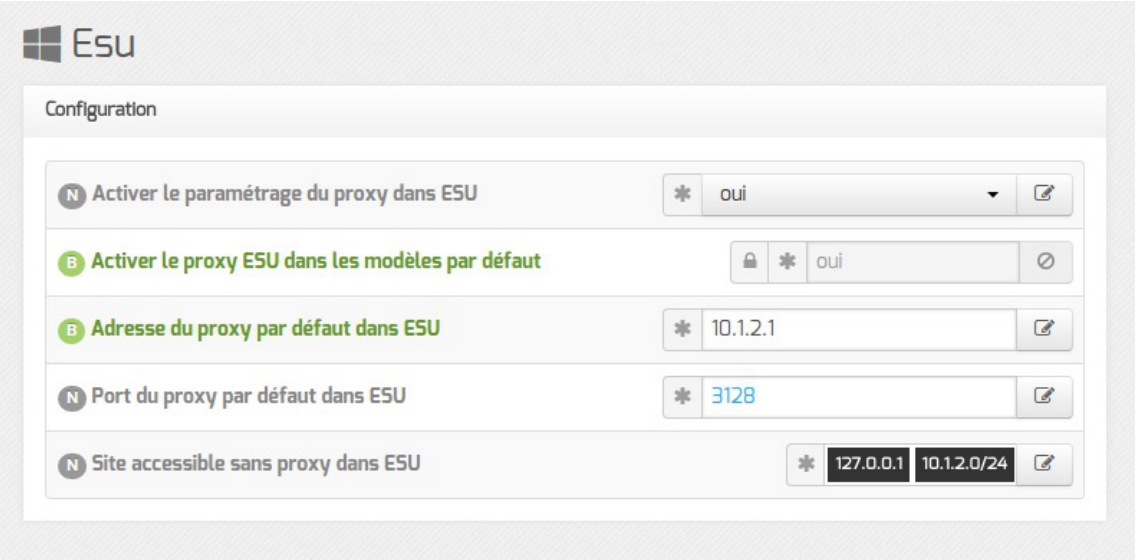
- Un procédure pour la mise en place d'OSCAR est disponible sur la forge EOLE à l'adresse : http://dev-eole.ac-dijon.fr/projects/oscar/wiki
- Une documentation sur l'utilisation d'OSCAR est disponible à l'adresse : http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/scribe/formationadminscribeoscar

4.18. Onglet Esu : Configuration du proxy ESU

Sur les modules Scribe et AmonEcole, l'utilisation du couple ESU / ClientScribe est obligatoire pour les stations Windows Microsoft rattachées au domaine et l'onglet `Esu` est d'emblée visible.

Sur le module Horus, l'onglet `Esu` n'est visible qu'après activation du service dans l'onglet `Services` en passant l'option : `Utiliser le logiciel ESU` à `oui`. Ce mode de fonctionnement nécessite l'installation du logiciel ClientHorus sur les stations clientes.

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



La configuration du proxy pour des stations clientes gérées par ESU s'effectue au niveau de l'interface de configuration du module dans l'onglet `Esu`.

Après avoir passé la variable `Activer le paramétrage du proxy dans ESU` à `oui` il est possible de paramétrer le proxy ESU.

La variable `Activer le proxy ESU dans les modèles par défaut` permet de définir le comportement du proxy ESU dans les modèles par défaut. Ce choix par défaut sera appliqué dans les modèles à l'instance et ne pourra plus être modifié par l'interface de configuration du module.

Si, à l'avenir, l'utilisateur souhaite changer le comportement du proxy il devra le faire au travers de l'interface ESU.

> Les paramètres suivants `Adresse du proxy par défaut dans ESU`, `Port du proxy par défaut dans ESU` et `Réseau par défaut sans proxy dans ESU` sont modifiables à souhait et sont appliqués dans les variables ESU à chaque reconfiguration du module.

Saisir l'adresse IP ou le nom du proxy ESU dans le champ `Adresse du proxy par défaut dans ESU` et si besoin changer le port `3128` proposé par défaut.

Le champ `Site accessible sans proxy dans ESU` (nommé `Réseau par défaut sans proxy dans ESU` dans les versions antérieures à EOLE 2.5.2) permet d'ajouter plusieurs adresses IP, réseaux, noms de domaine et noms de machines pour lesquels le proxy ESU ne sera pas utilisé (exemple de valeurs : `mozilla.org`, `asso.fr`, `192.168.1.0/24`).

> Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet `Interface-1` (variable : `adresse ip eth1 proxy link`).

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

L'utilisation du logiciel ESU modifie profondément la configuration des stations clientes (emplacement des icônes, ...) et sa désactivation ne restaure pas leur configuration d'origine.

Pour récupérer une station utilisable hors du domaine, vous pouvez :

- ré-activer ESU, renseigner les options telles qu'elles sont sur un Windows par défaut (cases décochées), ouvrir une session et désactiver ESU ;
- restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que celui fourni par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

4.19. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.774]) de type Windows NT.

Cela signifie qu'il permet une authentification centralisée des ouvertures de session sur les postes clients et qu'il fournit un ensemble de partages aux utilisateurs (dossier personnel, dossier de groupes, partages communs, d'icônes, etc.).

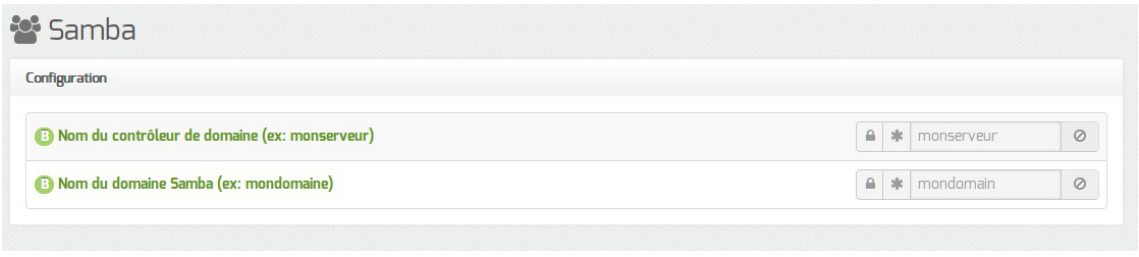
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

Sur le module Scribe, un professeur aura globalement plus de droits qu'un élève. Il a également à sa disposition des outils lui permettant d'interagir avec les élèves (observation, blocage, distribution de documents, etc.).

Seules deux variables sont à remplir avec attention pour obtenir un contrôleur fonctionnel.

Elles se trouvent dans l'onglet `Samba` de l'interface de configuration du module.

Domaine Samba



Configuration Samba

Le champ `Nom du contrôleur de domaine` (nom d'ordinateur NetBIOS[p.770][p.770]) est le nom qui sera utilisé pour accéder aux fichiers avec la syntaxe `\\machine`.

Sa taille maximale est fixée à 15 caractères et il ne doit pas être modifié une fois le module instancié.

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

En mode conteneur (sur les modules AmonEcole et ses variantes), il doit impérativement être différent du `Nom de la machine`.

Le champ `Nom du domaine Samba`, aussi appelé groupe de travail (workgroup) est le nom qui sera utilisé lors de l'intégration d'une station au domaine.



Sa taille maximale est également fixée à 15 caractères et il ne doit pas être modifié une fois que le module instancié.

Il doit impérativement être différent du `Nom du contrôleur de domaine`.



Caractères autorisés et non autorisés

Noms d'ordinateur NetBIOS peuvent contenir tous les caractères alphanumériques à l'exception des caractères étendus suivants :

- la barre oblique inverse (\) ;
- marque de barre oblique (/) ;
- signe deux-points (:) ;
- astérisque (*) ;
- point d'interrogation (?) ;
- guillemet (") ;
- inférieur à (<) signe ;
- signe supérieur à (>) ;
- barre verticale (|).

Attention, les noms peuvent contenir un point, mais ne peuvent pas commencer par un point.

Pour en savoir plus sur les conventions de nommage dans un domaine, vous pouvez consulter la page :

http://support.microsoft.com/kb/909264/fr

Fichiers invisibles sur les partages

Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

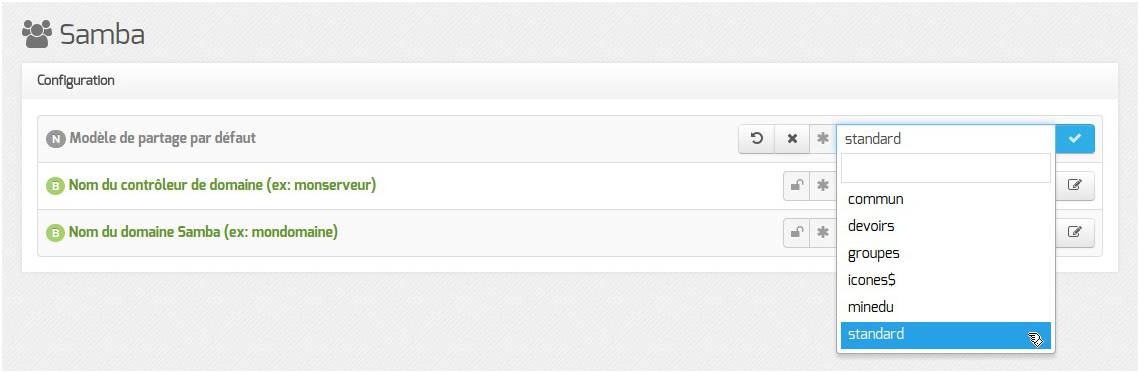
Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- desktop.ini : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`). En mode expert, la liste des fichiers cachés peut être personnalisée grâce à la variable `Fichiers à masquer dans le partage` ;
- $recycle.bin : les fichiers `$recycle.bin` générés par le fonctionnement de Windows sont cachés et inaccessibles par l'utilisateur (`veto files = /$RECYCLE.BIN/` dans le fichier `smb.conf`).

Modèle de partage par défaut

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

En mode normal il est possible de choisir le modèle de partage par défaut.



Le fichier de configuration Samba (`/etc/samba/smb.conf`) est généré à partir des informations contenues dans l'annuaire.

Par défaut, les partages utilisent le template python : `/usr/share/eole/fichier/models/standard.tmpl`

Il est possible d'utiliser un autre modèle de partage par défaut pour les nouveaux partages en renseignant son nom (sans l'extension `.tmpl`) au niveau de l'option `Modèle de partage par défaut`.

Il existe déjà plusieurs modèles à disposition :

- `standard`
  héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe
- `commun`
  héritage des permissions, accès en écriture, accessible à tous en lecture et en écriture, accès anonyme (guest)
- `devoirs`
  héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `groupes`
  héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `icones$`
  caché dans le voisinage réseau, accès anonyme (guest)
- `minedu`
  héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe, nom de fichier et répertoire en minuscules

Configuration avancée du serveur Samba

En mode expert il est possible d'affiner la configuration du serveur Samba.

Âge maximal par défaut des mots de passe

Définit la durée en jours avant expiration d'un mot de passe.

Cette durée est compté à partir de la date d'enregistrement du mot de passe.

Si la valeur est à 0 alors le mot de passe n'expire jamais.

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

Durée du cache des résultats de requêtes négatifs

Durée du cache des résultats de requêtes négatifs exprimée en secondes (une valeur de 1 désactive le cache).

Délai avant abandon pour la connexion au LDAP

Durée en secondes avant abandon de la connexion à l'annuaire LDAP.

Libellé du serveur Samba

Par défaut le libellé est le nom de l'établissement, il apparaît sur les stations clientes, il peut être modifié à votre convenance.

Activer la corbeille Samba

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

L'option `Activer la corbeille Samba` permet de paramétrer Samba pour que les fichiers supprimés soient déplacés dans un répertoire "corbeille".

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

Il est possible de rendre ce répertoire accessible en lui donnant un autre nom (exemple : `corbeille`).

La durée de conservation des fichiers supprimés est également 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.

Activer l'envoi de courriel en cas de dépassement des quotas

Un envoi de courriel peut être activé en cas de dépassement de quotas. L'envoi se fait une fois par jour durant les 7 jours alloués pour résoudre le problème d'espace disque.

Activer le mode invité sur le partage

Certaines configurations ou logiciels (exemple : *WPKG*) nécessitent de paramétrer des partages en mode invité (`guest ok = yes`).

Cela n'est possible que si le mode invité a été activé à l'aide de l'option `Activer le mode invité sur le partage`.

Niveau de log

Le niveau de log est à `0` par défaut, il peut être paramétré entre 0 et 10.

Nombre de minutes d'inactivité avant déconnexion automatique d'accès à un fichier

Cette option globale définit le nombre de minutes que Samba va attendre un client inactif avant de fermer sa session avec le serveur Samba. Un client est considéré comme inactif quand il n'a pas de fichiers ouverts et qu'il n'envoie aucune donnée.

Si la valeur de cette option est mise à `0`, cela qui signifie que Samba ne fermera jamais aucune connexion et cela peut conduire à une consommation inutile des ressources du serveur par les clients inactifs.

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

Pour la plupart des réseaux, l'utilisation de cette option ne posera pas de problème car la reconnexion du client sera réalisée de manière transparente pour l'utilisateur.

Fichiers à masquer dans le partage

Cette option permet de personnaliser la liste des fichiers qui doivent être cachés à l'utilisateur.



Il est impératif de respecter le format attendu par le fichier de configuration de Samba à savoir :

`/desktop.ini/fichier2/fichier3/`

Démarrer le serveur Wins

Sert à la résolution des noms de machine sur un réseau type Microsoft Windows.

Option à `oui` par défaut, désactivable si un autre service Wins est présent sur le réseau.

Rechercher des noms d'hôte dans le DNS

Recherche complémentaire sur le serveur DNS si le serveur n'a pas identifié la machine via Wins.

Option à `non` par défaut.

Activer les verrous opportunistes (oplocks)

Les verrous opportunistes augmentent les performances du serveur en activant un accès exclusif aux fichiers.

Option à `non` par défaut. Les verrous sont gérés côté client et certaines applications ne gèrent pas les verrous.

Activer le support des attributs DOS

Option à `non` par défaut. Permet à Samba d'utiliser les attributs DOS (caché, système et archive).

Niveau de candidature lors de l'élection d'un maître explorateur

Cette valeur va influer sur les chances de Samba de remporter les élections de maître explorateur.

La valeur par défaut est `99`. Elle doit être comprise entre 0 et 255.

Niveau de protocole maximum supporté par le serveur

Cette variable, disponible depuis la version 2.5.2 d'EOLE, permet de forcer l'utilisation d'un protocole.

Par défaut, la valeur sur un module EOLE 2.6 est `default`. Cette valeur est la valeur proposée par défaut par la version de Samba elle-même.



La valeur `default` est par exemple SMB3 pour la version 4.1.6 de Samba.



Depuis la version 1709 de Windows 10 l'intégration au domaine d'une station nécessite au préalable :

- de laisser le niveau de protocole maximum à la valeur `default` sur le module gérant le

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

domaine (Scribe, Horus ou AmonEcole) ;

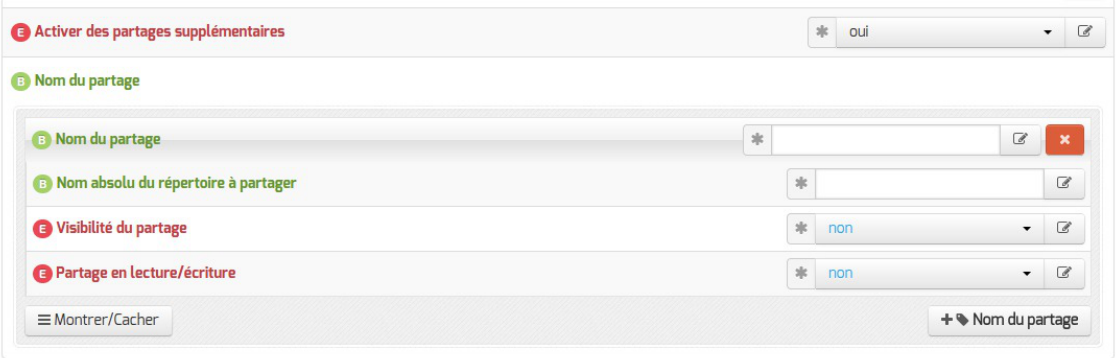
- d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.

Annoncer Spoolss comme architecture x64

Le service d'impression de Samba se présente par défaut comme étant 32-bit ("Windows NT x86"). `Annoncer Spoolss comme architecture x64`, disponible à partir de la version 2.5.2 d'EOLE, permet au serveur d'impression de se présenter comme étant 64-bit (Architecture = x64 de Windows) ce qui permet d'ajouter des pilotes d'imprimante 64 bits.

Activer des partages supplémentaires

Passer `Activer des partages supplémentaires` à `oui` permet d'activer un ou plusieurs nouveaux partages. Pour ajouter un ou plusieurs partages il faut cliquer sur le bouton `+ Nom du partage` .



Les options à saisir pour chaque partage supplémentaire sont :

- le `Nom du partage` ;
- le `Nom absolu du répertoire à partager` = chemin Unix du répertoire à partager ;
- la `Visibilité du partage` = visibilité dans le voisinage réseau ;
- le `Partage est en lecture/écriture` :
  - si la variable est à `oui` → lecture/écriture ;
  - si la variable est à `non` → lecture seule.



L'activation et la déclaration d'un partage supplémentaire ne crée pas le répertoire sur le disque. Il faut réaliser cette opération manuellement et affecter des droits adaptés sur le répertoire.

Partages manuels

Le fichier `smb.conf` est re-généré à chaque reconfiguration du serveur (commande `reconfigure`) et également lors de l'ajout d'un partage ou d'un groupe avec partage.

Ce fichier est généré à partir du template : `/usr/share/eole/creole/distrib/smb.conf` et des partages déclarés dans l'annuaire LDAP.

Le template, qui contient principalement la section `[global]`, peut éventuellement être patché.

La gestion des ACLs en elle-même est totalement indépendante de la configuration de Samba.

Il est possible de déclarer un partage supplémentaire manuellement en plaçant un fichier (possédant

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

l'extension `.conf`) décrivant le partage dans le répertoire `/etc/samba/conf.d/`.
Sa prise en compte nécessite un `reconfigure`.



Pour plus d'informations, vous pouvez consulter la page de manuel :
`# man smb.conf`
ou
http://manpages.ubuntu.com/manpages/xenial/en/man5/smb.conf.5.html

Autoriser l'ouverture de flux à partir d'un port source

Lors de diagnostic il peut être utile d'utiliser la commande `nmblookup` pour déterminer l'adresse IP du ou des serveurs contrôleurs de domaine sur le réseau local.
Pour que l'échange puisse se faire en UDP via le port 137 il est nécessaire que le serveur EOLE puisse en autoriser l'accès.

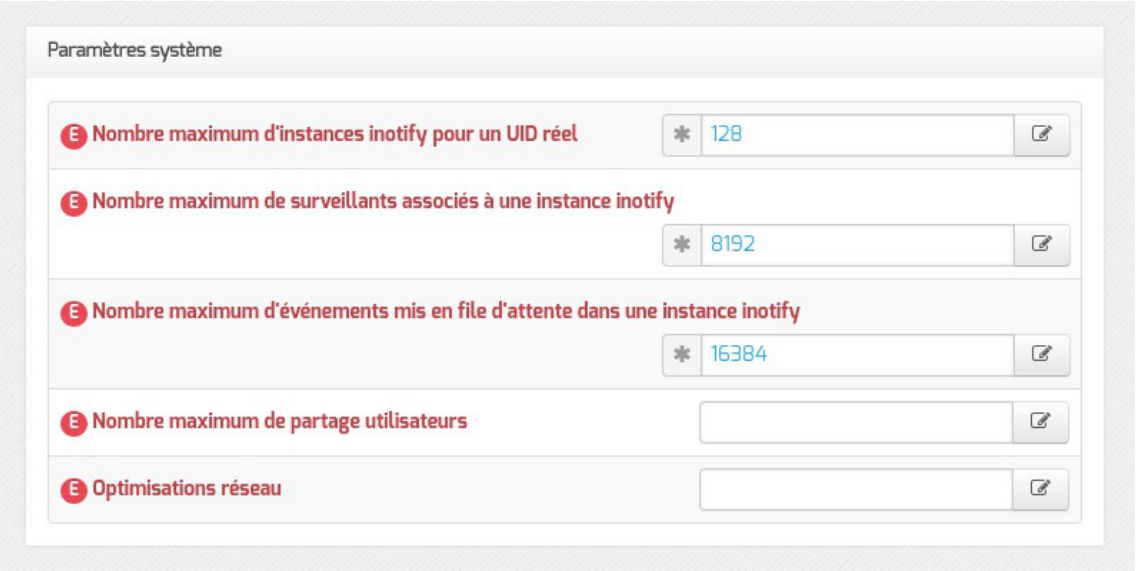
Pour activer cette fonctionnalité il faut passer `Autoriser l'ouverture de flux à partir d'un port source` à `oui`.



Les options pour le port autorisés et le protocole peuvent être laissés par défaut. Par contre il est important de choisir l'interface sur laquelle aura lieu cette autorisation.
Il est possible d'ajouter des autorisations sur plusieurs interfaces en cliquant sur le bouton `Port source à partir duquel les flux sont autorisés`.

Paramètres système

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



En cas de forte sollicitation d'accès à un partage Samba (nombre de fichiers ouverts par Samba supérieur à 20000) l'augmentation des valeurs sur les 3 paramètres ci-dessous permet d'éviter les pertes d'accès au partage :

- `Nombre maximum d'instances inotify pour un UID réel`
- `Nombre maximum de surveillants associés à une instance inotify`
- `Nombre maximum d'événements mis en file d'attente dans une instance inotify`

La variable `Nombre maximum de partage utilisateurs` permet de limiter le nombre de dossiers partagés par utilisateur (directive : *usershare max shares*). Par défaut, ceux-ci sont ignorés.

La variable `Optimisations réseau` permet de personnaliser les options de la directive Samba : *socket options*.

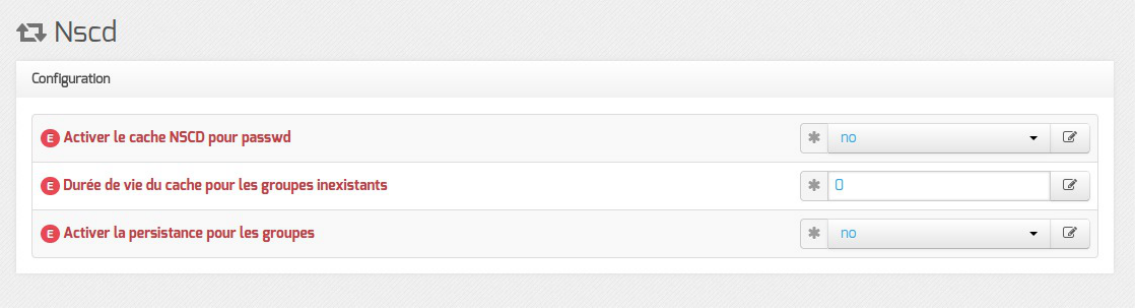
Voir aussi...

> Onglet Clamav : Configuration de l'anti-virus

4.20. Onglet Nscd

NSCD[p.771] est un démon qui fournit un cache pour limiter les requêtes vers l'annuaire LDAP.

Les options de configuration sont dans le fichier `/etc/nscd.conf`.



L'onglet Nscd permet de modifier quelques options pour mettre en cache des données utilisateurs :

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

- `Activer le cache NSCD pour passwd` : active explicitement le cache pour les mots de passe ;
- `Durée de vie du cache pour les groupes inexistants` : Si une entrée n'est pas trouvée par le service de nom, elle est ajoutée au cache et marquée comme inexistante. Cette option définit le nombre de secondes après lesquelles une telle entrée n'existant pas est retirée du cache. La valeur par défaut est 0 seconde pour le cache des groupes ;
- `Activer la persistance pour les groupes` : Si la persistance est activée, le contenu du cache sera conservé lors du redémarrage du service nscd.

4.21. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.771]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

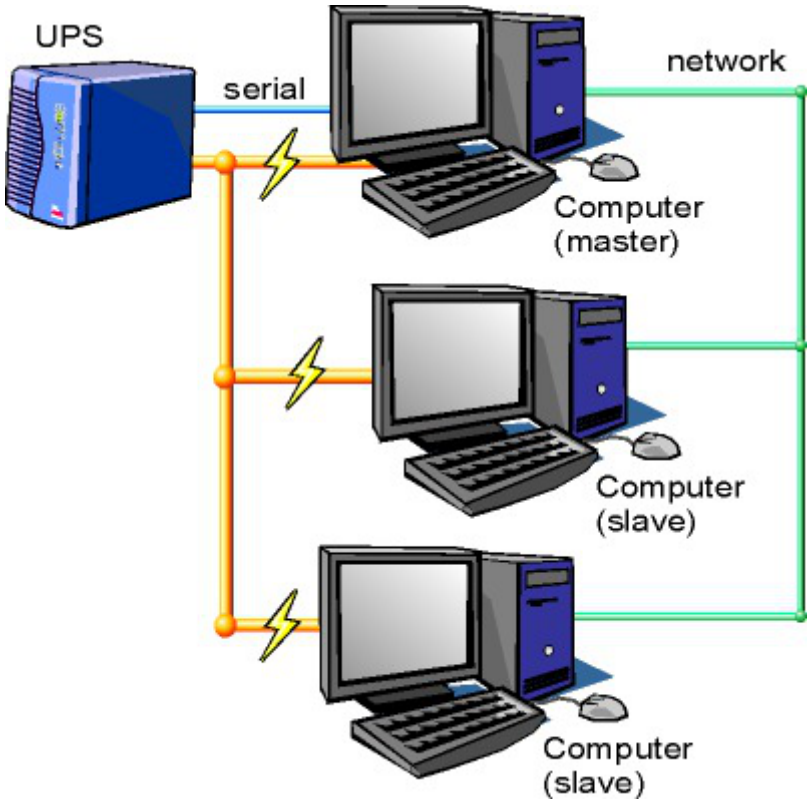


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

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

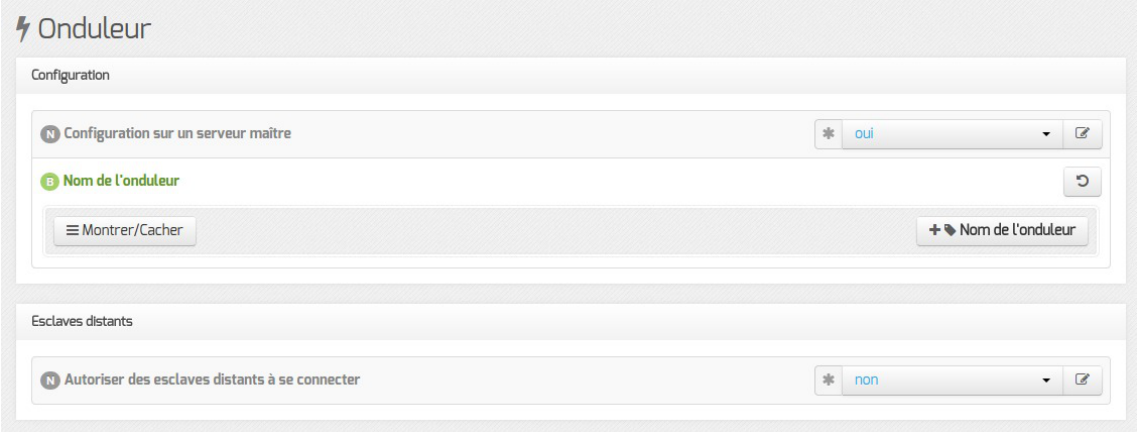
http://www.networkupstools.org/stable-hcl.html

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

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

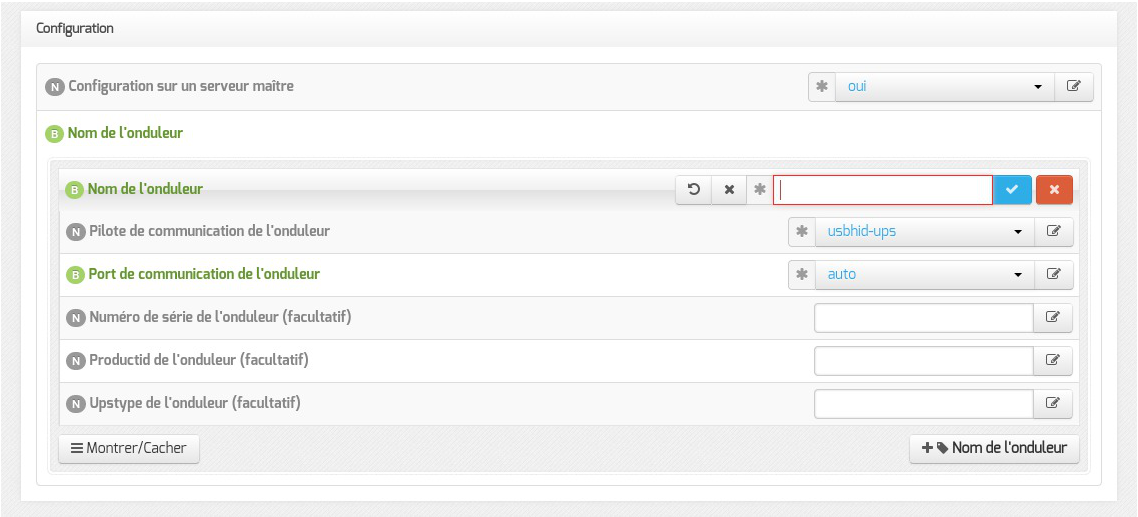
> `# apt-cache policy nut`
>
> ou encore :
>
> `# apt-show-versions nut`
>
> Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :
>
> http://www.networkupstools.org/source/2.7/new-2.7.1.txt
>
> Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :
>
> http://www.networkupstools.org/source/2.7/new-2.7.3.txt

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



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

La configuration sur un serveur maître



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

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

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

l'onduleur n'est pas USB.

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

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

Configuration d'un second onduleur sur un serveur maître

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

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

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

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

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

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

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

Deux onduleurs de même marque

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

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


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

Deux onduleurs différents

Un onduleur sur port série :

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

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

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

Onduleur sur port USB :

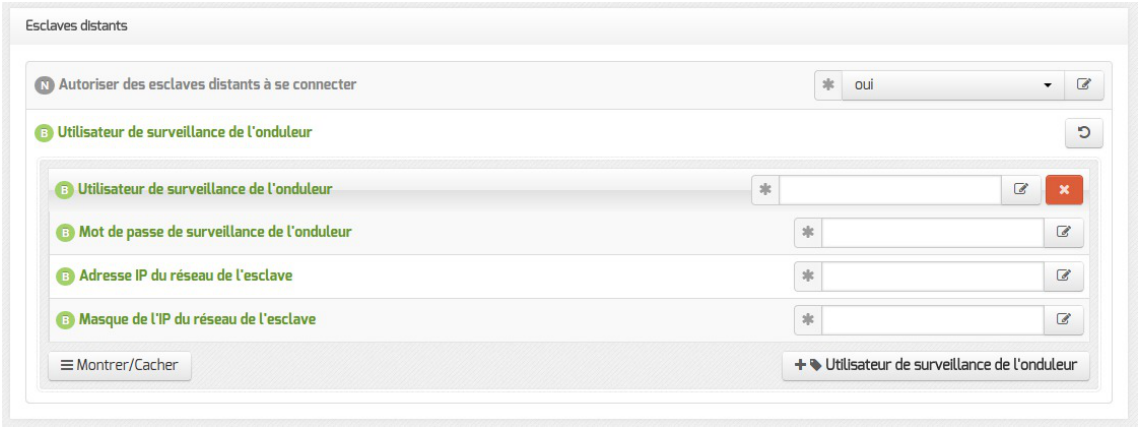
- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

La majorité des onduleurs USB sont détectés automatiquement.

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

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



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

Pour chaque utilisateur, il faut saisir :

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

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

- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)

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

Chaque utilisateur doit avoir un nom différent.

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

Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf` ou consulter la page web suivante : http://manpages.ubuntu.com/manpages/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` ;

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

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

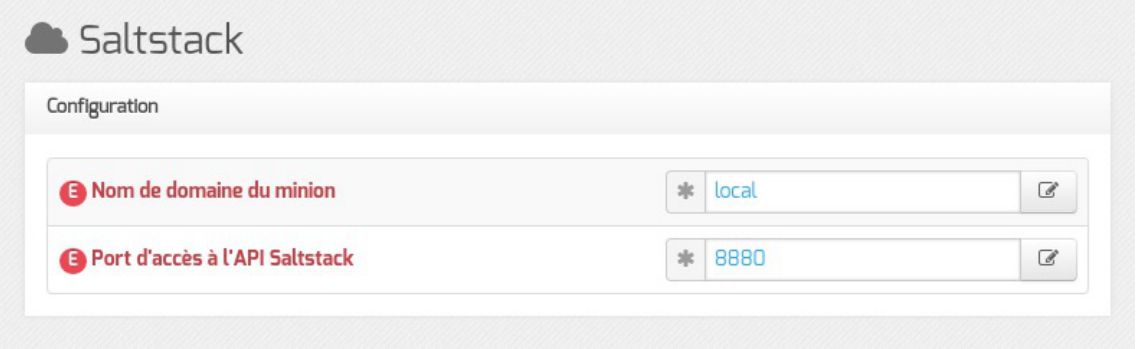
Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

4.22. Onglet Saltstack

L'onglet `Saltstack` permet de personnaliser la configuration de Saltstack[p.777].

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.

4.23. Onglet Applications web : Configuration des applications web

Les onglets `Applications web` et `Apache` ne sont disponibles qu'après activation du service, `Activer le serveur web Apache` à `oui`, dans l'onglet `Services`.

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



L'onglet `Applications web` permet un réglage minimum pour le fonctionnement des applications web. Il permet aussi d'activer/désactiver toutes les applications web EOLE installées sur le module.

Nom de domaine des applications web

Le choix du `Nom de domaine des applications web` est essentiel.

Pour un bon fonctionnement de toutes les applications, il est impératif d'utiliser un nom de domaine.

Dans la mesure du possible, il faut que celui-ci soit résolvable sur Internet. Si ce n'est pas le cas, il est possible d'utiliser un nom de domaine local diffusé par le serveur DNS[p.759] de l'établissement.

Ce paramètre ne doit pas être précédé du nom du protocole.

À partir de la version EOLE 2.6.1, les adresses IP ne sont plus autorisées pour cette variable.

Cette restriction est notamment due au durcissement du support du protocole HTTPS[p.764] par les navigateurs.

Application web par défaut

L'application web par défaut sera celle renseignée dans la variable : `Application web par défaut (redirection)`.

Si la variable `Application web par défaut` vaut `/webmail`, alors l'adresse `http://<adresse serveur>/` pointera vers `http://<adresse serveur>/webmail/`

Serveur web et proxy inverse

Lorsque le serveur web est derrière un proxy inverse, c'est l'adresse IP du proxy inverse et non celle de l'utilisateur qui est enregistrée dans les fichiers de journalisation. Pour éviter cela, il est possible de passer la variable `Le serveur web est derrière un reverse proxy` à `oui` et de déclarer son adresse (généralement l'adresse IP du module Amon sur la zone) dans `Adresse IP du serveur reverse proxy`.

Sur le module AmonEcole, si le proxy inverse est activé, les variables sont calculées et masquées : `Le serveur web est derrière un reverse proxy` est à `oui` et l'

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

> `Adresse IP du serveur reverse proxy` est celle du bridge interne : `192.0.2.1`.



> La déclaration du proxy inverse ajoute une entête qui contient une adresse IP qui peut potentiellement être falsifiée depuis la machine source.
>
> En cas d'utilisation d'un proxy, la récupération de l'adresse IP des stations du réseau local n'est pas garantie.



> Sur EOLE 2.6.0 et inférieur, cette fonctionnalité était implémentée via le module Apache additionnel RPAF : https://github.com/gnif/mod_rpaf.
>
> Sur EOLE 2.6.1 et supérieur, cette fonctionnalité est implémentée via le module Apache natif RemoteIP : https://httpd.apache.org/docs/current/fr/mod/mod_remoteip.html

Activer Bareos WebUI (gestion de la sauvegarde)

Bareos WebUI est une application web permettant de surveiller et gérer les sauvegardes Bareos.

Activer phpMyAdmin (administration des bases MySQL)

phpMyAdmin permet de gérer les bases de données MySQL hébergées par le module.

Pour activer/désactiver l'application web phpMyAdmin il faut passer la variable `Activer phpMyAdmin (administration des bases MySQL)` à `oui`.

Certificats

En mode expert il est possible d'activer la vérification de l'autorité de certification pour les applications web cassifiées et de modifier le chemin des certificats utilisés par le serveur web Apache.



4.24. Onglet Apache : Configuration avancée du serveur web

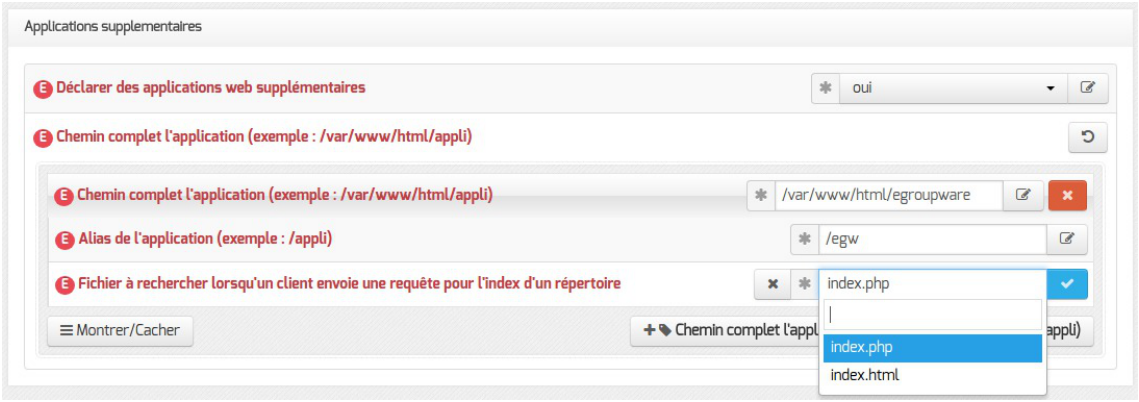
Les onglets `Applications web` et `Apache` ne sont disponibles qu'après activation du service, `Activer le serveur web Apache` à `oui`, dans l'onglet `Services`.

L'onglet expert `Apache` permet de déclarer des applications web supplémentaires et d'affiner la configuration du serveur web.

Applications supplémentaires

Pour déclarer de nouvelles applications web, il faut tout d'abord passer la variable `Déclarer des applications web supplémentaires` à `oui`.

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



Déclaration d'une application web dans gen_config

Il est ensuite possible d'ajouter des déclarations en cliquant sur le bouton `+ Chemin complet l'application (exemple : /var/www/html/appli)`, puis remplir les 2 paramètres :

- `Chemin complet l'application (exemple : /var/www/html/appli)` ;
- `Alias de l'application (exemple : /appli)`.

La variable `Fichier à rechercher lorsqu'un client envoie une requête pour l'index d'un répertoire` (disponible à partir de la version 2.6.2 d'EOLE) permet de définir le fichier ressource à rechercher lorsqu'un client envoie une requête pour l'index d'un répertoire, en ajoutant un '/' à la fin du nom de ce dernier (directive : `DirectoryIndex`).



- `Chemin complet l'application (exemple : /var/www/html/appli)` : /var/www/html/egroupware
- `Alias de l'application (exemple : /appli)` : /egw

Après instanciation ou reconfiguration du module, le logiciel doit répondre à l'adresse : `http://<adresse serveur>/egw`

La déclaration a pour effet la création d'un fichier de configuration Apache dans /etc/apache2/sites-enabled/. Elle n'installe pas et ne suffit en aucun cas à faire fonctionner une nouvelle application web.

Une section de la documentation décrit le processus complet d'ajout d'applications web.

Configuration Apache

Les variables permettent de modifier et de fixer une sélection de paramètres disponibles pour la configuration Apache MPM (module multi-processus) prefork dans différents fichiers de configuration : /etc/apache2/.

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



> Les nom de ces paramètres de configuration apache se retrouvent dans le nom des variables Creole et sont préfixés par la chaîne "`mpm_`", l'affichage du nom des variables s'obtient dans le mode debug de l'interface de configuration du module.

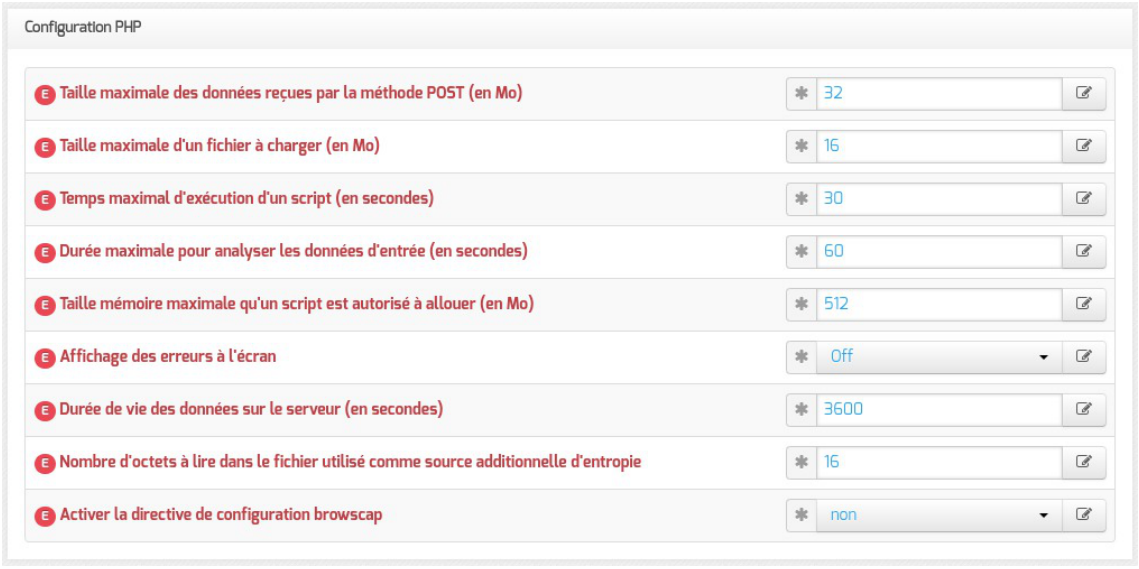
- `Permettre de lister les répertoires et leur contenu` : impacte le fichier `/etc/apache2/sites-available/default` en ajoutant la directive `Options -Indexes`.
- `Temps en secondes pendant lequel le serveur va attendre des entrées/sorties avant de considérer qu'une requête a échoué`.
- `Autoriser les connexions persistantes` : Passer ce paramètre à `Off` permet d'empêcher tout client de consommer trop de ressources du serveur.
- `Nombre de processus enfants du serveur créés au démarrage` : Cette directive permet de définir le nombre de processus enfants du serveur créés au démarrage.
- `Nombre minimum de processus serveurs enfants inactifs` : Cette directive permet de définir le nombre minimum désiré de processus serveurs enfants inactifs. Un processus inactif est un processus qui ne traite pas de requête. S'il y a moins processus inactifs que la valeur saisie, le processus parent va créer de nouveaux enfants de la manière suivante : il en crée un, attend une seconde, il en crée deux, attend une seconde, il en crée quatre, puis continue ainsi exponentiellement jusqu'à ce que son taux de création de processus enfants soit de 32 par seconde. Il ne s'arrête que lorsque le nombre de processus enfants correspond au chiffre saisi dans la directive.
- `Nombre maximum de processus serveurs enfants inactifs` : Cette directive permet de définir le nombre maximum souhaité de processus serveurs enfants inactifs. Un processus inactif est un processus qui ne traite pas de requête. S'il y a plus processus inactifs que le chiffre saisi, le processus parent arrêtera les processus excédentaires.
- `Nombre maximum de connexions pouvant être traitées simultanément` : Si la limite maximum est atteinte, toute tentative de connexion sera mise dans une file d'attente (la valeur de la directive *ServerLimit* ne doit pas être supérieur à la valeur de cette variable, aussi elle est automatiquement adaptée dans le template).
- `Nombre maximum de connexions qu'un processus enfant va traiter au cours de son fonctionnement` : Si ce nombre est défini à 0, il n'y a plus aucune limite sur le nombre de connexions que le processus pourra traiter.

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

Pour plus d'informations, vous pouvez consulter la liste des directives de la version MPM d'Apache : https://httpd.apache.org/docs/2.4/fr/mod/prefork.html

Configuration PHP

Les autres variables permettent de modifier et de fixer une sélection de paramètres disponibles dans le fichier de configuration : `/etc/php5/apache2/php.ini`.



Les nom de ces paramètres de configuration PHP se retrouvent dans le nom des variables Creole et sont préfixés par la chaîne "`php_`", l'affichage du nom des variables s'obtient dans le mode debug de l'interface de configuration du module.

- `Taille maximale des données reçues par la méthode POST (en Mo)` : Définit la taille maximale des données reçues par la méthode POST. Cette option affecte également le chargement des fichiers. Pour charger de gros fichiers, cette valeur doit être plus grande que la valeur de la `Taille maximale d'un fichier à charger (en Mo)`.

Si le module Scribe fonctionne avec un module Amon il faut également régler la `Taille maximale des données reçues par la méthode POST (en Mo)` en mode expert dans l'onglet `Reverse proxy` du module Amon.

- `Taille maximale d'un fichier à charger (en Mo)` : Définit la taille maximale d'un fichier à charger.
- `Temps maximal d'exécution d'un script (en secondes)` : Fixe le temps maximal d'exécution d'un script. Cela permet d'éviter que des scripts en boucles infinies saturent le serveur. La configuration par défaut est de 30 secondes.
- `Durée maximale pour analyser les données d'entrée (en secondes)` : Cette option spécifie la durée maximale pour analyser les données d'entrée via les méthodes POST et GET.

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

Cette durée est mesurée depuis le moment où PHP est invoqué sur le serveur jusqu'au début de l'exécution du script.

- `Taille mémoire maximale qu'un script est autorisé à allouer (en Mo)` : Cette option détermine la mémoire limite qu'un script est autorisé à allouer. Cela permet de prévenir l'utilisation de toute la mémoire par un script mal codé. Notez que pour n'avoir aucune limite, vous devez définir cette directive à -1.
- `Affichage des erreurs à l'écran` : Affiche les messages d'erreur PHP directement sur les pages consultées, attention cette option ne doit pas être utilisée en production et s'applique à toutes les applications web hébergées sur le serveur.
- `Durée de vie des données sur le serveur (en secondes)` : Spécifie la durée de vie des données sur le serveur. Après cette durée, les données seront considérées comme obsolètes, et supprimées.
- `Nombre d'octets à lire dans le fichier utilisé comme source additionnelle d'entropie` : Spécifie le nombre d'octets qui seront lus dans le fichier `/dev/urandom`. Par défaut, il vaut 0 , c'est à dire inactif.
- `Activer la directive de configuration browscap` : La directive de configuration *browscap* permet d'obtenir plus d'information sur les capacités du navigateur client grâce à la fonction *get_browser()* : http://browscap.org/.



Pour plus d'informations, vous pouvez consulter les exemples de configuration :

- `/usr/share/doc/php5-common/examples/php.ini-development`
- `/usr/share/doc/php5-common/examples/php.ini-production`

ou consulter la liste des directives du fichier `php.ini` : http://www.php.net/manual/fr/ini.list.php

Voir aussi...

Prise en charge d'applications supplémentaires [p.250]

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

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

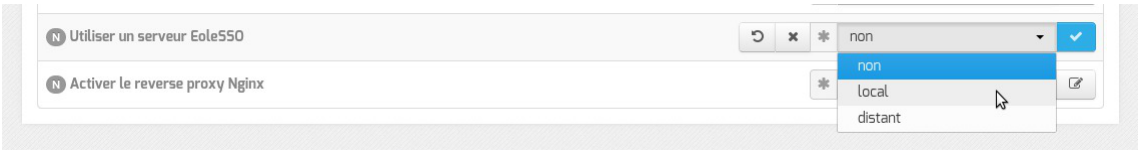
Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

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

Serveur local ou distant

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

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

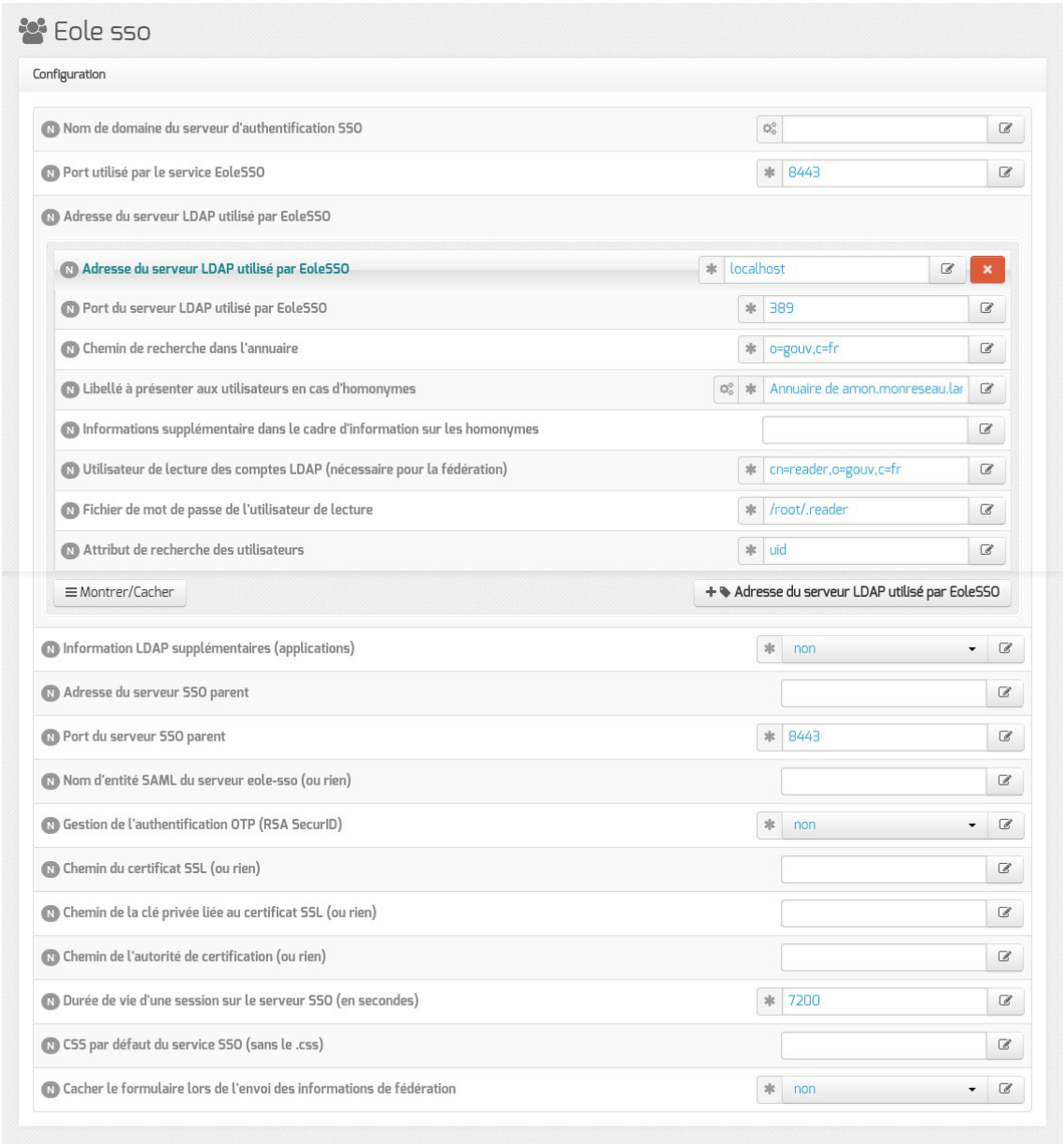


La variable `Utiliser un serveur EoleSSO` permet :

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

Adresse et port d'écoute

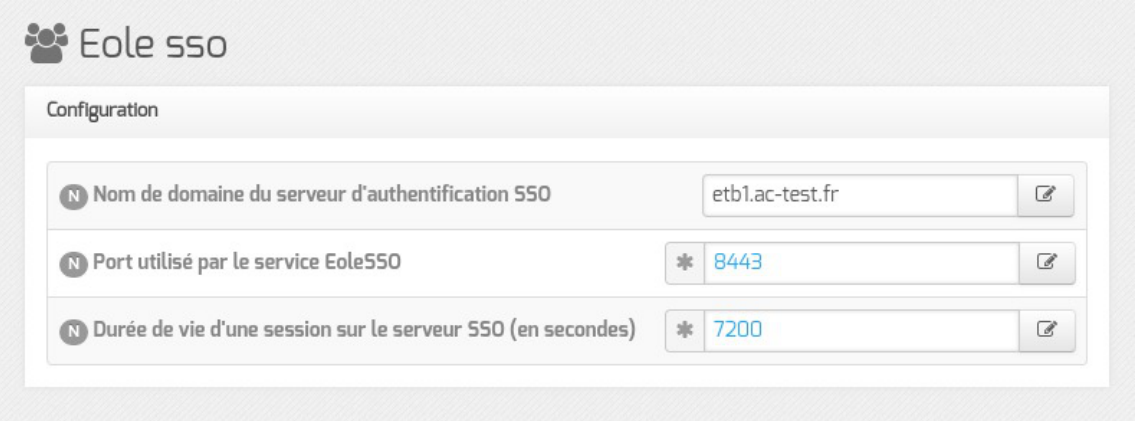
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

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

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



Configuration d'un serveur EoleSSO distant

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

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

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

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.766] pour authentifier les utilisateurs et récupérer leurs attributs.

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs (basedn) ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN[p.758] et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.773] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur

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

ayant accès en lecture au serveur LDAP configuré.

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

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

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

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

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

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.784] en HTTPS, sur le port défini pour le serveur EoleSSO).

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



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

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.778] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)

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

- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

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

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.765] du serveur et sont utilisés par défaut.

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

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.777] (version 2).

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

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

Autres options

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

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le

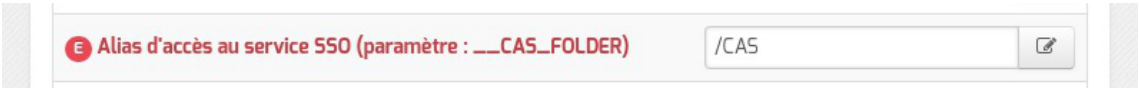
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

Configuration en mode expert

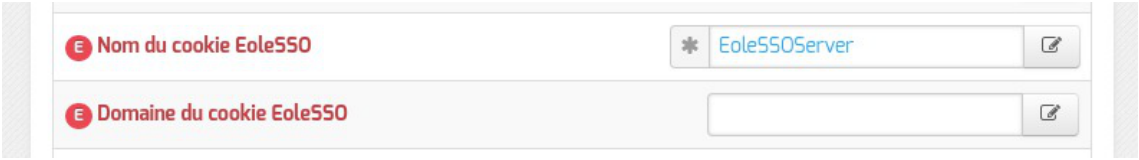
Options générales

En mode expert plusieurs nouvelles variables sont disponibles :

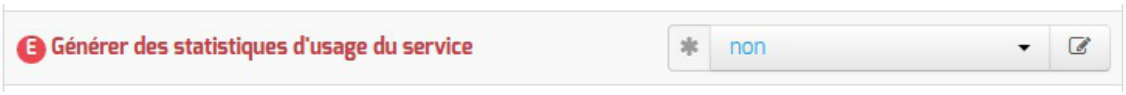


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP[p.767] ou keycloak[p.766].

  Cette variable est disponible uniquement à partir de la version 2.6.2 d'EOLE.

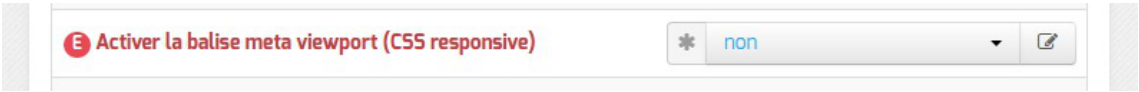


- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.



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

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



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



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

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

- À partir d'EOLE 2.6.2, la variable `Nombre maximum de sessions en attente (backlog)`

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

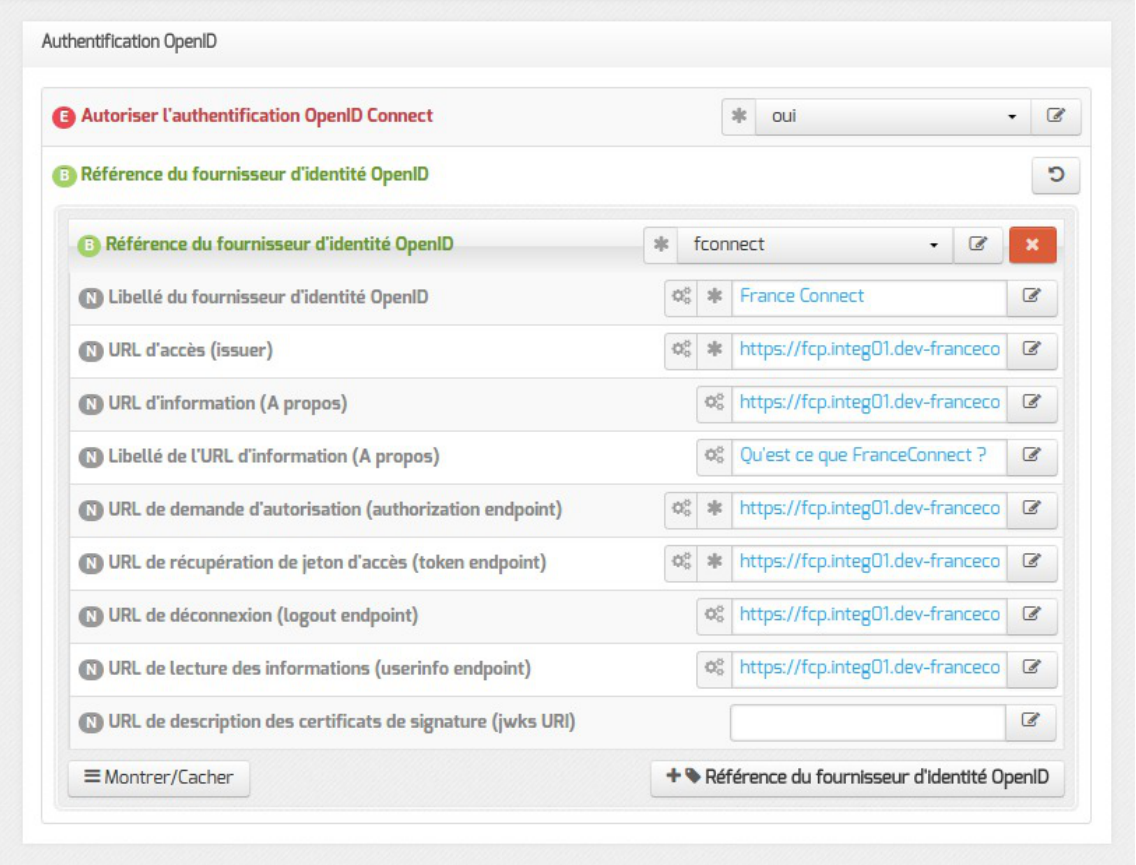
permet de définir la taille de la file d'attente des sessions.

Augmenter cette valeur est susceptible de résoudre des problèmes de lenteur voir de rejet des demandes d'authentification ;

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

  Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;
- `Utiliser l'authentification SSO pour l'EAD` est à `oui` par défaut. Le passer à `non` permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Configuration d'authentification OpenID Connect



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

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;

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

- /usr/share/sso/interface/images/logo-<libelle>.png : logo du fournisseur qui sera affiché sur la page d'association de comptes.

- Libellé du fournisseur d'identité OpenID : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- URL d'accès (issuer) : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- URL de demande d'autorisation (authorization endpoint) : URL permettant au client d'initier le processus d'authentification ;
- URL de récupération de jeton d'accès (token endpoint) : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- URL de déconnexion (logout endpoint) : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- URL de lecture des informations (userinfo endpoint) : URL permettant de récupérer les informations de l'utilisateur à l'aide du jeton fourni ;
- URL de description des certificats de signature (jwks URI) : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

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



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

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

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

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

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

Voir aussi...

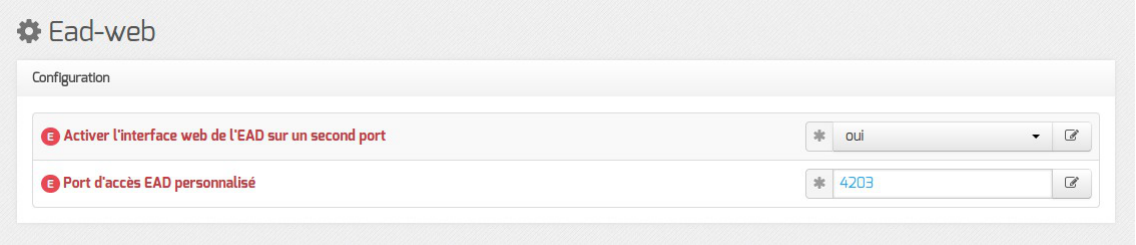
Gestion des sources d'authentification multiples [p.288]

Compatibilité OpenID Connnect [p.267]

4.26. Onglet Ead-web : EAD et proxy inverse

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

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



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

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

Voir aussi...

> Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur [p.375]

4.27. Onglet Mysql : Configuration du serveur MySQL

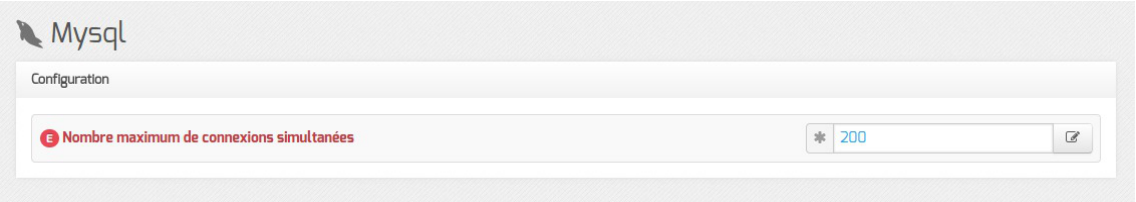
Sur les modules Scribe et AmonEcole, le serveur de base de données MySQL est obligatoirement activé.

Sur les autres modules, il est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option : `Activer le serveur de bases de données MySQL`. L'onglet expert `Mysql` apparaît uniquement si le service est activé.

L'onglet expert `Mysql` permet de modifier et de fixer une sélection de paramètres disponibles dans le fichier de configuration : /etc/mysql/my.cnf

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

Nombre maximum de connexions simultanées



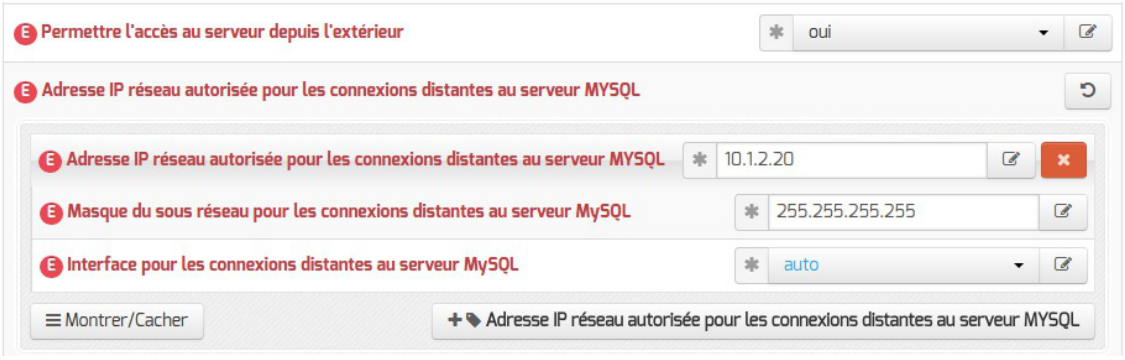
Ce paramètre permet d'augmenter le nombre de connexions clientes maximum simultanées.

Cela peut s'avérer nécessaire sur des sites où la fréquentation des applications web est très importante et où l'erreur MySQL `Too many connections` apparaît fréquemment.

Adresses autorisées à accéder à MySQL

À partir d'EOLE 2.6.1, il est possible de déclarer les adresses IP ou les réseaux autorisés à accéder au serveur MySQL local.

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



Pour autoriser des adresses à accéder au serveur MySQL, il faut passer la variable `Permettre l'accès au serveur` depuis l'extérieur à `oui` puis ajouter les couples d'adresse réseau/masque souhaités.

Dans le cas où le serveur possède plusieurs interfaces réseau, il est possible de préciser l'interface par laquelle les adresses définies ont le droit de se connecter.

Sur le module Horus, l'`Adresse IP réseau autorisée pour les connexions distantes au serveur MYSQL` est pré-renseignée avec l'adresse du réseau local.

Cette fonctionnalité n'est pas disponible sur les modules AmonEcole et AmonEcoleEclair.

Sur ces modules, les autorisations d'accès réseau sont à déclarer dans un modèle ERA[p.761].

Pour plus d'informations, vous pouvez consulter les exemples de configuration fournis dans :

`/usr/share/doc/mysql-server-5.7/examples/`

ou consulter :

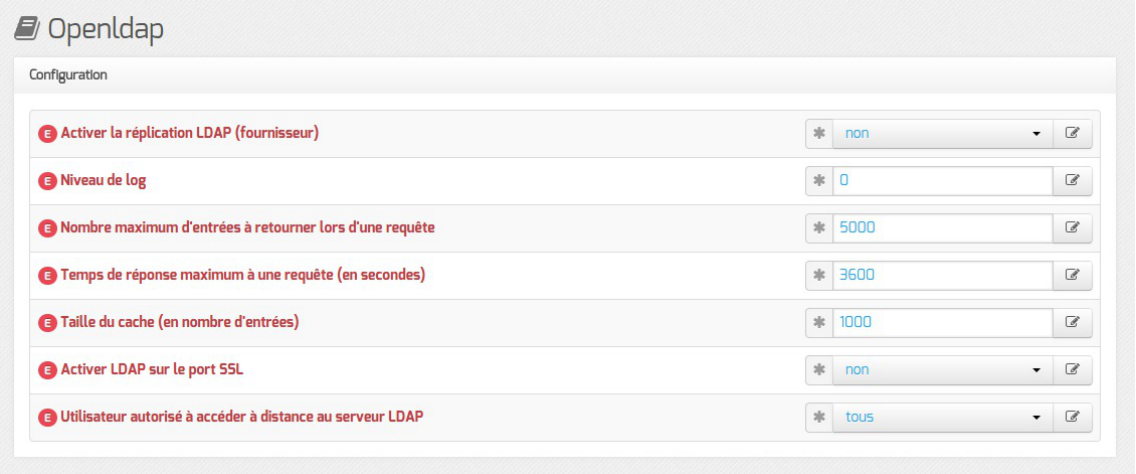
https://dev.mysql.com/doc/refman/5.7/en/

4.28. Onglet Openldap : Configuration du serveur LDAP local

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

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

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



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

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

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

Activer la réplication LDAP (fournisseur)

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

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

Niveau de log

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

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

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

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

La valeur par défaut est de `5000` entrées.

Temps de réponse maximum à une requête (en secondes)

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

La valeur par défaut est de `3600` secondes.

Taille du cache (en nombre d'entrées)

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

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

La valeur par défaut est de `1000` entrées.

Activer LDAP sur le port SSL

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



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

Utilisateur autorisé à accéder à distance au serveur LDAP

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

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



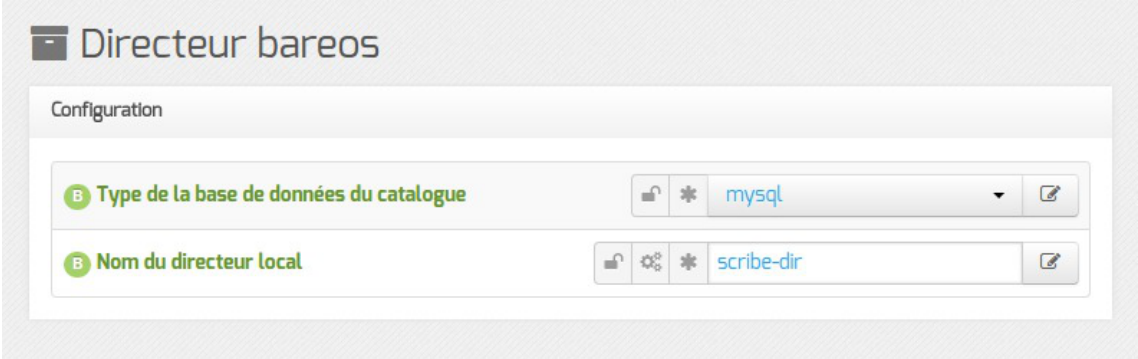
Pour plus d'informations, vous pouvez consulter la page de manuel :

```
# man slapd.conf
```

ou

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

4.29. 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.

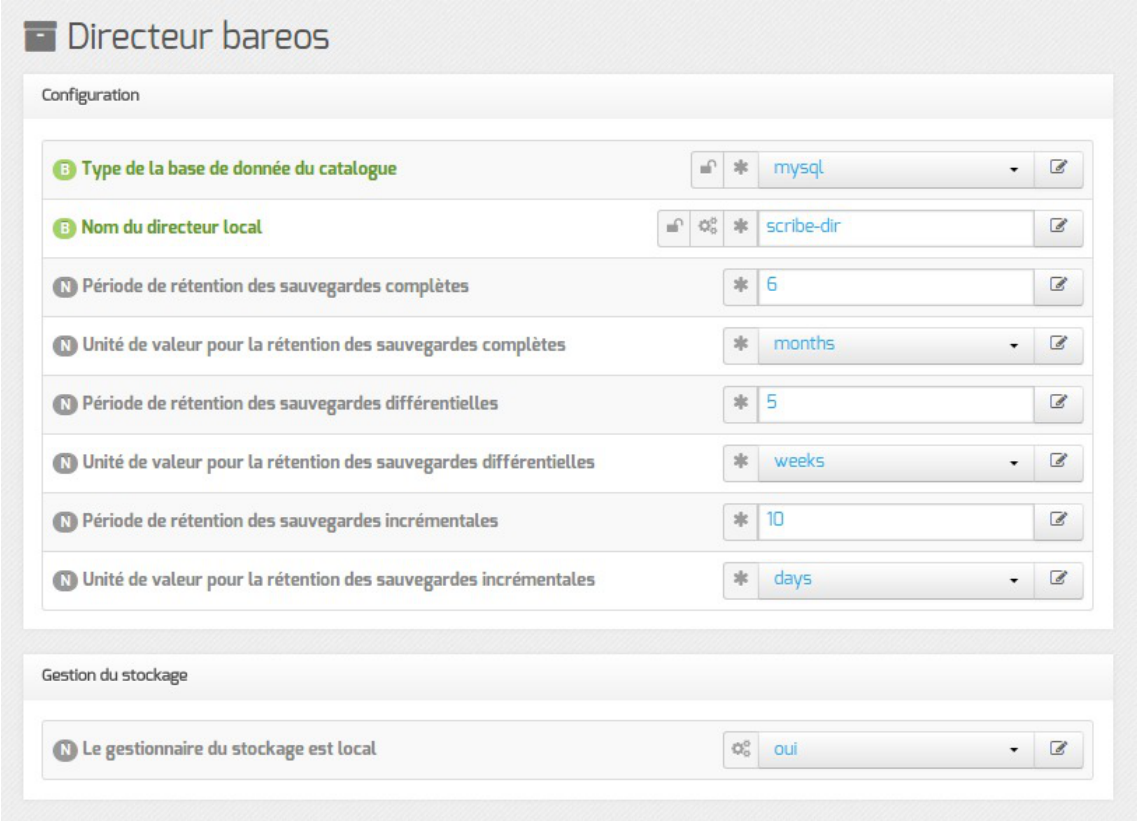


Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

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

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.759] 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 ;

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

- 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.

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.

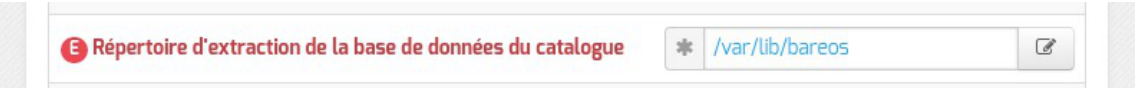
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

Le déport du service `bareos-sd` sur un autre serveur que `bareos-dir` ne permet pas de

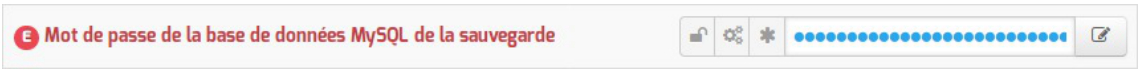
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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

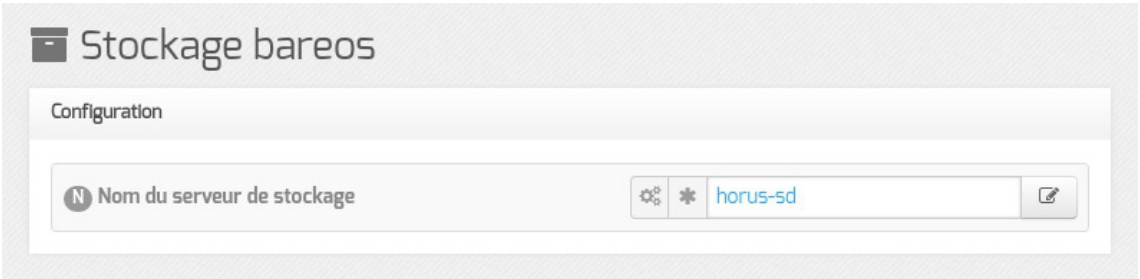
La durée maximale pour l'exécution complète d'une sauvegarde permet d'arrêter le job après un temps d'exécution fixé en seconde, par défaut le job est limité à 86 400 secondes soit 24 heures (la valeur 0 lève cette limite de temps).

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

4.30. 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.

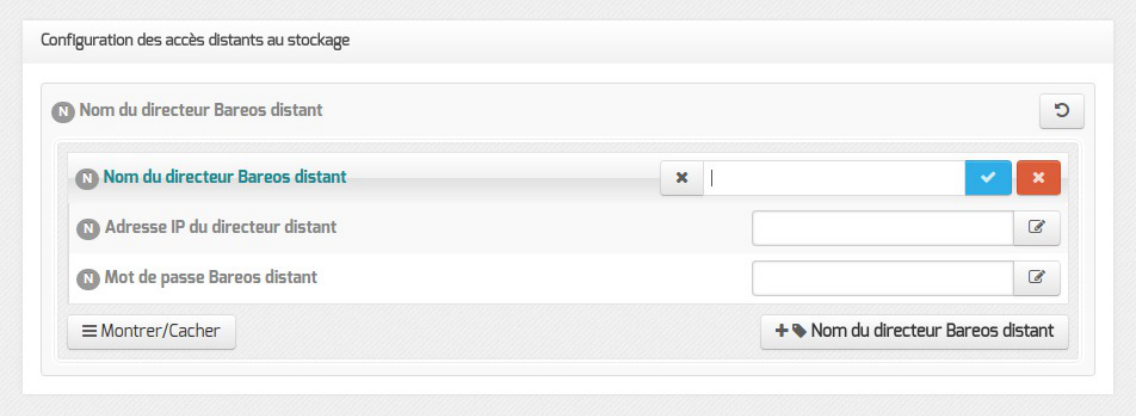


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.344]

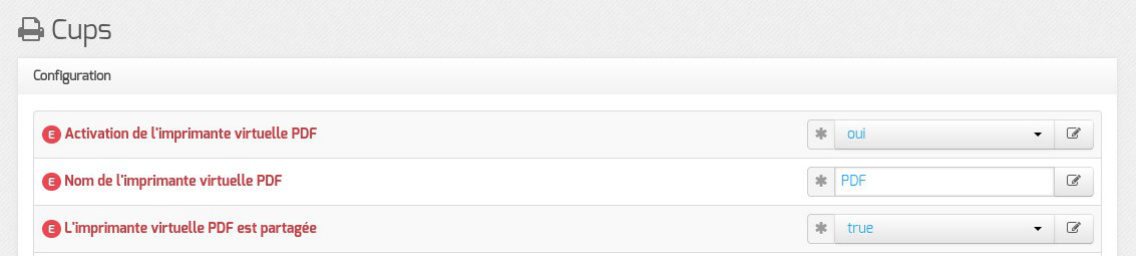
4.31. Onglet Cups : Configuration du serveur d'impression

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`.

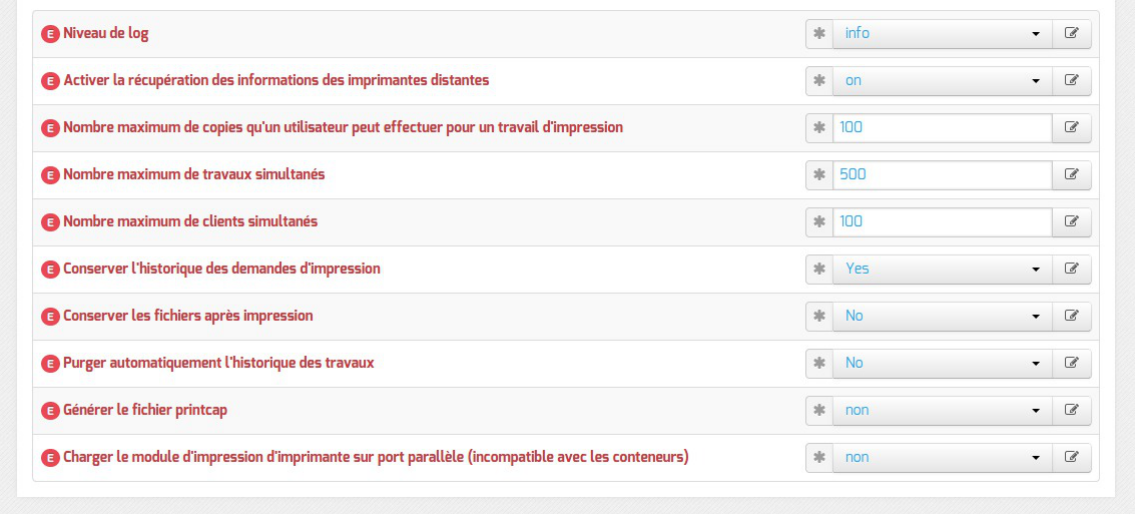
L'onglet `Cups` apparaît en mode expert uniquement si le service est activé.

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



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

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 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.

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

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` :

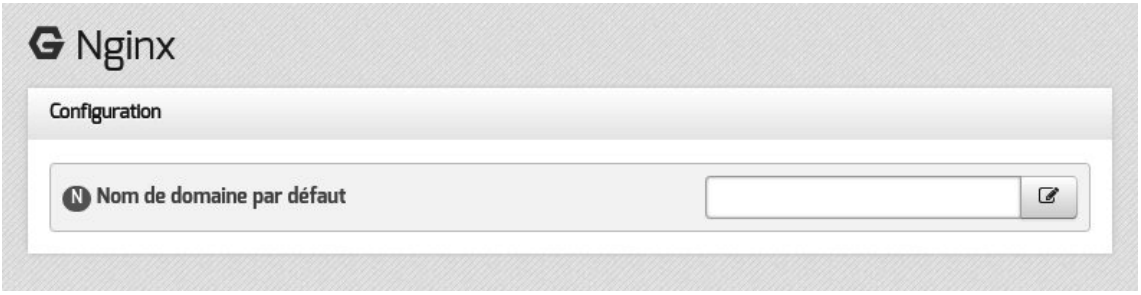
```
# man cupsd.conf
```

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

4.32. 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.

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



Dégrader la sécurité en HTTP

Il est possible de dégrader la sécurité du service Nginx en désactivant l'utilisation du HTTPS.

Si le protocole HTTPS est désactivé, certaines applications critiques publiées par Nginx telles que l'outil d'administration EAD3 ou l'interface de configuration du module ne seront plus disponibles.

Longueur maximum pour un nom de domaine

Sur une installation recevant de très nombreuses connexions, diminuer la valeur de la `Longueur maximum pour un nom de domaine` (server_names_hash_bucket_size) pourra améliorer les performances du proxy inverse. La valeur optimale varie d'une installation à l'autre.

Avec une valeur trop basse, le service Nginx refusera de démarrer et affichera un message d'erreur ressemblant à :

`could not build the server_names_hash, you should increase server_names_hash_bucket_size: 32`

Nginx Optimization : http://nginx.org/en/docs/http/server_names.html#optimization

Taille maximale des données reçues par la méthode POST

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

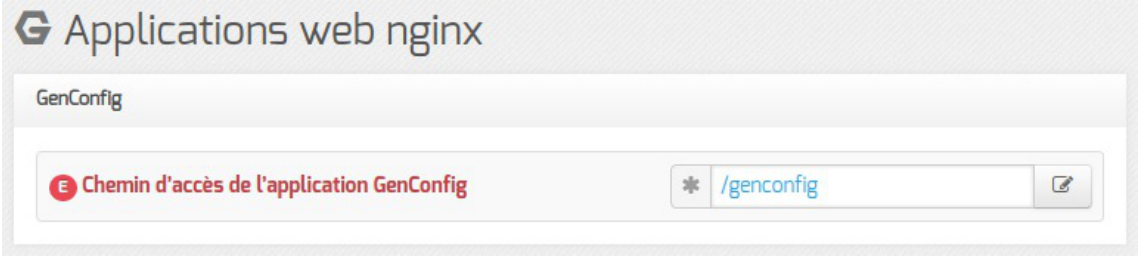
Dans le cas où, sur un module, le service `eole-web` est installé en plus du service `eole-reverseproxy` (ce qui est le cas sur les modules AmonEcole), le paramétrage de cette option s'effectue dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

4.33. 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 we`b

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

`par Nginx` doit également être à `oui` ce qui est le cas par défaut.



Le chemin d'accès des applications activées est personnalisable.

4.34. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.771].

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.758] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.779].

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.765]/*DNAT*.

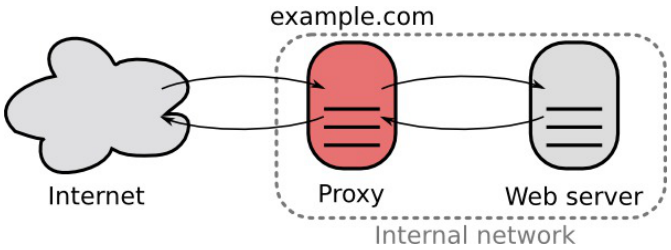
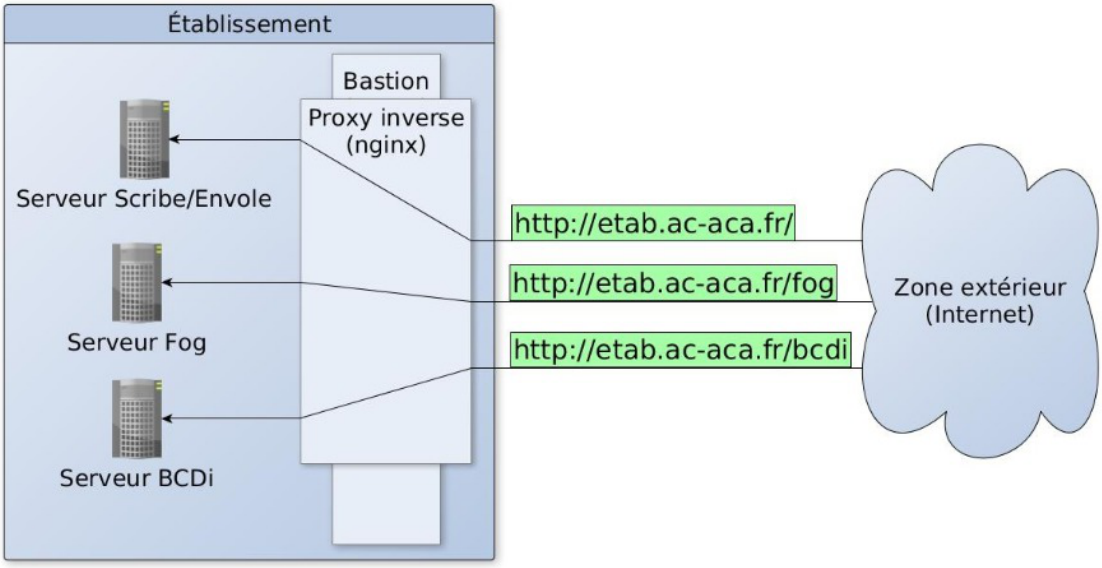


Diagramme d'un proxy inverse - Licence CC0

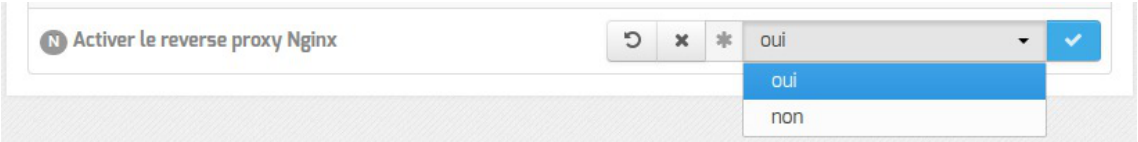
Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD[p.759] ;
- application EOP ;
- protocole HTTP[p.764] ;
- protocole HTTPS[p.764].

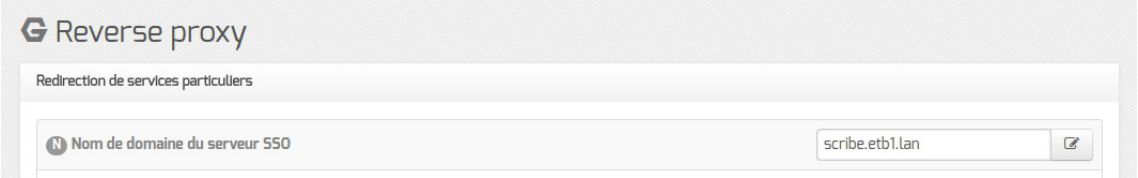
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

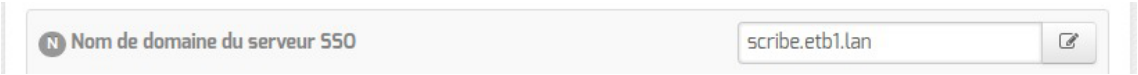


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

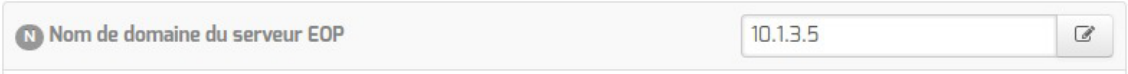
Redirection du service EoleSSO



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

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

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.783]).

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).

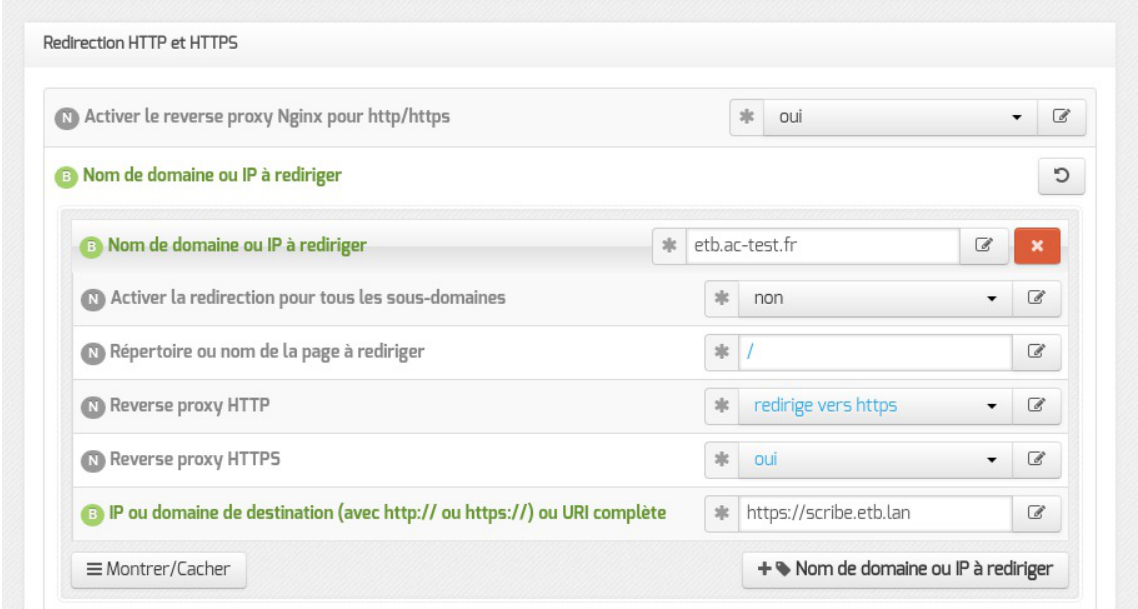
Redirection de l'interface d'administration EAD



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



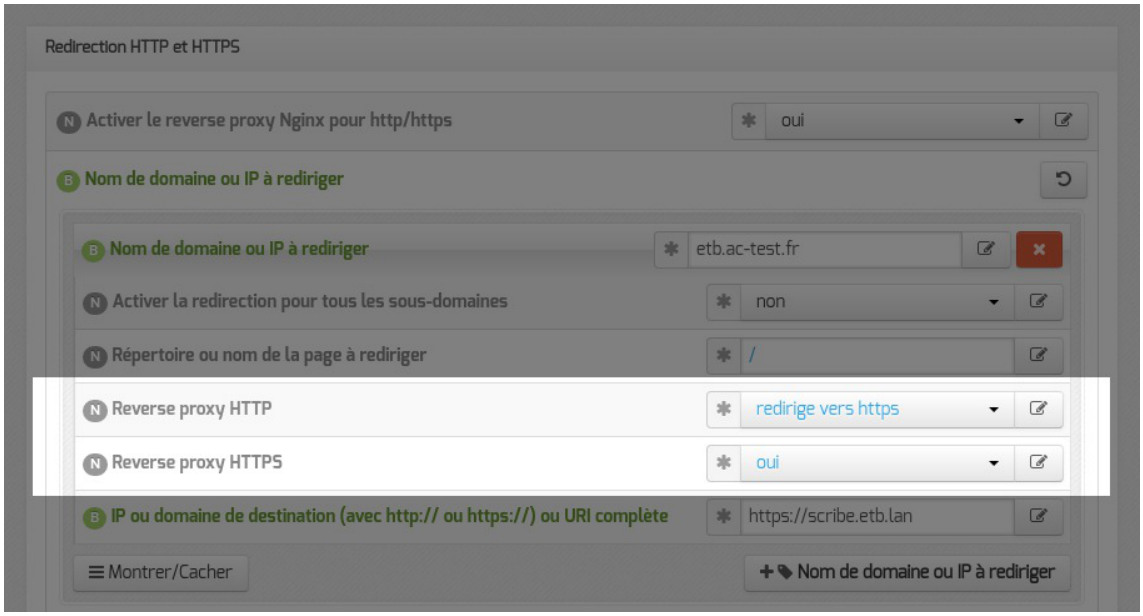
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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.783] (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`.

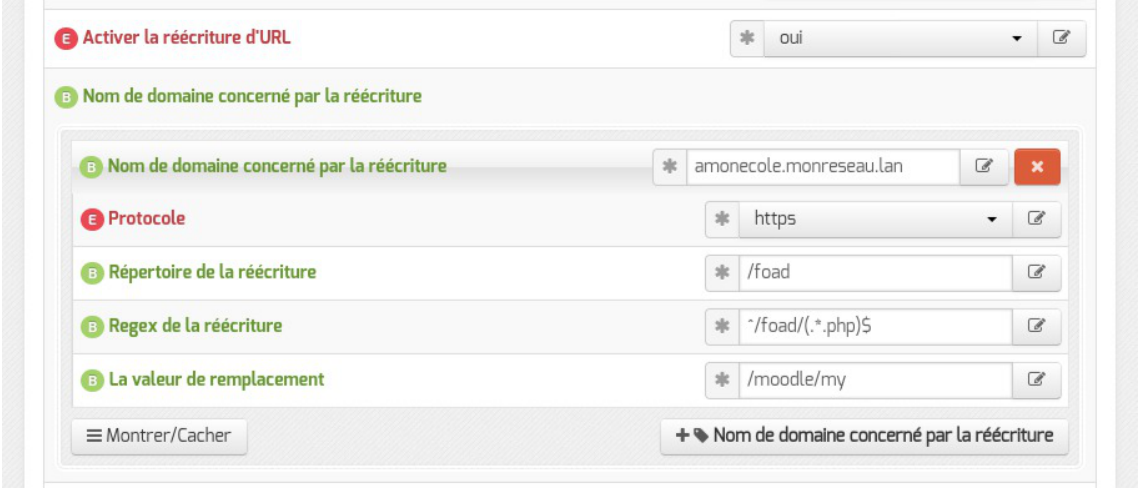


> Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.775], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Réécriture d'URL

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

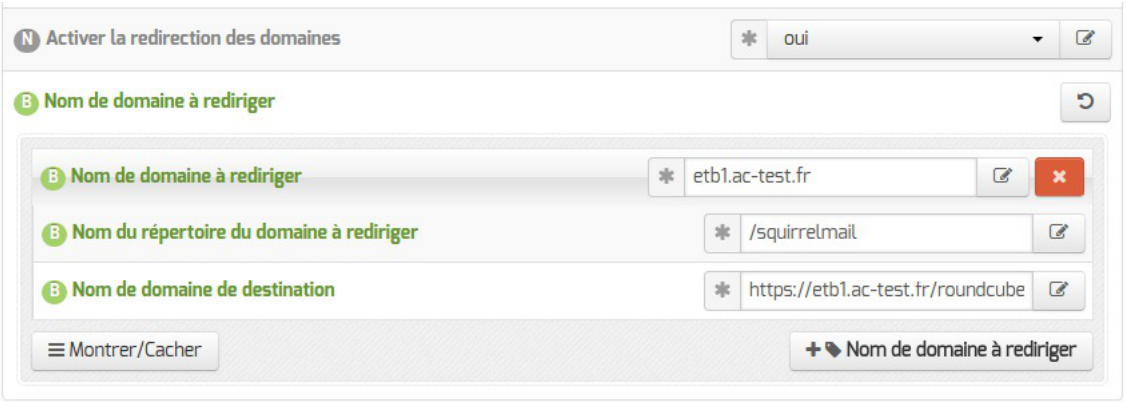
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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/`.

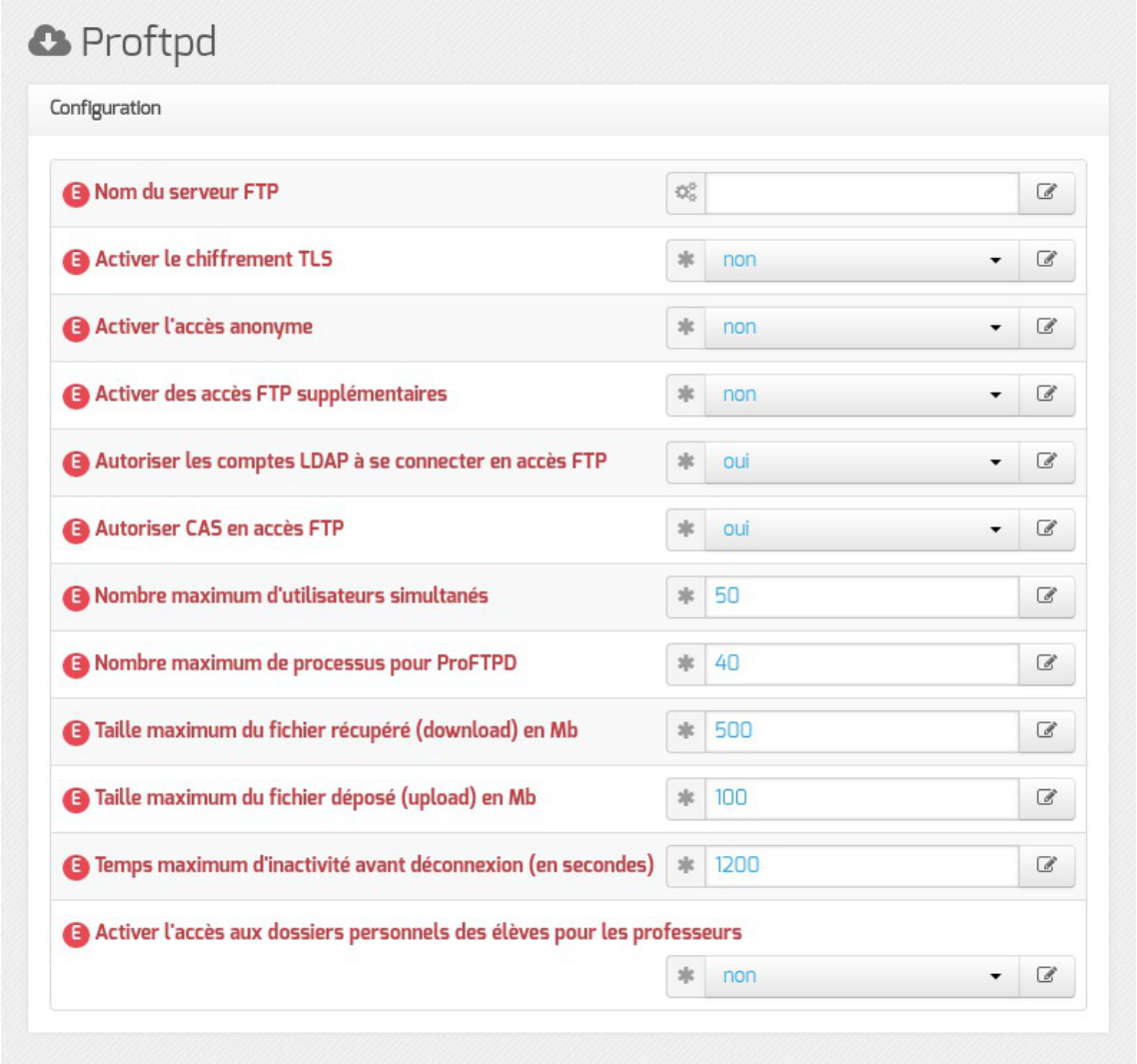
4.35. Onglet Proftpd : Configuration du serveur FTP

Le serveur FTP est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option `Activer l'accès FTP`. Le serveur FTP est basé sur le logiciel libre ProFTPD.

http://www.proftpd.org/

L'onglet `Proftpd` n'apparaît en mode expert que si le service est activé.

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



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

Paramétrage du serveur ProFTPD

Nom du serveur FTP

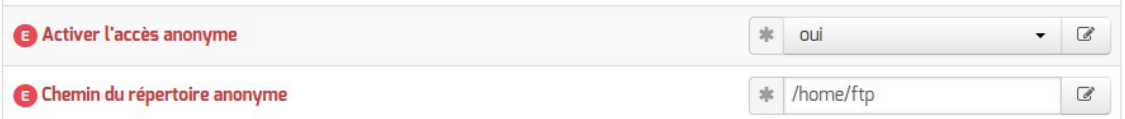
Ce paramètre permet de personnaliser le nom du serveur FTP. Ce nom apparaît lorsqu'on se connecte en FTP sur le serveur avec un client ou en ligne de commande.

Activer le chiffrement TLS

Passer cette option à `oui` permet d'activer le chiffrement TLS mais son utilisation est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

Activer l'accès anonyme

L'accès anonyme permet d'ouvrir l'accès en anonyme sur le répertoire de votre choix.



Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire anonyme` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas. L'utilisateur `anonymous` peut télécharger depuis le répertoire spécifié, il n'a pas par défaut les droits d'écriture.

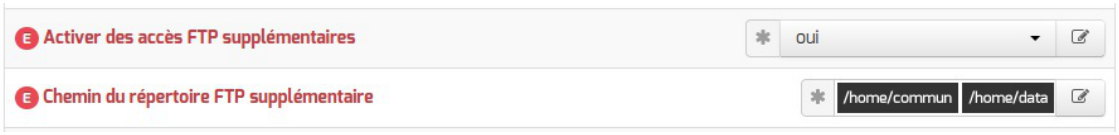
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le fichier de configuration contient la directive `<Limit WRITE>` :

```
<Limit WRITE>
DenyAll
</Limit>
```

Activer des accès FTP supplémentaires

L'accès FTP supplémentaire permet d'ouvrir l'accès à des comptes existants sur le répertoire de votre choix.



Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire FTP supplémentaire` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas et les droits doivent être ajustés. Les utilisateurs du module peuvent lire et écrire dans le répertoire spécifié.

Autoriser CAS en accès FTP

Cette option doit être activée pour l'utilisation de l'application Pydio sur le serveur.

Nombre maximum d'utilisateurs simultanés

Par défaut à `50` cette variable permet d'ajuster le nombre d'utilisateurs simultanés autorisés à se connecter en FTP.

Nombre maximum de processus pour ProFTPD

Par défaut à `40` cette variable permet d'ajuster le nombre maximum de processus simultanés du logiciel ProFTPD.

Taille maximum du fichier récupéré (download) en Mb

Par défaut à `500` cette variable permet d'ajuster la taille maximum des fichiers pouvant être téléchargés.

Taille maximum du fichier déposé (upload) en Mb

Par défaut à `100` cette variable permet d'ajuster la taille maximum des fichiers pouvant être déposés.

Temps maximum d'inactivité avant déconnexion (en secondes)

Par défaut à `1200` secondes (20 minutes) cette variable permet d'ajuster le temps d'inactivité avant déconnexion.

Accès FTP

Une fois l'accès FTP activé, il est possible d'accéder au service avec un client FTP (Filezilla, gFTP), par un navigateur web ou avec une application web FTP (Pydio, anciennement Ajaxplorer, sur le module Scribe).

Accès par un navigateur web

Pour accéder aux documents avec un navigateur web il faut préciser le protocole dans l'URL :

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

`ftp://user@<adresse_serveur>/`

ou

`ftp://<adresse_serveur>/`

Accès par une application web

Pour accéder aux fichiers par l'application web Pydio, il faut l'activer dans l'onglet `Applications web`. Pydio (anciennement Ajaxplorer) n'est pas pré-installé sur le module Horus (il s'installe avec la commande `apt-eole`, voir la documentation sur les applications web). Suite à une reconfiguration du serveur, l'application sera accessible à l'adresse `http://<adresse_serveur>/pydio/` moyennant l'authentification (mire EoleSSO).



Avec un client FTP (en mode passif par défaut) le mode actif doit impérativement être configuré. Dans ce mode c'est le client FTP qui détermine le port de connexion à utiliser.

Interdire l'accès FTP à des comptes utilisateur

Le fichier `/etc/ftpusers` contient une liste des utilisateurs qui ne doivent pas se connecter via le service FTP. Ce fichier est utilisé non seulement pour l'administration système mais également pour augmenter la sécurité du réseau. Il contient typiquement la liste des utilisateurs qui, soit n'ont rien à faire avec le transfert FTP, soit ont trop de privilèges pour être autorisés à se connecter au serveur. De tels utilisateurs sont en général `root`, `daemon`, `bin`, `uucp` et `news`.

La liste du fichier `/etc/ftpusers` peut être complétée avec des utilisateurs systèmes ou LDAP dont il faut désactiver l'accès au service FTP.



Attention lors des accès FTP, le mot de passe transite en clair sur le réseau.

Anti-virus ClamAV

Si l'anti-virus ClamAV est activé, la recherche de virus en temps réel sur le FTP est activé par défaut. Il est possible de désactiver cette option dans l'onglet `Clamav` en passant `Activer l'anti-virus temps réel sur FTP` à `non`.

Accès au dossier personnel des élèves par FTP

Sur les modules Scribe et AmonEcole, les professeurs n'ont, par défaut, pas accès au dossier personnel de leurs élèves par l'intermédiaire du protocole FTP.

Cette restriction peut être levée en répondant `oui` à la question `Activer l'accès aux dossiers personnels des élèves pour les professeurs`. Cette option diminue légèrement la sécurité du serveur.

4.36. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de

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

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 :

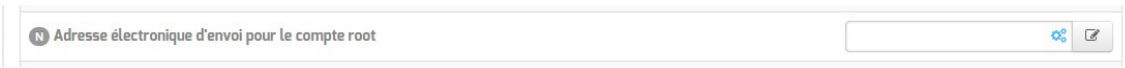
- `Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)`, saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-` ;
- `Adresse électronique recevant les courriers électroniques à destination du compte root`, permet de configurer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



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: »).

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

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. 756] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

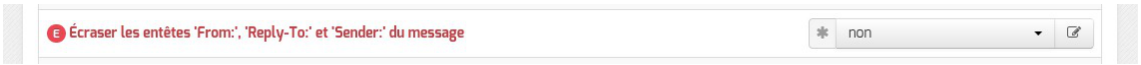
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

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

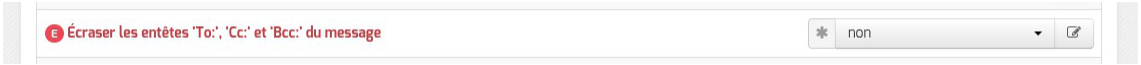
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

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

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



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



Réécriture de l'expéditeur :

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

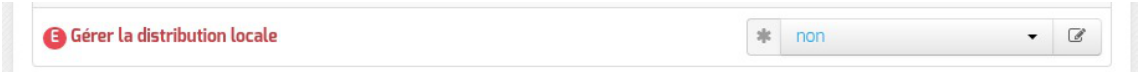
Réécriture du destinataire :

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

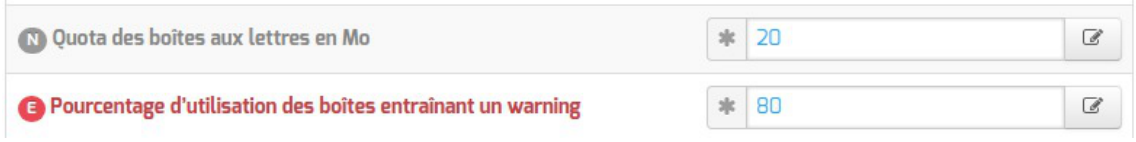
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Bcc :	user@conteneur.machine.domaine	system_mail_to

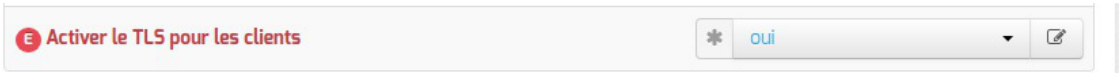
Par défaut, la distribution locale des messages est désactivée, sauf sur les modules Scribe et AmonEcole sur lesquels cette variable est masquée.



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.781] pour l'envoi de message est activé par défaut. La commande StartTLS[p.779] est supportée sur le port 25 (la connexion est initiée en mode non chiffré) et permet de basculer en TLS sur le port 465.

Passer cette variable à `non` rend l'authentification SMTP impossible ce qui empêche les utilisateurs d'envoyer des messages.

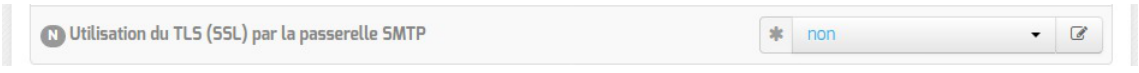
Relai des messages



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

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

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



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

`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.781] pour l'envoi de message. Si la passerelle SMTP[p.778] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.779] (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`
  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,

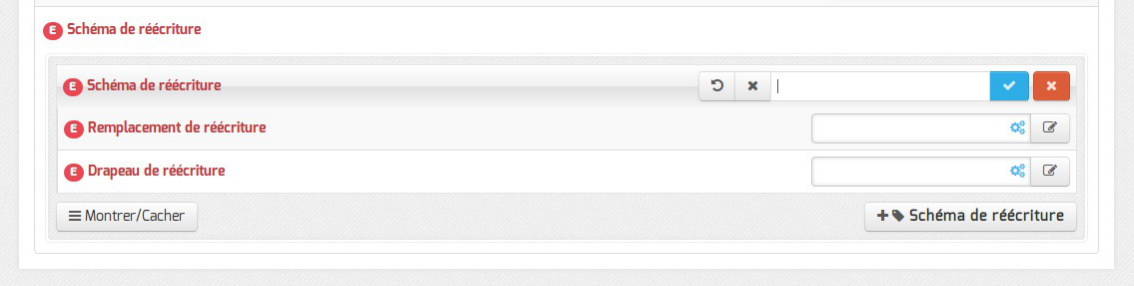
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

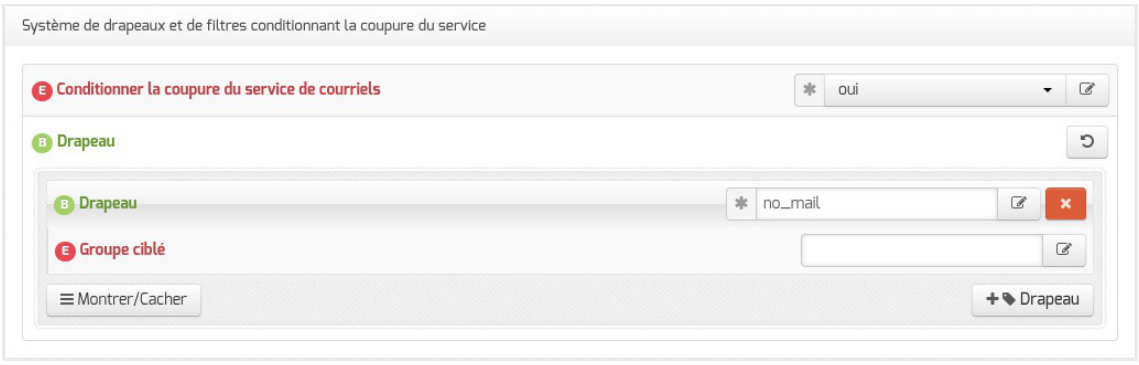
Fermeture de la messagerie

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`.



- `Drapeau` : nom du fichier qui sera recherché dans le répertoire `/var/run/eole/flags` par le serveur de courriels.

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

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.

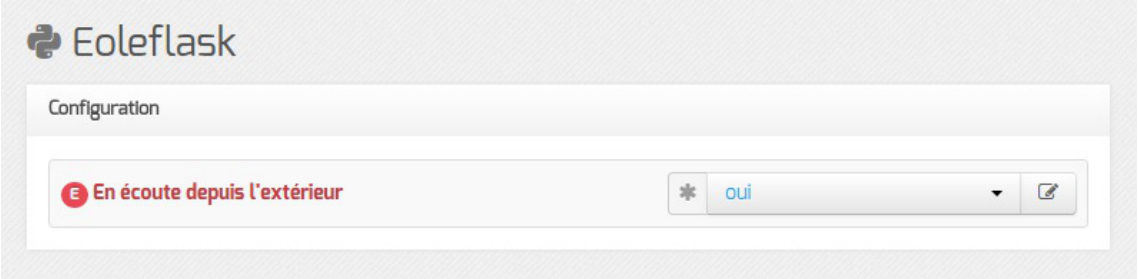


Sur EOLE 2.6.2, la création du drapeau n'est pas gérée automatiquement et le dossier `/var/run/eole/flags` n'existe pas par défaut.

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

4.37. Onglet Eoleflask

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



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

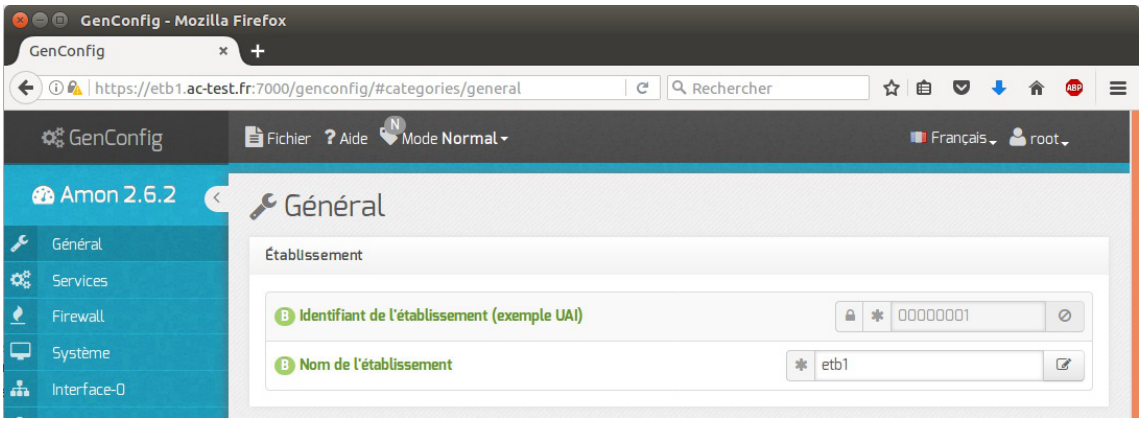
Accès distant (port 7000)

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

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

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

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

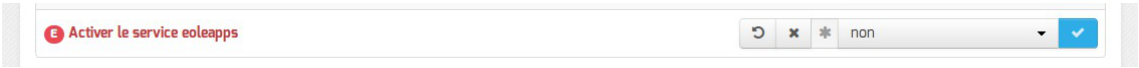


Vue de l'interface de configuration au travers d'un navigateur web (port 7000)

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

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.

Serveur d'applications



Si le le serveur web Apache est activé dans l'onglet Services, la variable supplémentaire Activer le service eoleapps apparait.

La passer à oui permet d'activer et d'utiliser le serveur d'applications flask[p.762] EOLE.

L'installation d'une application utilisant Eoleflask (EOP par exemple) active automatiquement le service eoleapps.

Activer manuellement le service eoleapps permet de mettre à disposition vos propres applications le service Eoleflask.

5. Prise en charge d'applications supplémentaires

Les modules Scribe, Horus, Seshat et AmonEcole fournissent tous les éléments nécessaires à l'installation d'applications web indépendamment de celles pré-configurées.

Les exemples sont basés sur l'installation du logiciel EGroupware mais sont facilement transposables pour l'installation de n'importe quelle application PHP/MySQL.

EGroupware est un logiciel collaboratif professionnel. Il vous permet de gérer vos contacts, vos rendez-vous, vos tâches, et bien plus pour toute votre activité.

http://www.egroupware.org/

Mode conteneur

L'installation d'applications sur les modules configurés en mode conteneur est plus complexe.

Certaines étapes de la mise en place diffèrent selon le mode, conteneur ou non conteneur.

Dans les exemples ci-dessous les modules Scribe et Horus sont en mode non conteneur et AmonEcole en mode conteneur.

5.1. Téléchargement et mise en place

Installation des fichiers

Pour télécharger une archive sur le module, il faut utiliser la commande wget :

```
# wget downloads.sourceforge.net/project/egroupware/eGroupware-14.2/eGroupware-14.2
```


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

Il faut ensuite décompresser l'archive à l'aide de la commande `tar` (ou `unzip`, pour le format zip) :

```
# tar xzvf egroupware-epl-14.2.20150310.tar.bz2
```

Dans cet exemple, cela créera le répertoire `egroupware`

Ensuite, il faut envoyer les fichiers dans le répertoire de destination, soit :

- sur les modules Scribe ou Horus :

  ```
  # cp -r egroupware /var/www/html/egroupware
  ```

- sur un module Horus dépourvu d'application web :

  ```
  # mkdir /var/www/html
  # cp -r egroupware /var/www/html/egroupware
  ```

- sur le module AmonEcole :

  ```
  # cp -r egroupware /opt/lxc/reseau/rootfs/var/www/html/egroupware
  ```

Affectation de droits

La plupart des applications nécessitent que l'utilisateur utilisé par le service Apache (ici, l'utilisateur système : ***`www-data`***) ait le droit d'écrire en certains endroits du disque.

Le propriétaire d'un fichier ou d'un répertoire se modifie à l'aide de la commande `chown` :

- sur les modules Scribe/Horus :

  ```
  # chown -R www-data: /var/www/html/egroupware
  # chmod 770 /var/www/html/egroupware
  ```
  (le temps de l'installation)

- sur le module AmonEcole :

  ```
  # ssh reseau
  # chown -R www-data: /var/www/html/egroupware
  # chmod 770 /var/www/html/egroupware
  ```
  (le temps de l'installation)

  `# ctrl + d` pour sortir du conteneur



Donner trop de droits à l'utilisateur ***`www-data`*** diminue la sécurité du serveur.

Consulter la documentation du logiciel pour n'attribuer que les droits nécessaires au fonctionnement de l'application.

Installation de paquets

Certaines applications nécessitent également des modules apache ou d'autres logiciels qui ne sont pas forcément présents sur le serveur.

Dans la majeure partie des cas, les éléments manquants sont disponibles en tant que paquet de la distribution.



Installation du paquet php5-imap

- sur les modules Scribe ou Horus :

  ```
  # apt-eole install php5-imap
  ```

- sur le module AmonEcole :

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

```
# apt-eole install-conteneur web php5-imap
```

Voir aussi...

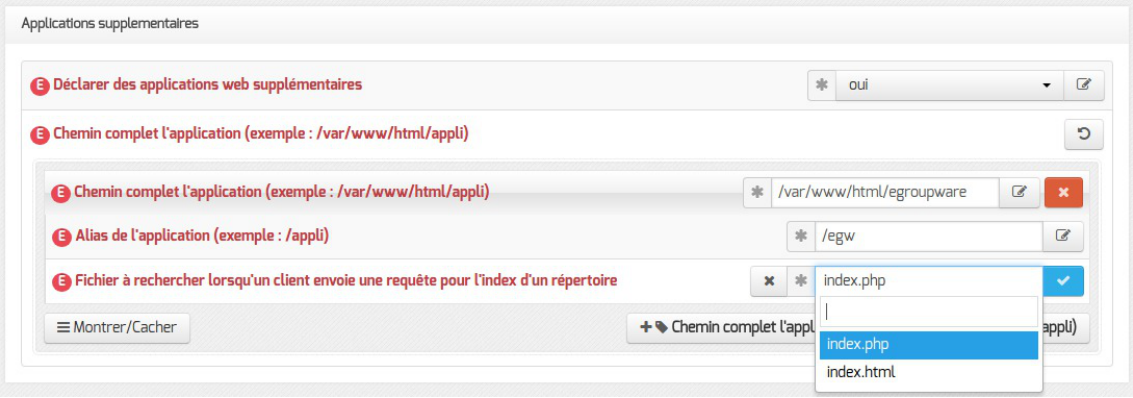
Installation manuelle de paquets [p.439]

5.2. Configuration Apache

Méthode Creole

Dans l'interface de configuration du module :

- aller dans l'onglet `Apache` en mode expert ;
- indiquer le chemin complet de l'application et l'alias de l'application `/var/www/html/egroupware` ;
- indiquer le chemin de l'alias de l'application `/egw` ;



Déclaration d'une application web dans gen_config

- enregistrer la configuration et quitter ;
- lancer la commande `reconfigure` ;
- le logiciel doit répondre à l'adresse : `http://<adresse serveur>/egw`

Le fichier de configuration apache pour cette application est `/etc/apache2/sites-available/eole`

La directive `php admin flag allow url fopen` On est nécessaire au bon fonctionnement d'EGroupware.

Méthode manuelle

- créer le fichier de configuration apache nommé `egroupware`
  - sur les modules Scribe ou Horus : `/etc/apache2/sites-available/egroupware.conf`
  - sur le module AmonEcole : `/opt/lxc/reseau/rootfs/etc/apache2/sites-available/egroupware.conf`

```
# Exemple basique de configuration de site #
```


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

```
Alias /egw /var/www/html/egroupware
<Directory "/var/www/html/egroupware">
    php admin flag allow url fopen On
    AllowOverride None
    DirectoryIndex index.php
    Order Allow,Deny
    Allow from All
</Directory>
```

- activer l'application à l'aide de la commande :
  `# CreoleRun "a2ensite egroupware" web`
- recharger la configuration d'Apache à l'aide de la commande CreoleService[p.757] :
  `# CreoleService apache2 reload`
- le logiciel doit répondre à l'adresse : ***http://<adresse serveur>/egw***

> Pour obtenir une configuration apache optimale, consulter la documentation de l'application.
> En cas de problème, consulter le fichier de journal /var/log/rsyslog/local/apache2/apache2.err.log
> Dans le cas d'EGroupware, il est nécessaire de supprimer le fichier ***.htaccess*** situé dans le répertoire racine du logiciel :
> `# rm -f /var/www/html/egroupware/.htaccess`
> La directive `php admin flag allow url fopen On` est également nécessaire au bon fonctionnement d'EGroupware.

5.3. Configuration MySQL

Méthode EOLE

Utiliser le script mysql_add.py :

```
Nom de la base de données à créer : egroupware
Nom de l'utilisateur MySQL administrant la base : egroupware
Mot de passe de l'utilisateur Mysql administrant la base : pwdsecret
## Création de la base egroupware ##
```

> Sur le module AmonEcole, il y a une question supplémentaire :
> `Nom du conteneur source : web`
> En répondant ***web*** cela permet que les requêtes vers MySQL soient autorisées depuis le conteneur dans lequel se trouvent les applications web.

Méthode semi-manuelle

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

- utiliser le script `mysql_pwd.py` ;
- réinitialiser le mot de passe `root` de MySQL à la valeur de votre choix ;
- utiliser l'interface de phpMyAdmin pour faire les manipulations nécessaires.



Il est recommandé de créer un utilisateur et une base MySQL spécifiques par application.

Sur le module AmonEcole, il faudra veiller à ce que l'utilisateur MySQL utilisé ait le droit d'accéder à la base de données depuis l'adresse IP du conteneur web, en l'occurrence `192.0.2.51`.

5.4. Configuration du logiciel

Vous pouvez maintenant utiliser le système automatique d'installation du logiciel disponible à l'adresse : `http://<adresse serveur>/egw`

Un `/install` ou `/config` sera à ajouter au chemin en fonction de l'application à installer.



Sur le module AmonEcole, l'adresse de la base de données à mettre dans l'interface de configuration de l'application est celle du conteneur `bdd` (`192.0.2.50`) et non `localhost`.

Affectation de droits après l'utilisation du système automatique d'installation du logiciel

Changer les droits d'accès :

```
# chmod 750 /var/www/html/egroupware
```

Changer le propriétaire des fichiers :

```
# chown -R root :www-data /var/www/html/egroupware
```

Authentification CAS

Informations utiles à la configuration d'une authentification CAS :

- adresse du serveur CAS : adresse IP (ou nom DNS) de votre module EOLE
- port d'écoute par défaut du serveur CAS : 8443 (CAS EOLE)
- URI sur le serveur CAS : *rien*
- Destination après la sortie : *rien*



Par défaut EoleSSO, fournit uniquement l'identifiant de l'utilisateur.

Pour chaque application, il est possible d'ajouter des filtres définissant des attributs supplémentaires à fournir.

Pour plus d'informations, consulter la documentation EoleSSO.

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

Authentification LDAP

Informations utiles à la configuration d'une authentification LDAP :

- adresse du service LDAP :
  - sur le module Scribe/Horus : adresse IP (ou nom DNS) de votre module EOLE
  - sur le module AmonEcole : adresse IP du conteneur bdd : `192.0.2.50`
- port d'écoute du serveur LDAP : 389 (port standard)
- base DN : o=gouv,c=fr



La majeure partie des informations stockées dans l'annuaire est accessible par des requêtes anonymes.

Si l'application a besoin d'accéder à des attributs LDAP protégés par une ACL[p.752] et non fournis par EoleSSO, il est possible d'utiliser le compte spécial `cn=reader,o=gouv,c=fr` dont le mot de passe est stocké dans le fichier `/root/.reader`

Voir aussi...

Utilisateurs spéciaux

Définition de filtres d'attributs

6. Authentification unique avec EoleSSO

6.1. Présentation du produit EoleSSO

Description du produit

EoleSSO est un serveur d'authentification développé pour répondre à la problématique du SSO[p.779] (authentification unique) dans différentes briques de l'architecture EOLE. Il est développé en langage Python à l'aide du framework Twisted[p.781].

Ce produit implémente en premier lieu un serveur d'authentification compatible avec le protocole CAS[p.754].

Une partie du protocole SAML[p.777] a été implémentée par la suite pour permettre de répondre à des problématiques de fédération avec d'autres produits (ou entre 2 serveurs EoleSSO).

Ce document décrit la configuration, l'administration et l'utilisation du serveur EoleSSO.

Principe de fonctionnement général

La gestion du Single Sign On[p.779] (SSO) dans EoleSSO est basée sur le protocole CAS[p.754].

Le principe est que l'utilisateur fournit ses identifiants sur la page d'authentification du service EoleSSO. Une fois les identifiants validés, le service pose un cookie de session SSO dans le navigateur. Ce dernier

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

n'est valide que sur une durée définie.

Tant que le cookie est valide, le service reconnaît automatiquement l'utilisateur à chaque fois qu'une application demandera de vérifier son authentification. Ce système présente plusieurs intérêts : l'utilisateur ne saisit qu'une fois ses identifiants pour se connecter à un ensemble d'applications et celles-ci n'ont jamais accès à ses identifiants réels (La liste des informations envoyées aux applications par le service SSO est configurable par application grâce à un système de filtres).

Le serveur d'authentification possède plusieurs caches de sessions :

- tickets utilisateurs (session SSO) : longue durée, réutilisable. Ces tickets sont la preuve d'authentification de l'utilisateur et sont stockés dans un cookie sécurisé dans le navigateur de l'utilisateur ;
- tickets d'application : courte durée (5 minutes par défaut), utilisable une seule fois et pour une seule application.

  Ces tickets sont également utilisés pour mémoriser une session de fédération avec un autre système (se reporter aux chapitres traitant de la fédération d'identité).

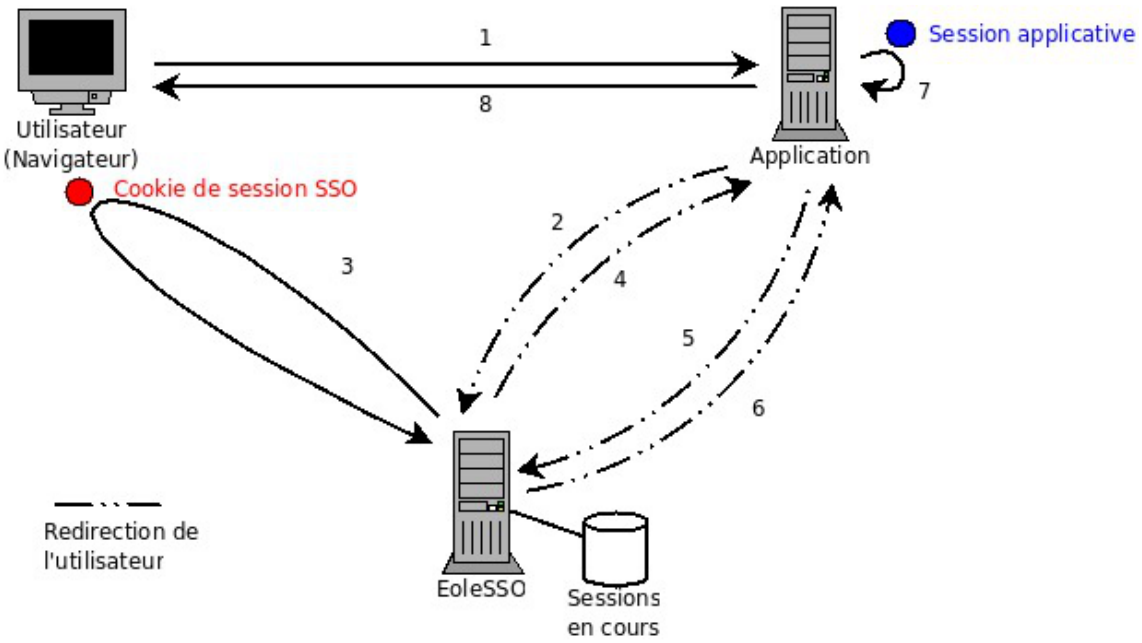
Les applications clientes n'ont pas accès à l'identifiant de la session utilisateur, il est échangé uniquement entre le serveur d'authentification et le navigateur.

Une fois qu'une application a obtenu un ticket, elle peut utiliser de façon classique une session interne pour ne pas surcharger le serveur par des appels trop nombreux.



La session SSO étant gérée par un cookie placé dans le navigateur du client, celui-ci doit être configuré pour accepter les cookies.

Déroulement de l'accès à une application via EoleSSO



1. L'utilisateur accède à une page d'une application (service) configurée pour utiliser le système SSO (application utilisant un client CAS).
2. L'application redirige l'utilisateur sur le serveur SSO en passant une URL de retour (paramètre `service`). Le serveur SSO vérifie qu'un cookie de session est présent et qu'il correspond à une

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

session valide.

3. Si ce n'est pas le cas, il demande à l'utilisateur de saisir ses identifiant et mot de passe pour établir une nouvelle session SSO.
4. Une fois la session validée, le serveur SSO génère un ticket d'application valable pour une courte durée et réservé à l'URL du service. Il redirige alors l'utilisateur sur cette URL en passant le ticket en paramètre.
5. L'application récupère le ticket. Elle redirige l'utilisateur sur l'URL de validation du serveur SSO en passant en paramètre le ticket reçu et son URL de service.
6. Le service SSO vérifie que le ticket est encore valide et correspond à l'URL de service. puis redirige sur l'URL de service en incluant une réponse. Si cette réponse est positive (le ticket est valide), elle contient également des informations sur l'utilisateur (les informations renvoyées dépendent de l'application, se reporter au chapitre traitant des filtres).
7. L'application reçoit la réponse et crée éventuellement une session interne pour l'utilisateur.
8. La page de l'application est renvoyée à l'utilisateur



Le fonctionnement peut être plus complexe dans le cas de l'utilisation du mode proxy pour accéder à des services non web (par exemple, pour accéder à un service IMAP ou FTP).

Se reporter à la description du site officiel du protocole CAS pour plus de détail :

http://www.apereo.org/cas

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

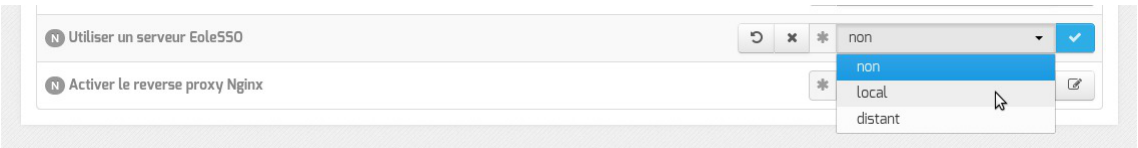
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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

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

Serveur local ou distant

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



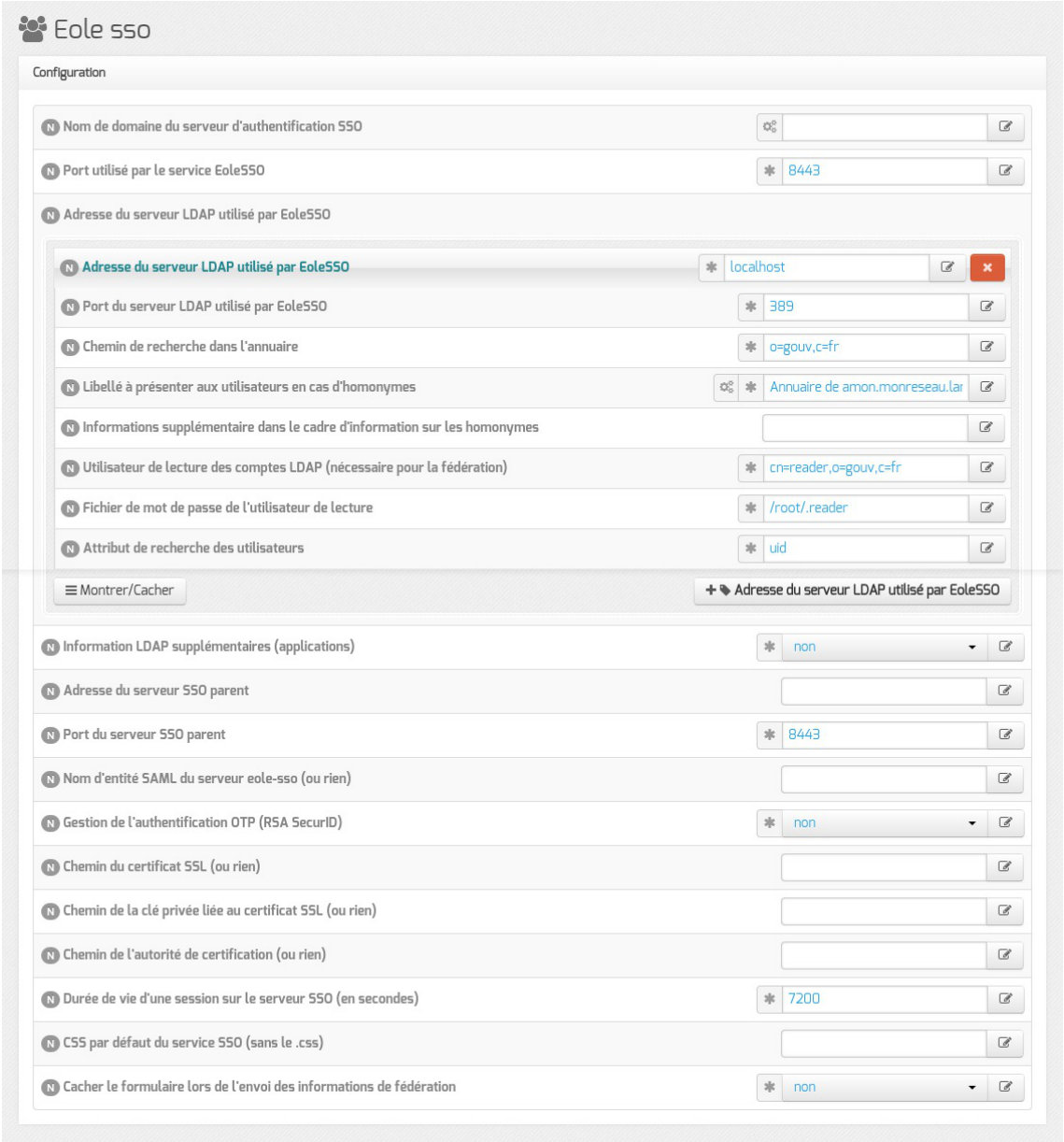
La variable `Utiliser un serveur EoleSSO` permet :

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

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

Adresse et port d'écoute

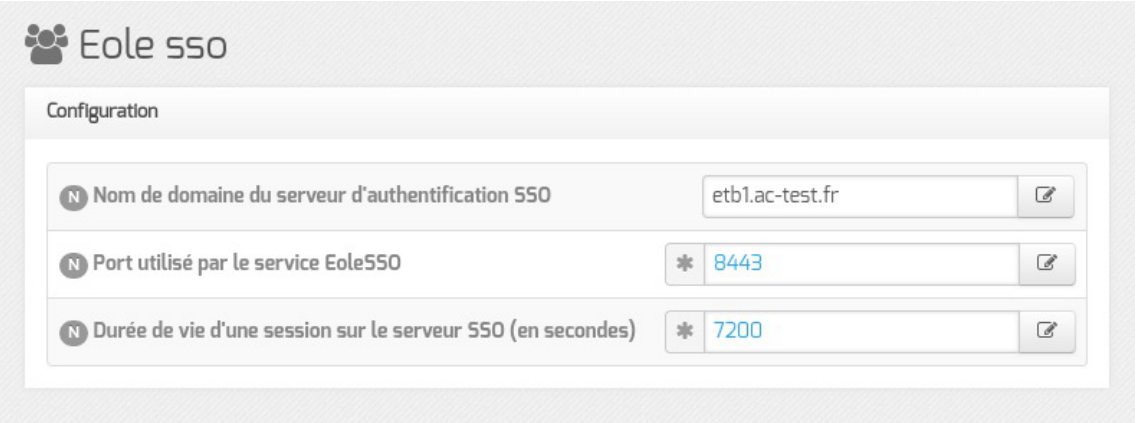
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.



Configuration d'un serveur EoleSSO local

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

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



Configuration d'un serveur EoleSSO distant

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

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

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

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.766] pour authentifier les utilisateurs et récupérer leurs attributs.

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs (basedn) ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN[p.758] et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.773] si disponible *(voir plus loin)*.

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur

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

ayant accès en lecture au serveur LDAP configuré.

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

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

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

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

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

- `Utilisateur de lecture des comptes ldap` : renseignez son *dn* complet dans l'annuaire
- `fichier de mot de passe de l'utilisateur de lecture` : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.784] en HTTPS, sur le port défini pour le serveur EoleSSO).

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

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

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID[p.778] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)

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

- Répondre `oui` à la question `Gestion de l'authentification OTP (RSA SecurID)`

Des champs supplémentaires apparaissent :

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

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation[p.765] du serveur et sont utilisés par défaut.

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

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.777] (version 2).

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

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

Autres options

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

`CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le

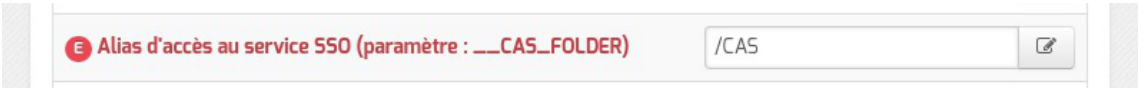
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

Configuration en mode expert

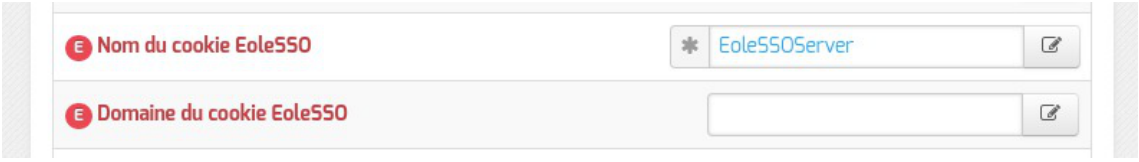
Options générales

En mode expert plusieurs nouvelles variables sont disponibles :

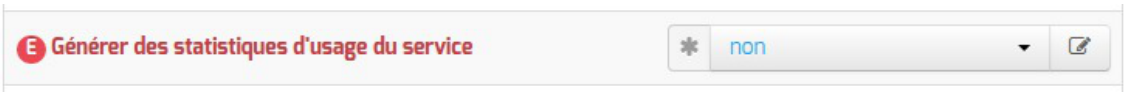


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP[p.767] ou keycloak[p.766].

  Cette variable est disponible uniquement à partir de la version 2.6.2 d'EOLE.

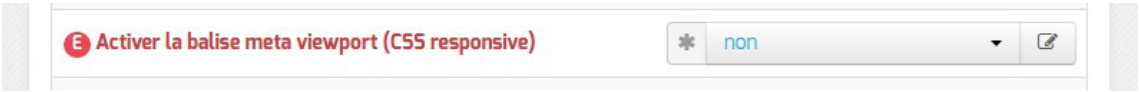


- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.



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

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



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



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

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

- À partir d'EOLE 2.6.2, la variable `Nombre maximum de sessions en attente (backlog)`

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

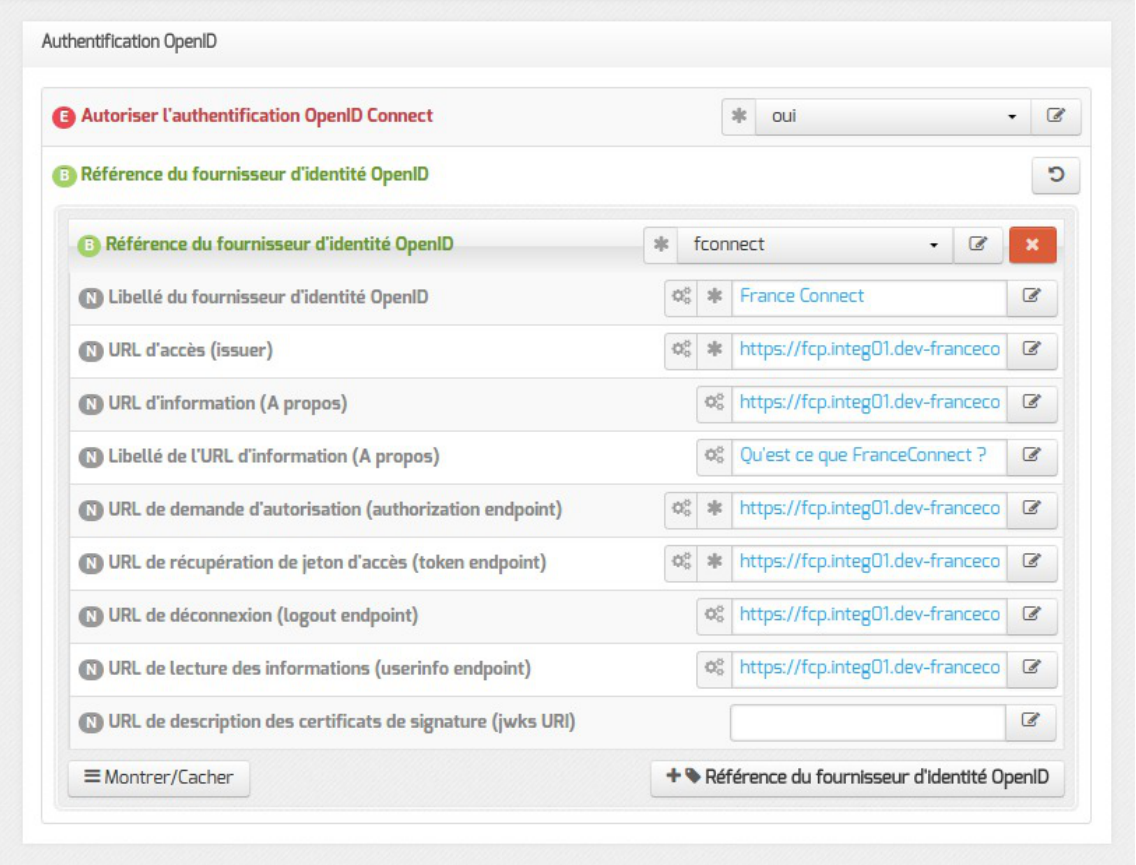
permet de définir la taille de la file d'attente des sessions.

Augmenter cette valeur est susceptible de résoudre des problèmes de lenteur voir de rejet des demandes d'authentification ;

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

  Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;
- `Utiliser l'authentification SSO pour l'EAD` est à `oui` par défaut. Le passer à `non` permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Configuration d'authentification OpenID Connect



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

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - /usr/share/sso/interface/images/<libelle>.png : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;

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

- /usr/share/sso/interface/images/logo-<libelle>.png : logo du fournisseur qui sera affiché sur la page d'association de comptes.

- `Libellé du fournisseur d'identité OpenID` : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- `URL d'accès (issuer)` : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- `URL de demande d'autorisation (authorization endpoint)` : URL permettant au client d'initier le processus d'authentification ;
- `URL de récupération de jeton d'accès (token endpoint)` : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- `URL de déconnexion (logout endpoint)` : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- `URL de lecture des informations (userinfo endpoint)` : URL permettant de récupérer les informations de l'utilisateur à l'aide du jeton fourni ;
- `URL de description des certificats de signature (jwks URI)` : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

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



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

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

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

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

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

Voir aussi...

Gestion des sources d'authentification multiples [p.288]

Compatibilité OpenID Connnect [p.267]

6.3. Protocoles supportés

6.3.1. Compatibilité CAS

Fonctions implémentées au niveau serveur

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



Le serveur EoleSSO implémente le protocole CAS[p.754].

Vous pouvez retrouver la description de ce protocole sur le site officiel du protocole :

http://www.apereo.org/cas/protocol

Les version 1 et 2 du protocole sont gérées.

En plus des fonctionnalités de base décrites dans le protocole, les fonctions suivantes ont été ajoutées pour permettre une meilleure compatibilité avec des versions plus récentes (CAS 3) :

- échange de messages au format SAML 1.1 dans une enveloppe SOAP ;
- implémentation d'une déconnexion centralisée pour les sessions établies via le protocole CAS. Cette fonctionnalité peut être activée ou désactivée au niveau du serveur (active par défaut) ;
- envoi d'attributs utilisateur supplémentaires dans la réponse du serveur, avec un système de filtres suivant l'URL de destination.



Les protocoles 1 et 2 de CAS utilisent un format de messages différent. Le serveur peut être configuré pour répondre à l'un ou l'autre des formats, mais ne peut pas gérer les 2 en même temps. La version 1 du protocole est disponible pour permettre au serveur de répondre à des clients plus anciens, mais dans ce cas les fonctionnalités du serveur seront très limitées (en particulier, le mode proxy et l'envoi d'attributs ne sont pas gérés).

Compatibilité du client

Suivant le client utilisé, certaines fonctionnalités peuvent ne pas être disponibles.

- La prise en compte des requêtes de déconnexion envoyées par le serveurs nécessitent l'utilisation d'un client récent (phpCAS version 1.1.0 ou supérieur).

Une version modifiée du client phpCAS est disponible dans les dépôts de la distribution EOLE.

6.3.2. Compatibilité SAML2

Pour permettre de répondre à des problématiques de fédération de l'identité des utilisateurs dans des référentiels différents, le serveur EoleSSO est désormais capable d'échanger des messages au format SAML 2[p.777] . Cela permet, par exemple, que des utilisateurs authentifiés au niveau d'un établissement scolaire puissent accéder à des ressources gérées en académie sans s'authentifier à nouveau.

Les fonctionnalités implémentées correspondent à un certain nombre de scénarios envisagés. Les profils et bindings définis par le standard ne sont pas tous implémentés. En particulier, les binding `HTTP Artifact` et `SOAP` ne sont pas gérés, le serveur EoleSSO ne peut donc pas actuellement être considéré comme pleinement conforme au standard SAML 2.

Pour plus de détail, se reporter au document [http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf] publié sur le site d'OASIS.

Les fonctionnalités absentes seront éventuellement implémentées dans des versions ultérieures selon les besoins.

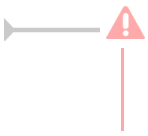
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les mécanismes suivants sont implémentés :

- WebSSO : AuthnRequest (POST/Redirect) / IDP Response (POST) ;
- Single Logout : LogoutRequest (POST/Redirect) / LogoutResponse (POST/Redirect).

Le serveur EoleSSO met à disposition un fichier de méta-données pour faciliter la mise en relation avec une entité partenaire.

Il gère également un répertoire de fichiers de méta-données pour récupérer les informations sur ces entités. Se reporter au chapitre `gestion des méta-données` pour plus de détails.



Les requêtes et assertions échangées doivent être signées. La clé de signature de l'entité partenaire doit être inclue dans le fichier de méta-données.

Scenarii gérés :

1. En tant que fournisseur d'identité :
   - émission d'une assertion d'authentification à destination d'un fournisseur de service (initié par le fournisseur d'identité ou suite à réception d'une requête authentification émise par un fournisseur de service valide) ;
   - déclenchement du processus de déconnexion globale à l'initiative du fournisseur ou suite à la réception d'une requête de déconnexion valide.
2. En tant que fournisseur de service :
   - création d'une session locale suite à la réception d'une assertion d'authentification d'un fournisseur d'identité (et redirection vers l'adresse spécifiée par le paramètre *relayState* si il est présent) ;
   - émission d'une requête de déconnexion en direction du fournisseur d'identité en cas de demande de déconnexion depuis une application cliente.

6.3.3. Compatibilité RSA Securid

Principe de fonctionnement

Le service EoleSSO est capable de vérifier l'authentification d'un utilisateur auprès d'un serveur RSA utilisant le protocole SecurID[p.778] (authentification de type One Type Password).

L'authentification est effectuée par l'intermédiaire du module PAM[p.773] SecurID fourni par la société RSA.

Le principe est de vérifier l'authentification de l'utilisateur auprès du serveur RSA, et de conserver cette information dans la session SSO de l'utilisateur.

Lorsque l'utilisateur essaie ensuite de se connecter à un fournisseur de service, les messages SAML envoyés pour établir la fédération seront adaptés pour refléter le niveau d'authentification de l'utilisateur (mot de passe à utilisation unique).

Actuellement, cette fonctionnalité n'est disponible que sur un serveur EoleSSO configuré pour gérer l'authentification OTP[p.773].

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

> Il est prévu par la suite de pouvoir déléguer cette validation à un autre serveur EoleSSO (moyennant l'établissement d'un lien de fédération entre les deux serveurs).

Utilisation

Lors de la première utilisation, l'utilisateur se connecte au serveur EoleSSO avec ses identifiants habituels (authentification LDAP). Avant de valider le formulaire d'authentification, il peut cocher la case `Enregistrer mon identifiant OTP`. Il peut alors renseigner l'utilisateur associé à sa clé OTP sur le serveur RSA, ainsi que son code PIN et le mot de passe actuel.



> Le serveur SSO ne gère pas la saisie initiale du code PIN d'un utilisateur. Dans le cas d'un nouvel utilisateur, il faudra au préalable que celui-ci se connecte sur la mire RSA pour créer son code PIN.

Le serveur EoleSSO va vérifier l'authentification LDAP, puis va valider l'authentification auprès du serveur RSA. Si les deux authentifications réussissent, il va enregistrer l'identifiant de l'utilisateur sur le serveur RSA et va l'associer à l'utilisateur LDAP.

Par la suite, lorsque l'utilisateur revient sur la page d'authentification, le système détecte qu'il s'est déjà enregistré (après saisie de son identifiant habituel). L'utilisateur a alors la possibilité de cocher la case '`Connexion par clé OTP`'. Dans ce cas, il lui suffit de saisir son code PIN et mot de passe OTP pour s'authentifier.

6.3.4. Compatibilité OpenID Connnect

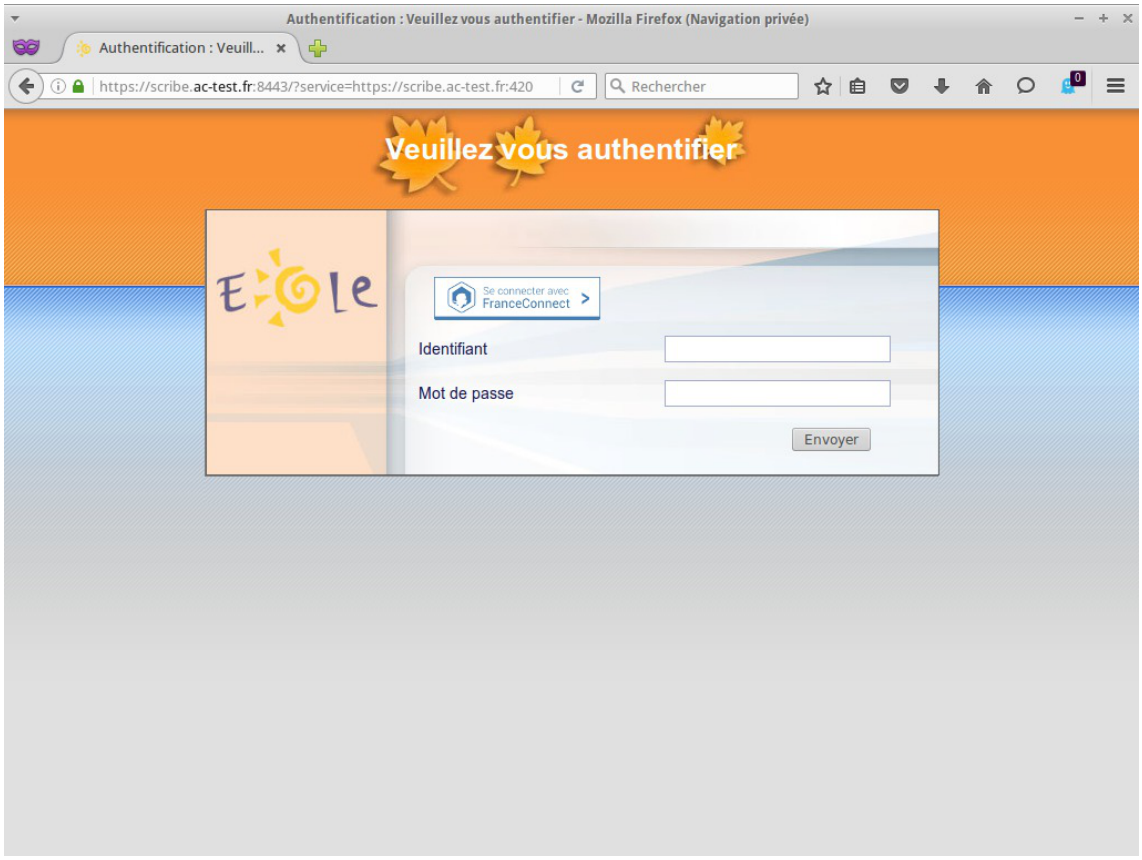
Des modifications ont été apportées à EoleSSO pour permettre d'authentifier les utilisateurs auprès du fournisseur d'identité France Connect[p.762].

Il est également possible de configurer d'autres fournisseurs d'identité OpenID Connect[p.772] dans les limites des fonctionnalités implémentées. Seul France Connect et l'authentification OAuth[p.771] 2.0 de Google ont été testés à ce jour.

Le principe de fonctionnement est le suivant :

- l'utilisateur se connecte à une application protégée par EoleSSO et est redirigé sur la mire d'authentification ;
- la mire d'authentification EoleSSO présente un bouton pour chaque fournisseur d'identité OpenID configuré ;

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



- lorsqu'un utilisateur clique sur un de ces boutons, il est redirigé vers le portail de connexion du fournisseur correspondant ;

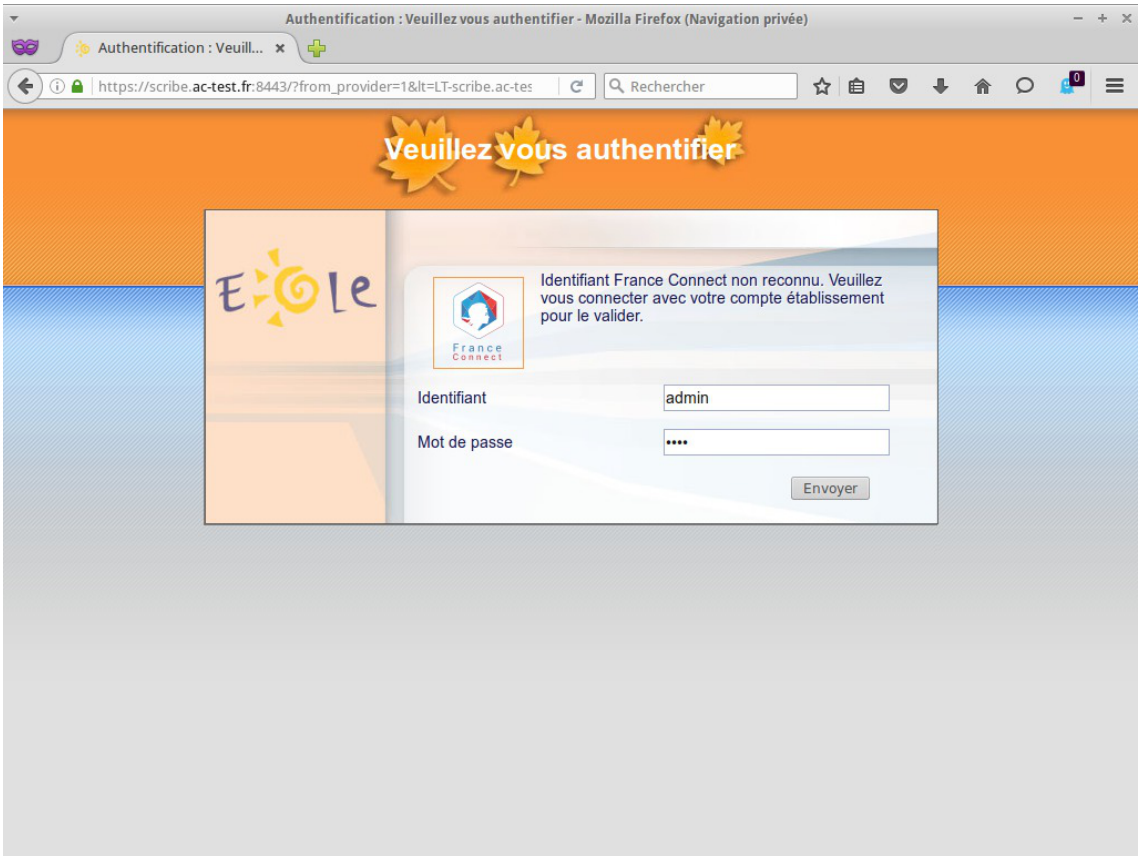


- après authentification, il est renvoyé sur le portail EoleSSO ;
- lors de la première connexion de l'utilisateur avec ce fournisseur, EoleSSO demande de renseigner le

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

couple identifiant/mot de passe habituel, et l'associe à l'identifiant retourné par le fournisseur ;

- si l'association a déjà été réalisée, EoleSSO retrouve le compte associé, et créer directement la session de nécessaire à l'utilisateur ;



- l'utilisateur est redirigé vers l'application à laquelle il souhaite accéder.

Données échangées

Le protocole OpenID Connect prévoit que le fournisseur de service précise un ensemble de données auxquelles il veut accéder (scope dans le vocabulaire OpenID).

Cela peut permettre de récupérer diverses informations (sous réserve du consentement de l'utilisateur) , comme l'adresse de messagerie, le numéro de téléphone…

Pour l'implémentation de OpenID réalisé dans EoleSSO, le but est de récupérer un identifiant pérenne et que l'utilisateur l'associe à son compte local. Le scope minimal nommé `openid` est utilisé et seul l'attribut `sub` est récupéré par EoleSSO (identifiant nom nominatif de l'utilisateur et sans informations personnelles).

La correspondance entre l'identifiant local et l'identifiant OpenID est stockée dans un fichier `/usr/share/sso/openid_users/<référence_fournisseur>_users.ini`

Pré-requis à la mise en œuvre

OpenID Connect repose sur un principe de confiance entre un fournisseur de service (Relying Party, par exemple EoleSSO), et un fournisseur d'identité (OpenID Provider, par exemple France Connect).

Pour mettre en place cette relation de confiance, le fournisseur de service va effectuer une demande d'enregistrement auprès du fournisseur d'identité. Celui-ci lui renverra un identifiant et une clé secrète.

Le fournisseur d'identité met à disposition un certain nombre d'URLs nécessaires à la configuration du

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

client.

Un principe de configuration automatique est prévu par le protocole, mais il est rarement utilisé dans la pratique et n'a pas été implémenté dans EoleSSO.

Les modalités de cet échange d'informations sont spécifiques à chaque fournisseur.

Dans la plupart des cas, il sera demandé :

- une adresse dite de callback : c'est l'adresse sur laquelle est renvoyé l'utilisateur après authentification.

  Dans le cas d'EoleSSO cette adresse est :

  `https://<adresse_serveur_eolesso>:8443/oidcallback`
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie...) qui apparaîtra sur la page d'authentification du fournisseur d'identité.

Gestion de la déconnexion

La cinématique de déconnexion (single logout) n'est pas implémentée par tous les fournisseurs.

Par ailleurs, certains acteurs utilisent une cinématique de déconnexion spécifique. Des adaptations ont ainsi été réalisées pour la déconnexion de Google (testée) ainsi que pour celles de Facebook et Microsoft (non testées).

6.3.4.a. Configuration du fournisseur d'identité France Connect

Pour mettre en place la relation de confiance entre EoleSSO et France Connect, il faut effectuer une demande d'enregistrement auprès de France Connect : https://franceconnect.gouv.fr/inscription

Le fournisseur d'identité France Connect renvoi un identifiant client (Client ID) et une clé privée secrète (Client secret) utilisé pour valider les échanges. Il met à disposition un certain nombre d'URLs nécessaires à la configuration du client.

Pour l'inscription il est demandé les informations suivantes:

- le nom du service ;
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie...) qui apparaîtra sur la page d'authentification de France Connect ;
- une adresse dite de callback : adresse sur laquelle est renvoyé l'utilisateur après authentification.

  Dans le cas d'EoleSSO cette adresse est :

  `https://<adresse_serveur_eolesso>:8443/oidcallback`

Les logos et bouton de connexion France Connect sont déjà fournis avec EoleSSO.

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

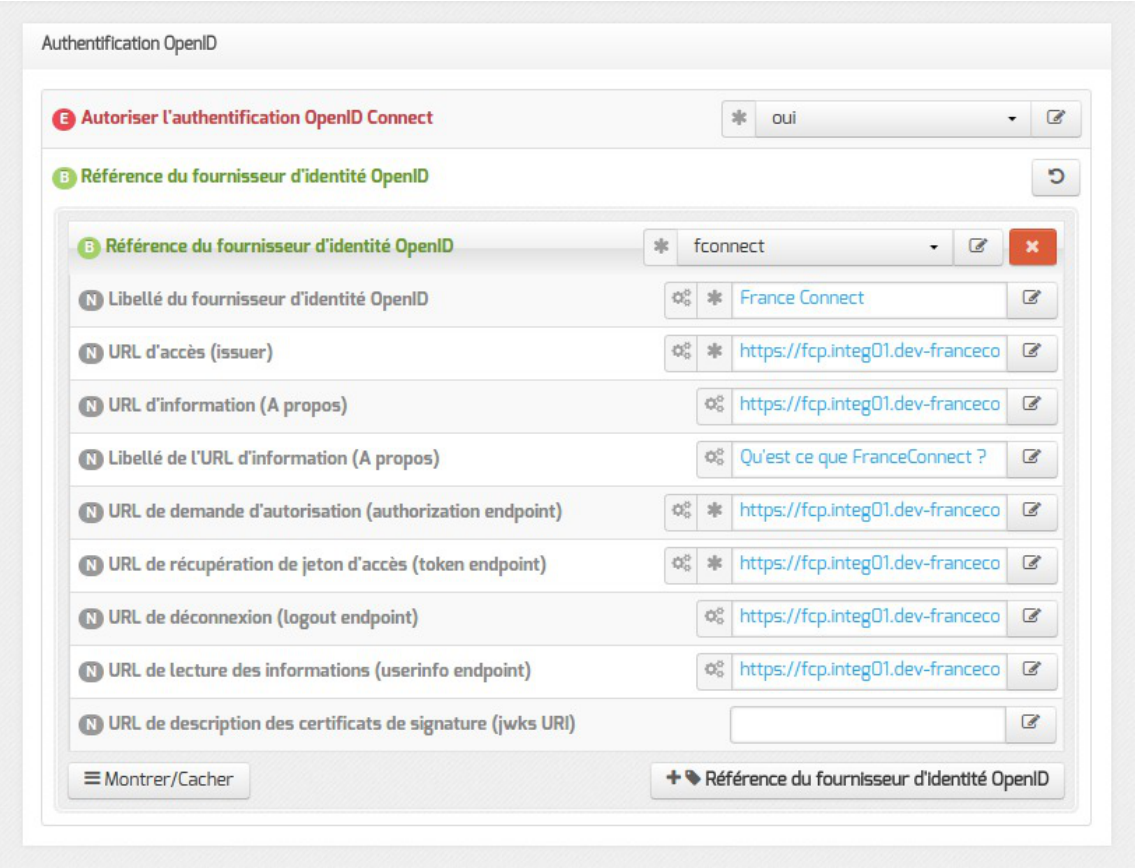
Pour plus d'informations sur le fonctionnement et la configuration, se reporter à : https://franceconnect.gouv.fr/fournisseur-service

Les conditions d'utilisation de France Connect et le processus de raccordement sont décrites dans le document PDF suivant :

https://franceconnect.gouv.fr/files/CGU FS - Annexe Processus d'implementation de FC par FS V2.1.pdf [https://franceconnect.gouv.fr/files/CGU%20FS%20-%20Annexe%20Processus%20d'implementation%20de%20FC%20par%20FS%20V2.1.pdf]

À noter que parmi les conditions, une **déclaration CNIL** simplifiée est disponible et une **recette de la solution technique** mise en œuvre doit être effectuée par le SGMAP[p.778].

Une configuration prédéfinie est fournie pour France Connect.



Pour l'activer, choisissez `fconnect` dans la liste déroulante de la variable `Référence du fournisseur d'identité OpenID`, ne pas oublier de valider le choix pour faire apparaître les différentes variables.

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

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

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


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

> Le `nom fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.
>
> Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Voir aussi...

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

6.3.4.b. Configuration du fournisseur d'identité Google (Google APIs).

Déclaration d'EoleSSO comme fournisseur de service

Pour récupérer votre Client ID / Client Secret, vous devez créer un compte développeur depuis cette adresse : https://developers.google.com/

Rendez-vous dans la console développeur de Google afin de déclarer votre service EoleSSO comme application : https://console.developers.google.com

- Créez un nouveau projet (barre supérieure de la console -> `select a project` -> `create a project`) ;
- Une fois le projet créé, cliquez sur la barre de menu gauche (3 barres horizontales), puis sur `API Manager`. Cliquez ensuite sur `Credentials` (à gauche) ;
- Cliquer sur `Oauth Consent Screen` et renseigner au minimum le champ `Product name shown to users` (par exemple 'établissement xxx') ;
- Sauvegarder et dans Credentias, cliquer sur `Create credentials`, *Oauth Client ID" ;
- Choisir `Web application` et renseigner les champs suivants :
  - Name : au choix
  - Authorized JavaScript origins : https://[adresse_serveur_sso]:8443
  - Authorized redirect URIs : https://[adresse_serveur_sso]:8443/oidcallback
- Cliquer sur Create et recopier l'identifiant et la clé secrète fournis ;

Configuration du fournisseur d'identité (Google) dans l'interface de configuration du module

Une fois les identifiants récupérés, vous pouvez configurer les paramètres d'EoleSSO (gen_config, onglet Eole SSO en mode expert)

- Passer à `oui` la variable `Autoriser l'authentification OpenID Connect`;
- ajouter un forunisseur en cliquant sur `+Référence du fournisseur d'identité OpenID` ;
- `Référence du fournisseur d'identité OpenID` : google (des logos sont présents et utilisés automatiquement en choisissant ce libellé) ;
- `Libellé du fournisseur d'identité OpenID` : Google (ou autre description de votre choix) ;
- `issuer` : https://accounts.google.com ;
- `authorization endpoint` : https://accounts.google.com/o/oauth2/v2/auth ;

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

- `token endpoint` : https://www.googleapis.com/oauth2/v4/token ;
- `userinfo endpoint` : https://www.googleapis.com/oauth2/v3/userinfo ;
- `jwks uri` : https://www.googleapis.com/oauth2/v3/certs .

En cas de problème, les paramètres en cours de validité sont décrits ici : https://accounts.google.com/.well-known/openid-configuration

Pour plus d'informations sur le support d'OpenID de Google : https://developers.google.com/identity/protocols/OpenIDConnect



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

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

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

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

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

Voir aussi...

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.217]

6.4. Gestion des attributs des utilisateurs

Le gestionnaire de sessions permet de récupérer des informations de l'utilisateur connecté, par exemple :

- les données LDAP de l'utilisateur (récupérées lors de la phase d'authentification) ;
- le numéro et le libellé de l'établissement hébergeant le serveur d'authentification.

Le serveur EoleSSO permet également :

- d'étendre les données disponibles en définissant des attributs calculés ;
- de créer des filtres définissant quels attributs seront disponibles ;
- de décrire des URL afin de différencier les applications et leur appliquer un filtre.



En cas d'ajout de filtres, de définitions d'applications ou d'attributs calculés, il est possible de demander au serveur de les prendre en compte sans le redémarrer. Pour cela, il faut utiliser l'option `reload` du script de démarrage du service :

```
# CreoleService eole-sso reload
```


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

6.4.1. Ajout d'attributs calculés

EoleSSO permet de définir des attributs calculés en plus des données récupérées dans l'annuaire à la connexion de l'utilisateur. Ces attributs sont calculés par des fonctions écrites en langage Python et ayant accès aux attributs connus de l'utilisateur.

Pour ajouter un attribut calculé, créer un fichier `<nom_attribut>.py` dans le répertoire `/usr/share/sso/user_infos/` :

```
# -*- coding: utf-8 -*-

use_cache = True

... imports et fonctions utilitaires pour le calcul ...

def calc_info(user_info):
    .....
    return valeur_attributs
```

- `use_cache` est une directive spécifiant si l'attribut doit être mis en cache (voir Optimisation des attributs calculés) ;
- `user_info` est le dictionnaire des données existantes, il est passé automatiquement à la fonction par le serveur SSO ;
- `valeur_attributs` peut être
  - une liste Python contenant les valeurs à associer à l'attribut <nom_attribut> :
    `return [val1, val2, ...]`
  - un dictionnaire Python dont les clés sont le nom de champ et les valeurs la liste de valeurs associées (calcul d'attributs multiples) :
    `return {'attribut1' : [val1, val2, ...], 'attribut2' : [val1, val2, ...], ...}`

Pour que ces données soient envoyées aux applications clientes du service EoleSSO, il faut les assigner dans un filtre de données (cf. paragraphes suivants)

Nom de l'attribut retourné

Dans le cas ou une simple liste de valeur est retournée, c'est le nom du fichier qui détermine le nom d'attribut auquel seront assignées les valeurs (nom du fichier sans l'extension `.py`).

Dans le cas du calcul d'attributs multiples, le nom de fichier n'est pas pris en compte , le nom de l'attribut est indiqué directement dans la structure retournée.

Données à disposition des fonctions de calcul

L'objet `user_infos` est un dictionnaire Python contenant les informations connues sur l'utilisateur (récupérées au moment de sa connexion). Il contient les informations suivantes :

- tous les champs de l'utilisateur dans l'annuaire LDAP qui sont accessibles par lui en lecture, à l'exception des mots de passe. Comme c'est le cas dans l'annuaire, les valeurs des attributs sont multivaluées. Par exemple, pour récupérer la première valeur du champ mail, utiliser `user_infos['mail'][0]` ;

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

- une entrée `user_groups` qui contient la liste des groupes Samba auxquels l'utilisateur est inscrit (récupérée également dans l'annuaire) ;
- une entrée `info_groups` contenant un dictionnaire dont les clés sont l'attribut `cn` des groupes présents dans `user_groups` et les valeurs sont les attributs du groupe correspondant dans l'annuaire LDAP. Seuls les attributs suivants sont conservés : `sambaGroupType`, `displayName`, `cn`, `objectClass`, `gidNumber`, `mail`, `description` et `niveau` ;
- une entrée `dn` contenant le DN complet de l'utilisateur (utilisé pour récupérer le RNE d'origine d'un utilisateur dans le cas d'un annuaire multi-établissements) ;
- les entrées `rne` et `nom_etab` qui correspondent aux informations présentes dans la configuration Creole du serveur (ou dans le fichier de configuration du serveur EoleSSO le cas échéant) ;
- au fur et à mesure du calcul des attributs, ceux déjà traités sont rendus disponibles dans `user_infos`.

Ordre de traitement et mise à disposition des attributs

2 règles s'appliquent pour déterminer dans quel ordre les attributs calculés sont évalués :

- Les fichiers sont traités par **ordre de tri alphanumérique** sur le noms des fichiers. Si un attribut dépend d'un autre, il est recommandé de préfixer le nom de fichier par un numéro (par exemple `00_attribut1.py`, `01_attribut2.py` si attribut2 doit récupérer la valeur d'attribut1) ;
- Les fichiers renvoyant les valeurs d'**un seul attribut** (renvoi de liste) sont **prioritaires sur celles renvoyant des attributs multiples** (renvoi de dictionnaire, même si celui-ci contient un seul attribut). Cela permet par exemple de disposer d'un ensemble d'attributs renvoyés par une seule fonction, puis d'écraser au cas par cas certains attributs si des adaptations sont nécessaires d'un serveur à l'autre (ou de redéfinir un des attributs comme non mis en cache).

Optimisation des attributs calculés

Toutes les fonctions présentes sont calculées lors de la création de la session d'un utilisateur et lorsqu'une application accède aux informations de l'utilisateur.

Pour éviter de surcharger le serveur EoleSSO lors de requêtes multiples, les attributs peuvent être mis en cache pour la durée de la session SSO de l'utilisateur. Pour qu'un attribut utilise ce cache, il faut ajouter la ligne suivante dans le fichier de calcul :

```
use_cache = True
```

Il est conseillé d'utiliser cette directive sur tous les attributs, sauf ceux dont la valeur doit être ré-évaluée durant la session de l'utilisateur.

Dans le cas d'une utilisation du produit EoleSSO hors du cadre de la distribution EOLE, certains attributs peuvent ne pas être disponibles (en fonction de l'organisation des données dans l'annuaire). Certaines informations comme le libellé de l'établissement ou son code RNE peuvent être renseignées dans le fichier de configuration principal du serveur : `/usr/share/sso/config.py`.

En plus des données ci-dessus, un certain nombre d'attributs calculés sont livrés par défaut par le serveur :

- `classes` : la classe d'un élève ou les classes d'un professeur (livré par `groupes.py`) ;

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

- `disciplines` : les matières enseignées pour un professeur (livré par `groupes.py`) ;
- `niveaux` : le niveau (attribut `Mefclf`) d'un élève ou les niveaux dans lesquels un professeur enseigne (livré par `groupes.py`) ;
- `secureid` : identifiant opaque calculé avec un MD5[p.769] de l'UID et du RNE de l'utilisateur ;
- `ENTPersonProfils` : renvoie le profil de l'utilisateur tel que défini dans le SDET (par ex. National_1 pour un élève) ;
- `ENTPersonStructRattachRNE` : le numéro d'établissement d'origine de l'utilisateur, calculé à partir de son DN dans l'annuaire (utile dans le cas d'un annuaire centralisé regroupant plusieurs établissements) ;
- `ecs_profil` et `ecs_rne` : version spécifique des 2 attributs précédents (applications xDesktop et eConnect, voir le site http://envole.ac-dijon.fr) ;
- `entlogin` : renvoie l'attribut `ENTPersonProfil` de l'utilisateur. Si ce champ n'est pas renseigné, l'équivalent de `secureid` est renvoyé.

Attribut calculé secureid (identifiant unique et opaque à destination de services externes)

Contenu du fichier `/usr/share/sso/user_infos/secureid.py` :

```
# -*- coding: utf-8 -*-

def calc_info(user_infos):
    """calcule secureid : identifiant crypté unique pour chaque utilisateur"""
    from md5 import md5

    # calcul d'un identifiant crypté unique
    user_hash = md5("%s@%s" % (user_infos['uid'][0], user_infos['rne'][0]))

    return [user_hash.hexdigest()]
```

6.4.2. Filtrage des données par application

EoleSSO implémente un mécanisme permettant de renvoyer des informations différentes concernant l'utilisateur en fonction de l'application qui émet la requête.

Ce mécanisme nécessite la mise en place de deux fichiers de configuration :

- un fichier de description de l'application. Ces fichiers doivent être placés dans le répertoire `/usr/share/sso/app_filters` et leur nom doit se terminer par `_apps.ini`.
- un fichier de filtre (dans le même répertoire), devant se nommer `<nom_du_filtre>.ini`.

La description d'une application se fait selon le modèle suivant (exemple avec une application fictive) :

`[editeurs]` # nom de l'application (indicatif)

`port=80` # port de l'application (facultatif)

`baseurl=/providers` # url de l'application

`scheme=both` # type de protocole : http/https/both

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

`addr=^appserv..*.fr$` # adresse des serveurs autorisés

`typeaddr=regexp` # type d'adresse

`filter=mon_filtre` # nom du filtre à appliquer

`proxy=default` # proxy http nécessaire pour accéder à l'application

Si `port` est spécifié, il devra apparaître dans l'URL du service désirant s'authentifier. Pour que la définition fonctionne quel que soit le port (ou si le port n'est pas dans l'URL), enlevez la ligne concernant le port, ou mettez `port=` sans valeur

Il y a 2 types de vérification de l'adresse (`typeaddr`) :

1. type **ip** : l'adresse donnée peut être une adresse IP ou un couple adresse/netmask.

   Les formats d'écriture suivants sont possibles :

   - 192.168.230.1
   - 192.168.230.0/255.255.255.0
   - 192.168.230.0/24

2. type **regexp** : l'adresse est donnée comme une expression régulière à comparer à l'adresse DNS du client.

   Dans l'exemple : ^appserv..*.fr$ -> correspond à toutes les adresse du type par appserv.<qqe_chose>.fr

   Ces données seront comparée avec l'URL associée à la session dans le serveur SSO (dans le cadre du protocole CAS, cette URL correspond au champ service donné lors de l'obtention d'un ticket d'application).



Pour vérifier le fonctionnement d'une regexp, lancer un shell python:

```
>>> import re
>>> regexp = '<votre regexp>'
>>> url = '<une url à comparer avec la regexp>
>>> print re.match(regexp, url) is not None
```

`baseurl` correspond au chemin de l'application.

Dans l'exemple ci dessus, une URL du type `http://appserv_test.fr:80/providers` sera reconnue (A noter que `http://appserv_test.fr:80/providers/toto` est aussi considéré comme valide).

La partie requête de l'URL n'est pas prise en compte (dans cet exemple, `http://appserv_test.fr:80/providers?variable=1&variable2=test` sera considérée valide).

Pour vérifier quelle URL est reçue, vous pouvez regarder dans /var/log/rsyslog/local/eolesso/eolesso.info.log . L'URL est affichée dans les lignes commençant par : `adding session for service : ....`

`filter` indique le nom du fichier de filtre à utiliser (sans l'extension.ini) pour les applications correspondant à cette description. Voir la section suivante pour plus de détail.

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

`proxy` indique que l'utilisation d'un proxy est nécessaire pour accéder à l'application depuis la machine hébergeant le serveur EoleSSO.

si la valeur est '`default`', le proxy déclaré dans la configuration (dans l'onglet general de gen_config) est utilisé. Il est aussi possible de spécifier un proxy particulier avec une valeur du type '`nom_hote:port`'. Le proxy déclaré sera utilisé dans les procédures suivantes :

- envoi d'une requête de déconnexion CAS à une application
- envoi d'un ticket PGT à un client CAS en mode proxy

6.4.3. Définition de filtres d'attributs

Toutes les données connues de l'utilisateur peuvent être propagées vers les applications lorsque celles-ci valident l'authentification de l'utilisateur auprès du serveur EoleSSO.

Pour décider quelles informations seront renvoyées aux différentes applications, un système d'application de filtres a été mis en place. Le principe est de définir dans un fichier un ensemble d'attributs à renvoyer à une(des) application(s), ainsi que le nom à leur donner dans le cadre de ce filtre.

Ces fichiers sont à placer dans le répertoire `/usr/share/sso/app_filters` et doivent avoir le format suivant :

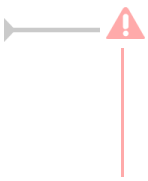
```
[section1]
libelle=variable
libelle2=variable2
....
[section2]
....
```

- **section** sert à la mise en forme de la réponse (pour CAS, un nœud dans le XML retourné lors de la validation du ticket)
- **variable** correspond à l'identifiant LDAP de la donnée utilisateur à récupérer
- **libelle** est le nom qui sera utilisé pour présenter cette donnée dans la réponse du serveur

Le choix d'un filtre d'attribut est conditionné par l'adresse du service à atteindre (voir chapitre précédent). Il est également possible de créer dans le répertoire `app_filters` des **fichiers de filtres globaux** dont les attributs seront ajoutés à tous les filtres.

Le format est le même, mais ces fichiers doivent avoir l'extension `.global`.

Dans le cas ou un attribut défini dans un filtre global existe également dans le filtre d'une application, c'est la définition spécifique à l'application qui sera prise en compte lors de l'envoi des attributs à celle-ci.



Si vous souhaitez appeler la méthode statique `getUser(…)` dans votre application il est impératif d'utiliser au minimum la correspondance `user=uid` dans votre filtre. Sinon l'authentification ne peut pas aboutir : `CAS Authentification failed !`



Exemple de fichier de profil stocké dans `/usr/share/sso/app_filters/mon_filtre.ini`

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

(correspond à l'exemple du paragraphe précédent).

```
[utilisateur]
user=uid
codeUtil=uidNumber
nom=sn
prenom=givenName
niveau=niveau
mail=mail
[etablissement]
codeRNE=rne
nomEtab=nom_etab
```



Si vous utilisez EoleSSO dans le cadre d'une distribution EOLE, un certain nombre de filtres et de définitions d'applications sont disponibles.

Il faut installer le paquet `envole-conf-sso` avec la commande `apt-get install envole-conf-sso` pour les récupérer.

Les filtres sont installés dans `/usr/share/sso/filters_available` et `/usr/share/sso/applications/available`.

Pour les utiliser, recopiez les fichiers voulus dans `/usr/share/sso/app_filters` et rechargez la configuration du service avec la commande `service eole-sso reload`

6.5. Fédération avec une entité partenaire

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO, ou vers d'autre types de serveurs compatibles avec le protocole SAML (version 2). Les sections suivantes détaillent la mise en œuvre d'une telle solution suivant 2 méthodes différentes.

- Une première méthode de fédération simplifiée est gérée via la notion de serveur parent. Elle est utilisable uniquement entre deux serveurs EoleSSO et présente un certain nombre de limitations.
- La deuxième méthode, plus complète mais également plus complexe à mettre en œuvre, est gérée par l'implémentation d'un certain nombre d'éléments du protocole SAML[p.777] dans sa version 2. Ce type de fédération est compatible avec d'autres produit, et a principalement été testé pour une fédération avec la plateforme RSA/FIM. Des tests sont également en cours pour une fédération vers des ENT comme k-d'école de la société Kosmos.

6.5.1. Déclaration d'un serveur parent

Le fait de renseigner un serveur parent (serveur B) dans la configuration du serveur EoleSSO (serveur A) permet de fédérer ces deux serveurs. Cette solution correspond plus à une agrégation des référentiels des deux serveurs plutôt qu'à une fédération.

On considère par exemple que le serveur A est installé dans un établissement scolaire (annuaire local), et le serveur B est situé dans un rectorat (branché sur un annuaire académique).

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

Une fois l'adresse du serveur parent renseignée, le comportement sera le suivant :

Lorsqu'un utilisateur se connecte sur le serveur A, le serveur va d'abord vérifier le couple login/mot-de-passe auprès du serveur B (par un échange XMLRPC encapsulé dans le protocole HTTPS).

1. Si le serveur B indique une erreur d'authentification, l'authentification va alors être vérifiée localement (sur l'annuaire du serveur A).

   En cas de réussite, une session SSO est établie pour le serveur A, et l'utilisateur sera authentifié auprès des services configurés pour utiliser A. Dans le cas contraire, on considère que l'authentification a échoué.

   On retrouve donc ici le même schéma de fonctionnement que si le serveur A n'avait pas de serveur parent.

2. Si le couple login/mot-de-passe est accepté par le serveur B, une session locale 'déportée' est créée sur le serveur A. L'utilisateur est considéré comme authentifié, mais lors des échanges avec les applications, les validations seront faites auprès du serveur B.

   Le serveur A va également rediriger le navigateur de l'utilisateur vers le serveur B afin qu'un cookie de session soit créé pour celui-ci (il redirige sur le serveur A une fois le cookie créé). A la fin de cette procédure, l'utilisateur est donc identifié en même temps sur les serveurs A et B. La durée de validité de la session est gérée par le serveur B qui refusera toute validation au serveur A une fois sa session expirée.



Limitations de ce système :

- Cette solution n'est pas à proprement parler un système de fédération des 2 serveurs. Il est recommandé de l'utiliser seulement dans des cas assez simples d'utilisation, par exemple pour permettre aux personnel des équipes académiques de se connecter avec leur identifiants dans un établissement (il faut ensuite prévoir de leur attribuer des droits dans les applications, ou un profil d'administrateur sur l'EAD, ...)
- Le système de serveur parent se base sur l'adresse IP du serveur parent. Pour des raisons de sécurité (attaques de types man in the middle[p.769]), il est conseillé d'utiliser cette solution dans le cadre d'un réseau sécurisé (par exemple, à travers un RVP). Le cas échéant, on préférera la solution proposée dans le paragraphe suivant.

6.5.2. Fédération SAML : Gestion des Associations

La solution retenue pour effectuer une fédération entre deux systèmes est l'utilisation de messages SAML[p.777] pour transmettre les informations d'authentification.

La mise en place de cette fédération s'effectue en deux étapes :

- définition des attributs permettant de retrouver les utilisateurs dans les référentiels des deux systèmes (clé de fédération) ;
- échange de fichiers de méta-données (métadata[p.762]) et de certificats entre les deux entités pour établir un lien de confiance.

Pour que la fédération soit possible, il faut pouvoir établir une correspondance entre les utilisateurs des deux entités partenaires.

Pour cela, il est nécessaire de définir les attributs qui seront utilisés de chaque côté pour faire la jointure

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

entre les deux référentiels.

configuration en tant que fournisseur de service

Jeux d'attributs

Le fichier de méta-données du serveur EoleSSO indique quels attributs sont requis pour identifier les utilisateurs dans son référentiel (l'annuaire LDAP).

Cette partie des méta-données est calculée depuis les fichiers de jeux d'attributs présents dans le répertoire `/usr/share/sso/attribute_sets` (voir plus loin). Après création ou modification de ces fichier, le serveur doit être relancé (reload est suffisant) pour que les méta-données soient mises à jour.



> Le fichier `attributes.ini` présent sur les anciennes versions n'est plus utilisé. Des jeux d'attributs différents pouvant être assignés à chaque fournisseur d'identité, il peut être gênant de forcer les attributs requis en mode fournisseur de service. (voir paragraphe suivant).
>
> Un numéro d'index est attribué automatiquement à chaque jeu d'attribut au démarrage du serveur (ne le renseignez pas vous même). Dans le cas ou les fichiers de jeux d'attributs seraient perdus, il faudra envoyer à nouveau le fichier metadata du serveur aux entités partenaires afin que la nouvelle numérotation soit prise en compte.

Pour retrouver les utilisateurs après réception d'une assertion en provenance d'un fournisseur de service, le serveur EoleSSO va utiliser un jeu d'attributs. Ceux-ci sont renseignés dans des fichiers au format `.ini` situés dans `/usr/share/sso/attribute_sets/`.

Le format des fichiers est :

```
[user_attrs]
attribut_1=attribut_a
attribut_2=attribut_b
....
[optional]
attribut_3=attribut_c
....
[branch_attrs]
attribut_x=element_dn_y
....
```

Les attributs de gauche correspondent aux attributs reçus dans l'assertion du fournisseur d'identité, ceux de droite correspondent aux attributs auxquels il doivent correspondre localement.

La section `branch_attrs` permet d'utiliser certains attributs pour déterminer une branche de l'annuaire dans laquelle rechercher l'utilisateur.

Cela permet de limiter les problèmes dans le cas où des utilisateurs peuvent avoir le même identifiant dans l'annuaire (par exemple, dans le cas d'une fédération basée sur l'uid de l'utilisateur à destination d'un serveur Seshat répliquant l'annuaire de plusieurs Scribe).

Pour ces attributs, le fonctionnement est le suivant :

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

- lors de la recherche de l'utilisateur, le serveur va rechercher une correspondance sur 'element_dn_y=valeur_attribut_x' dans la liste des annuaires qui sont répliqués par le serveur LDAP local ;
- si plusieurs attributs de ce type sont renseignés, la branche de recherche devra correspondre à tout ces attributs.

Par exemple, si on renseigne `rne=ou` et que les attributs de l'utilisateur recherché contiennent `rne=0000000A`, le serveur EoleSSO va utiliser une branche d'annuaire dont la base de recherche contient ou=0000000A.

Les attributs de la section `user_attrs` (ou toute autre section différente de `branch_attrs` ou `optional`) seront utilisés pour retrouver l'utilisateur correpondant à la réponse du fournisseur d'identité dans le(s) serveur(s) LDAP utilisé(s) par EoleSSO.

Tous les attributs de droite doivent exister côté fournisseur de service.

Les attributs de la section `optional` seront envoyés ou non à l'initiative du fournisseur d'identité.

Si ils sont envoyés dans la réponse, ils seront intégrés aux attributs stockés dans la session SSO de l'utilisateur. Si un attribut local avec le même nom qu'un attribut optionnel existe, c'est l'attribut local qui sera conservé. Cela permet de rajouter des attributs provenant du fournisseur d'identité aux attributs connus dans le référentiel du fournisseur de service.

Par exemple, avec le fichier ci-dessus, le fournisseur de service peut récupérer l'attribut `attribut_c` dans la réponse du fournisseur d'identité et le stocker en tant qu'`attribut_3` dans la session locale.

⚠ Cadre d'utilisation

L'utilisation des attributs de type `branch_attrs` est pour l'instant limitée au cas suivant :

- l'annuaire est sur le serveur hébergeant le service EoleSSO ;
- l'annuaire est configuré pour répliquer l'annuaire d'autres serveurs (les branches de recherche correspondant aux différents serveurs répliqués sont récupérées dans /etc/ldap/replication.conf).

Dans l'état actuel, cela correspond typiquement à un service EoleSSO présent sur un serveur Seshat en académie (avec réplication de plusieurs serveurs Scribe).

Dans le cadre de l'utilisation de serveurs Scribe et Seshat, il est plutôt recommandé d'utiliser la configuration par défaut (fédération sur l'attribut FederationKey récupéré depuis l'annuaire fédérateur AAF).

Configuration de l'association avec un fournisseur d'identité

Le fichier /usr/share/sso/attribute_sets/associations.ini permet de définir les options de fédération pour chaque fournisseur de service partenaire. Sa syntaxe est la suivante

```
[nom entité1]
option=valeur
[nom entité2]
option=...
```

Le nom de l'entité doit être le nom de l'entité SAML apparaissant dans le fichier métadata du partenaire concerné (`entityID`).

Tout fichier de type .ini commençant par '`associations`' pourra également être utilisé. Cela peut

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

permettre, par exemple, de distribuer une association correspondant à un serveur Seshat fournisseur de services en académie sur l'ensemble des serveurs Scribe d'une académie. (en passant par une variante dans Zéphir).

Il est possible de spécifier les paramètres supplémentaires suivants pour chaque association avec un fournisseur d'identité (tous facultatifs) :

- `attribute_set` : nom du jeu d'attributs à utiliser (correspond au nom du fichier de ce jeu, sans l'extension .ini)
- `allow_idp` ('true' par défaut) : si spécifié à 'false', aucune assertion provenant du fournisseur d'identité ne seront prises en compte.
- `allow_idp_initiated` ('true' par défaut) : si spécifié à 'false', les assertions envoyées par le fournisseur d'identité sans requête préalable ne seront pas traitées.
- `force_auth` ('false' par défaut) : si spécifié à 'true', le fournisseur d'identité demandera ses identifiants à l'utilisateur, même si celui ci était déjà connecté.
- `passive` ('false' par défaut) : si spécifié à 'true', le fournisseur d'identité ne demandera pas ses identifiants à l'utilisateur, même si il n'est pas reconnu. Dans ce cas, une réponse négative sera renvoyée par le fournisseur d'identité.
- `default_service` (aucun par défaut): si une url est renseignée ici, elle sera utilisée comme service de destination par défaut si aucun service n'est indiqué pendant le processus de fédération.
- `default_logout_url` : Adresse sur laquelle lorsqu'une déconnexion a été initiée par le fournisseur de service (utilisée seulement si la session a été établie depuis ce fournisseur d'identité). Cela permet par exemple de rediriger sur la mire du fournisseur d'identité.
- `force_logout_url` ('false' par défaut) : Force la redirection sur l'url décrite ci dessus, même si une autre url à été spécifiée dans la demande de déconnexion (par défaut, c'est donc l'url passée en paramètre est prioritaire).
- `req_context` : niveau d'authentification requis pour accepter une assertion. Les valeurs reconnues par EoleSSO sont 'urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport' (par défaut, mot de passe saisi depuis une page sécurisée) et 'urn:oasis:names:tc:SAML:2.0:ac:classes:TimeSyncToken' (connexion par clé OTP)
- `comparison` : opérateur de comparaison du niveau d'authentification indiqué par le fournisseur d'identité avec le niveau défini dans req_context. Par défaut cet opérateur est `exact` (valeur identique). Il est possible d'utiliser `minimum` (équivalent ou supérieur à), `maximum` (inférieur à) et `better` (strictement supérieur à).



Dans le cas d'une fédération entre des serveurs scribes et un serveur seshat avec réplication des annuaires scribe en central, il peut être utile de définir sur Seshat le paramètre default_logout_url pour chaque établissement fédéré.

Cela permet de revenir automatiquement sur le portail de l'établissement après une déconnexion depuis le portail ou un service de Seshat (l'utilisateur s'étant connecté à l'origine en établissement). Un script est fourni (`/usr/share/sso/get_domains.py`) pour essayer de déterminer automatiquement l'adresse du portail de chaque établissement en s'appuyant sur le serveur Zéphir.

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

Si le nom d'entité est `default`, les options définies seront utilisées par tous les fournisseurs d'identité n'ayant pas de valeur spécifique définie dans leur section. Dans le cas où aucune association avec `default` n'est présente, le fichier default.ini fourni avec le serveur sera utilisé comme association par défaut (et les options par défaut sont celles décrites ci-dessus).



Par défaut, aucun fichier d'association n'est fourni. Il faut ajouter manuellement la section correspondant à un fournisseur d'identité pour modifier les paramètres d'association avec les entités définies dans les métadonnées.

L'option `allow idp` étant à 'true' par défaut, cela veut dire que tout fournisseur d'identité décrit dans les fichiers de métadonnées sera considéré comme valide (les assertions venant de lui seront traitées).

Pour avoir plus de contrôle sur les fournisseurs d'identité valides, Il est possible par exemple de redéfinir cette valeur à '`false`' pour l'entité `default`, puis de la définir à '`true`' au cas par cas pour chaque fournisseur d'identité que l'on veut autoriser.



Pour vérifier que les jeux d'attributs sont bien pris en compte :

- relancer le serveur ou recharger la configuration avec la commande `CreoleService eole-sso restart (ou reload)`
- consulter les logs du serveur (/var/log/rsyslog/local/eolesso/eolesso.info.log). Si un jeu d'attribut est disponible pour une entité, une mention apparaîtra à côté de son nom. Par exemple :

```
2010/06/03 15:22 +0200 [-] - Fournisseur de services configuré : urn:fs:ac-dijon:etablissements:1.0
2010/06/03 15:22 +0200 [-] - Fournisseur de services configuré : urn:fi:ac-dijon:et-Collège du parc:1.0 (jeu d'attributs : parc)
```

Ici, le premier fournisseur utilisera le jeu d'attributs par défaut, alors que le deuxième utilisera un jeu spécifique.

Configuration en tant que fournisseur d'identité

Dans ce mode de fonctionnement, le serveur EoleSSO va envoyer des messages SAML à un partenaire fournisseur de service pour lui permettre de valider l'identité de l'utilisateur connecté. Les attributs envoyés dans ce message dépendent du filtre qui est appliqué lors de l'envoi du message (voir les paragraphes précédents sur la gestion des attributs).

Par défaut, le serveur EoleSSO va utiliser les attributs définis dans le filtre SAML (/usr/share/sso/app_filters/saml.ini). Il est également possible de spécifier un filtre d'attributs différent en fonction du fournisseur de service auquel la réponse est envoyée. Pour cela, il faut créer une description d'application correspondant à l'URL de réception des messages du fournisseur de services, et lui associer un filtre renvoyant les attributs voulus.



Dans le cas d'une fédération SAML, il est possible de renseigner directement le nom de

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

l'entité partenaire au lieu de décrire l'URL de réception des messages. Par exemple, la section suivante est suffisante pour déclarer un filtre :

`[mon_partenaire_saml]` (indicatif, affiché dans les logs au démarrage du serveur) `sp_ident=id_entité_fournisseur_service` (entityID dans le fichier metadata) `filter=nom_filtre` (nom du fichier de filtre sans l'extension `.ini`)

Dans le cas où le filtre appliqué ne permettrait pas d'envoyer au fournisseur de service tous les attributs qu'il a indiqué comme requis (dans son fichier de méta-données), un message d'erreur apparaît à l'envoi des informations d'authentification.



Dans le cadre d'une fédération d'un serveur Scribe en établissement avec un serveur EOLE (par exemple un module Seshat) situé dans les services académiques, nous utilisons l'adresse mail académique comme attribut de fédération (celle-ci est stockée sur Scribe dans l'attribut FederationKey lors de l'import de fichiers extraits de l'annuaire fédérateur).

Par défaut, le serveur est configuré pour utiliser cet attribut comme clé de jointure.

Le filtre utilisé par défaut lors de l'envoi d'assertion d'authentification (`/usr/share/sso/app_filters/saml.ini`) envoie l'attribut FederationKey dans le message envoyé au fournisseur de service.

6.5.3. Fédération SAML : Gestion des méta-données

Pour permettre d'établir un lien de confiance avec une entité partenaire, le serveur EoleSSO utilise des fichiers métadata[p.762] comme défini dans les standards SAML.

1. Envoi des informations du service EoleSSO à un partenaire :
   - Le fichier métadata du service EoleSSO doit être mis en place sur le serveur partenaire. La procédure varie suivant le logiciel utilisé. Ce fichier est disponible sur le serveur à l'adresse `https://<adresse_serveur_eolesso>:8443/saml/metadata`
   - Dans le cas où ils ne sont pas pris en compte depuis le fichier de métadata, les certificats du serveur doivent être envoyés séparément, et parfois convertis vers un autre format. Le certificat utilisé par défaut dans le cadre d'un serveur EOLE est /etc/ssl/certs/eole.crt, sauf si l'utilisation d'un autre fichier a été configurée (voir l'exemple de fédération avec un serveur RSA/FIM dans les annexes pour un exemple de conversion du certificat)
2. Mise en place des information du partenaire sur le serveur EoleSSO :
   - Le fichier métadata de l'entité partenaire doit être mis en place sur : `/usr/share/sso/metadata/<nom_fichier>.xml`. Si possible utilisez un nom court, car le nom du fichier (sans le .xml) peut être utilisé dans des URLs pour faire référence à l'entité au lieu d'utiliser son identifiant SAML.
   - Une fois le fichier en place, il faut redémarrer le service EoleSSO pour qu'il soit pris en compte : `CreoleService eole-sso restart` (reload est suffisant dans ce cas)



Si l'entité partenaire n'est pas un serveur EoleSSO, il faut vérifier que les informations suivantes sont disponibles dans le fichier métadata fourni :

- Certificat de signature des messages

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

- L'entité doit être capable de recevoir et envoyer des messages en utilisant les bindings `HTTP-Redirect` ou HTTP-POST. Actuellement, le serveur EoleSSO ne gère pas les bindings `HTTP-Artifact` et `SOAP/PAOS`.
- En mode fournisseur de service, le serveur EoleSSO ne gère pas le service `Idp Discovery` (détection automatique du fournisseur d'identité à l'aide d'un cookie sur un domaine commun). Il est possible cependant d'initier le processus d'authentification en tant que fournisseur de service en spécifiant le fournisseur d'identité à interroger.

6.5.4. Fédération SAML : Accès aux ressources

Activation des différents rôles dans un accord de fédération

Pour résumer, une fois les fichiers de métadata échangés entre EoleSSO et une entité partenaire (protocole SAML), les différents rôles disponibles sont conditionnés comme suit :

- Si un fichier de description de l'entité partenaire (soit par l'URL de réception des assertions, soit par son nom d'entité) est présent dans `/usr/share/sso/app_filters`, EoleSSO pourra envoyer des assertions à ce partenaire en tant que fournisseur d'identité.
- Si le nom d'entité du partenaire est présent dans un fichier d'association dans le répertoire `/usr/share/sso/attribute_sets`, ce partenaire pourra jouer le rôle de fournisseur d'identité auprès d'EoleSSO. Si l'option `allow idp initiated` est à `false` pour ce partenaire, ses assertions ne seront prises en compte que si elles font suite à une requête d'authentification émise au préalable (via l'URL `discovery` décrite ci-dessus).

Accéder à une ressource d'un fournisseur de service

Une fois la fédération mise en place entre EoleSSO et un fournisseur de service (FS), il est possible d'accéder aux services du FS à l'aide d'une URL au format suivant :

https://adresse_serveur_sso:8443/saml?sp_ident=id_fs&RelayState=service [https://adresse_serveur_sso:8443/saml?sp_ident=id_fs&RelayState=adresse_service]

`id fs` est soit l'identifiant du fournisseur de service (entityID tel que défini dans son fichier de méta données), soit le nom de son fichier de méta données placé dans `/usr/share/sso/metadata` (sans l'extension .xml).

`RelayState` est une information indiquant au fournisseur de service ou rediriger l'utilisateur une fois son identité confirmée. Les données à envoyées peuvent être l'URL d'une application protégée par le fournisseur de service, l'identifiant de l'établissement depuis lequel l'utilisateur se connecte, ... (variable suivant le fournisseur de service).

L'accès à cette URL va déclencher la cinématique suivante :

- vérification par le serveur EoleSSO de la session SSO de l'utilisateur (si il n'est pas connecté, une nouvelle session est établie après saisie des identifiants) ;
- génération et envoi d'une réponse SAML au FS pour lui indiquer l'identité de l'utilisateur ;
- Traitement de la réponse reçue par le fournisseur de service et recherche des informations sur l'utilisateur dans le référentiel du FS (profil associé, permissions, ...) ;
- Redirection de l'utilisateur sur la ressource définie par RelayState (ou sur une ressource définie par défaut le cas échéant).

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

Accéder à une ressource en tant que fournisseur de service

Dans le cas où le serveur EoleSSO est utilisé comme fournisseur de service, l'accès à une ressource peut se faire de 2 façons :

1. en envoyant directement une réponse SAML d'authentification sur l'URL de traitement des assertions d'EoleSSO (FS) depuis le fournisseur d'identité (processus dit 'IDP initiated'). Une URL de service à atteindre peut être fournie par le paramètre RelayState.
2. en envoyant une requête SAML d'authentification depuis EoleSSO (FS) en spécifiant le fournisseur d'identité à interroger et le service à atteindre après authentification (méthode préférable).

Dans les 2 cas, une fois l'assertion reçue validée, une session est établie sur le serveur EoleSSO.

L'utilisateur est ensuite redirigé sur l'URL du service à atteindre (il est possible de définir un service par défaut pour chaque fournisseur d'identité, voir le chapitre précédent concernant la configuration des associations).



Dans le cas d'un serveur Scribe servant de fournisseur de service, il est possible par exemple de spécifier dans RelayState l'accès à l'application Pydio (accès au FTP de Scribe). Si le fournisseur d'identité est également un serveur EoleSSO (adresse_FI), l'accès se fera à travers l'adresse suivante (cas 1) :

```
https://adresse_FI:8443/saml?sp_ident=id_scribe&RelayState=https://
```

L'adresse à utiliser dans le cas 2 serait la suivante :

```
https://adresse_scibe:8443/discovery?idp_ident=id_fournisseur_ident
```

Gestion de la Déconnexion

Le serveur EoleSSO intègre la notion de déconnexion unique (single logout) dans le cadre de l'établissement d'un lien de fédération.

La procédure de déconnexion peut être initiée de deux façons.

1. Directement depuis le service EoleSSO, en accédant à l'URL : https://adresse_serveur_sso:8443/logout;
2. En utilisant le système de déconnexion de l'entité partenaire si celle-ci gère également la déconnexion unique.

Dans le deuxième cas, une demande de déconnexion au format SAML est envoyée au service EoleSSO, qui va enclencher la déconnexion et envoyer une confirmation une fois la procédure terminée (une adresse de redirection peut également être fournie avec la demande de déconnexion).

Une fois la procédure de déconnexion enclenchée, EoleSSO va envoyer une demande de déconnexion SAML à chaque entité partenaire sur laquelle l'utilisateur a établi une session par fédération.

Dans le cas où EoleSSO est également utilisé pour accéder à des applications locales, par exemple, pour le portail Envole du serveur Scribe, Il va également envoyer des requêtes de déconnexion aux applications ayant demandé un ticket au serveur SSO (ce comportement peut être désactivé dans la configuration du serveur).

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



Le mode de fonctionnement de la déconnexion unique est basé sur une suite d'aller-retours (par redirection) vers les différentes entités.

Dans le cas où une erreur se produit lors de la procédure de connexion sur une entité partenaire, il se peut que la procédure s'arrête dans un état de déconnexion partielle (la déconnexion n'est pas propagée à toutes les entités).

Dans ce cas, plusieurs solutions sont prévues pour limiter le problème :

- si l'URL de déconnexion du serveur EoleSSO est à nouveau sollicitée, le serveur va considérer que la dernière requête de déconnexion envoyée a échoué et va reprendre la procédure en passant au partenaire suivant.

- si une autre URL du serveur est sollicitée (création d'une nouvelle session, demande d'authentification par une application, ...), la session SSO précédente est dans tous les cas invalidée par le serveur (il devra donc se ré-authentifier).

Dans le dernier cas, il se peut que l'utilisateur possède toujours une session sur une entité partenaire.

La seule façon de résoudre le problème est de **fermer le navigateur**.

6.5.5. Gestion des sources d'authentification multiples

Il est possible de se retrouver confronté à des problèmes d'utilisateurs homonymes dans le cas où plusieurs annuaires sont utilisés comme source d'authentification ou dans le cadre d'un réplica d'annuaire distant comme c'est le cas avec le module Seshat.

EoleSSO a été amélioré pour prendre en compte ce problème.

Principe de fonctionnement

Si plusieurs annuaires sont configurés, EoleSSO va gérer une branche de recherche par annuaire. Lorsqu'un utilisateur va saisir son identifiant, une recherche va être effectuée dans chaque annuaire afin de vérifier si celui-ci est présent plusieurs fois. Si c'est le cas, une liste va être affichée pour permettre à l'utilisateur de choisir sa provenance.

La liste affichée est basée sur le libellé renseigné pour chaque annuaire dans l'interface de configuration du module. Il convient donc de bien renseigner ces informations pour que l'utilisateur soit capable de choisir.

Cas particulier : la réplication d'annuaire (Scribe/Seshat)

Gestion de la liste de choix de la source d'authentification

Dans le cadre de la réplication, l'unique annuaire à utiliser est celui du serveur hébergeant EoleSSO.

Des procédures ont été mises en place pour gérer automatiquement des branches de recherche sur chaque annuaire répliqué.

La procédure `active_replication` nécessite que les 2 serveurs (serveur répliqué/serveur de réplication) soient enregistrés sur le serveur Zéphir.

Lorsque le serveur Zéphir va envoyer au serveur répliquant les éléments nécessaires à la mise œuvre de la réplication, il va également lui envoyer un fichier décrivant l'établissement dans lequel la machine

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

répliquée est installée (le libellé doit donc être renseigné correctement dans l'application Zéphir).

Sur le module Seshat, il est possible de demander manuellement une récupération de ce fichier auprès du serveur Zéphir en lançant le script :

```
/usr/share/sso/update_etabs.py
```

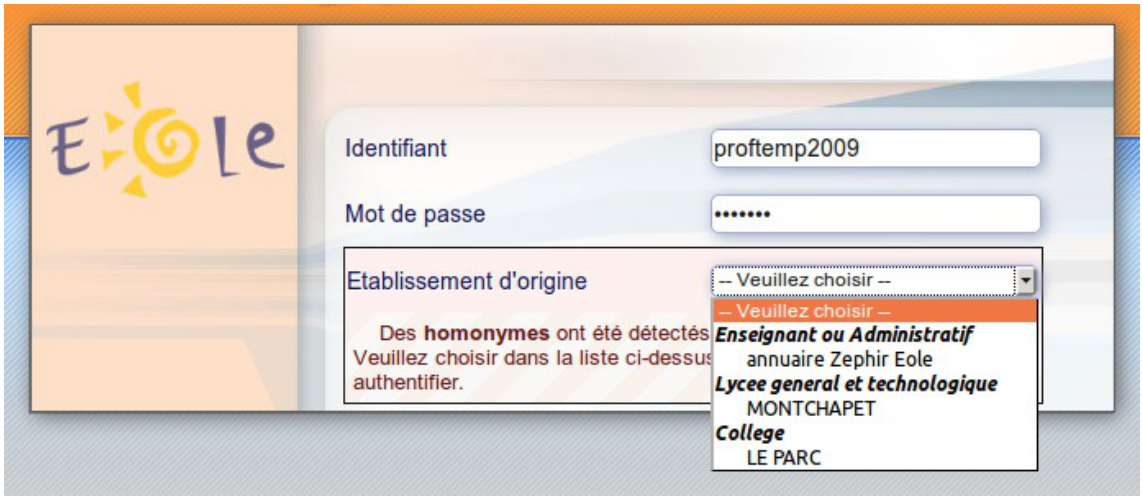
Les informations sont stockées dans le fichier `/etc/ldap/replication/zephir/etabs.ini` dont le format est le suivant :

```
[rne]
libelle_etab=....
type_etab=....
portail_etab=...
```

Ces informations sont détectées automatiquement par le serveur Zéphir lorsque c'est possible.

Le numéro RNE sert à faire la liaison avec les branches de recherche disponibles dans EoleSSO (en se basant sur le DN qui est du type `ou=<rne>,ou=ac-<academie>,ou=education,o=gouv,c=fr`).

Le type d'établissement permet de créer des sections dans la liste présentée à l'utilisateur afin d'en faciliter la lecture.



Dans le cas où toutes les informations ne sont pas détectées ou en cas de données mal renseignées dans l'application Zéphir, il est possible de modifier ou d'ajouter des informations en créant un(des) fichier(s) au même format.

Ils sont à placer dans le répertoire `/etc/ldap/replication` et doivent se nommer `etabs_xxx.ini` (la partie xxx n'est pas déterminante). Les données présentes dans ces fichiers seront prioritaires sur celles remontées par le serveur Zéphir.

Par exemple, le fichier suivant permet de corriger l'adresse du portail ENT de l'établissement 000000A1 (si celle-ci n'est pas correcte ou absente). Les autres informations remontées par le serveur Zéphir seront conservées (libellé et type d'établissement)

`/etc/ldap/replication/etabs_perso.ini`

```
[000000A1]
portail_etab=ent.mon_etab.ac-acd.fr
```

Dans l'affichage final (voir capture d'écran ci dessus), le libellé de l'établissement sera affiché en majuscules.

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

> Si une description commence par le type d'établissement (ex : COLLEGE VICTOR HUGO), celui-ci sera supprimé pour simplifier l'affichage.
>
> Au démarrage du service `eole-sso`, ces informations sont lues et rassemblées dans le fichier `/usr/share/sso/interface/scripts/etabs.js` qui est utilisé pour générer la liste des établissements dans lesquels un identifiant donné est présent.
>
> Si l'application `eole-dispatcher` est installée sur la machine, un fichier d'informations est également généré pour celle-ci dans `/var/www/html/dispatcher/utils/etabs.ini`. Cette application permet de rediriger automatiquement les utilisateurs vers les portails ENT auxquels ils ont accès (pour plus d'informations, se reporter aux annexes).

Aide au choix de la source d'authentification

Lorsque des homonymes sont détectés, la mire d'authentification va générer la liste des choix disponibles.

Pour aider l'utilisateur dans sa décision, différentes informations sont affichées.

Si un fichier `/usr/share/sso/interface/login_help.tmpl` est présent, un lien apparaîtra sur la mire d'authentification (`Quel est mon identifiant?`). Un survol de ce lien avec la souris fait apparaître le contenu du fichier sous forme d'un cadre en surimpression (classes liées à `a.aide` dans la feuille de style).

Un exemple est fourni dans le fichier `/usr/share/sso/interface/login_help_example.tmpl`.

Le but de ce cadre est d'indiquer à l'utilisateur l'identifiant qu'il doit utiliser.



Un deuxième cadre d'information est affiché lorsque des homonymes ont été trouvés pour l'identifiant saisi par l'utilisateur (`#homonyme` et `#homonymetext` dans la feuille de style).

Le contenu de celui-ci est conditionné par les choix disponibles. Le but est d'aider à choisir parmi les sources proposées.

Le début du texte est générique et indique à l'utilisateur que plusieurs entrées sont disponibles pour l'identifiant renseigné.

Il est ensuite possible de spécifier un fichier d'information pour chaque annuaire LDAP, dont le contenu sera ajouté au cadre si l'identifiant entré y est présent (l'information doit donc être au format HTML).

Un exemple est fourni dans `/usr/share/sso/interface/personnel_acad.html`, et donne le résultat suivant :

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



Voir aussi...

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.217]

6.6. Personnalisation de la mire SSO

Ce chapitre répertorie les différentes possibilités offertes pour personnaliser l'apparence de la page d'authentification du serveur EoleSSO (pour une meilleure intégration dans l'environnement existant, et en particulier dans le cadre d'un portail d'accès aux ressources d'un établissement).

Message d'avertissement (CNIL)

Il est prévu de pouvoir afficher un message relatif à la déclaration CNIL du site.

- mettre le texte du message d'avertissement (formaté en HTML) dans un fichier `avertissement.txt` qui est à placer dans le répertoire `/usr/share/sso/interface/theme` ;
- relancer le service : `CreoleService eole-sso restart`

Exemple de déclaration

Conformément à la loi, nous vous informons que ce site a fait l'objet d'une déclaration de traitement automatisé d'informations nominatives auprès de la CNIL Loi du 6 janvier 1978 relative à l' « Informatique et aux Libertés » :

Conformément à la loi n° 78-17 du 6 janvier 1978, vous pouvez à tout moment accéder aux informations personnelles vous concernant et détenues par l'établissement, demander leur modification ou leur suppression. Ainsi, vous pouvez, à titre irrévocable, demander que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations vous concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte ou l'utilisation, la communication ou la conservation est interdite.

Pour toutes demandes, veuillez contacter l'administrateur à l'adresse : administrateur@etablissement.fr

CSS : Méthode 1

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

La feuille de style par défaut /usr/share/sso/interface/main.css importe les feuilles de style ./theme/style/theme.css et ./leaves.css :

```
[ …]
@import url(./leaves.css);
@import url(./theme/style/theme.css);
[…]
```

Comme le fichier ./theme/style/theme.css est appelé en deuxième dans la feuille il va permettre une surcharge de la première feuille de style ./leaves.css.

Éditer le fichier vide ./theme/style/theme.css appelé dont le chemin absolu est /usr/share/sso/interface/theme/style/theme.css.

S'inspirer des balises de style utilisées dans le fichier /usr/share/sso/interface/leaves.css pour les surcharger.

Utiliser le répertoire /usr/share/sso/interface/theme/images pour ajouter vos images.

Recharger votre page d'authentification sans même redémarrer le service `eole-sso`, la feuille de style est importée avec les modifications.



Cette méthode n'est pas compatible avec la personnalisation Envole Thèmes. Celui-ci écrase le contenu du fichier /usr/share/sso/interface/theme/style/theme.css à chaque reconfigure. Il est possible d'enlever Envole Thèmes avec la commande suivante : `# apt-get remove eole-envole-themes`

CSS : Méthode 2

Un certain nombre de thèmes sont fournis dans le répertoire /usr/share/sso/interface/themes/.

Il suffit de copier le thème voulu pour le rendre actif :

```
# /bin/cp -R /usr/share/sso/interface/themes/<nomDuTheme>/* /usr/share/sso/interface/theme
```

Recharger votre page d'authentification sans même redémarrer le service `eole-sso`, la feuille de style est importée avec les modifications.



N'hésitez pas à proposer votre thème, il sera ajouté au paquetage et reversé à la communauté d'utilisateurs.

CSS : Méthode 3

La feuille de style CSS par défaut utilisée lors de l'affichage de la page d'authentification au portail est :

/usr/share/sso/interface/leaves.css

Il est possible d'utiliser une feuille de style CSS personnalisée pour la mire SSO.

Les fichiers CSS à utiliser sont à placer dans :

/usr/share/sso/interface/

Dupliquer la feuille de style originale sous un autre nom.

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

Modifier à volonté `votre_nouvelle_feuille.css`

Renseigner le nom de votre feuille sans l'extension (`.css`) dans l'onglet `Eole sso` depuis l'interface de configuration du module.

Réaliser autant de feuilles de style que souhaités.

- Si vous faites appel à des images, placez-les dans : `/usr/share/sso/interface/images/`
- Il est possible de passer le nom de la CSS en paramètre dans URL : `http://<adresse serveur>/css=<nom de la feuille CSS>`
- Si vous utilisez un client phpCAS, il faudra modifier le client pour utiliser cette méthode (les URLs sont calculées par le client).

Choix de la CSS par le filtre SSO

Si un fichier CSS porte le même nom qu'un filtre d'application (par exemple, `ead2.css`), cette feuille de style CSS sera automatiquement utilisée lors des demandes à cette application (dans le cadre d'un portail web par exemple).

6.7. Configuration d'EoleSSO en mode cluster

Fonctionnement en mode cluster

EoleSSO peut être paramétré pour stocker les sessions SSO dans une base de données Redis[p.776] (locale ou distante).

En branchant plusieurs services EoleSSO sur la même base, il est possible de mettre en place une configuration de type cluster en répartition de charge ou en basculement.

Cette documentation couvre seulement la configuration d'un (ou plusieurs) services EoleSSO et d'un service Redis pour permettre le stockage des sessions SSO dans une base de données partagée. La configuration de la répartition de charge ou du basculement (à travers ha-proxy ou autre système) n'est pas abordée ici.

La configuration peut se faire :

- en mode serveur (partage d'une base Redis) ;
- en mode client (accès à la base Redis par EoleSSO).

Installation et configuration en mode serveur

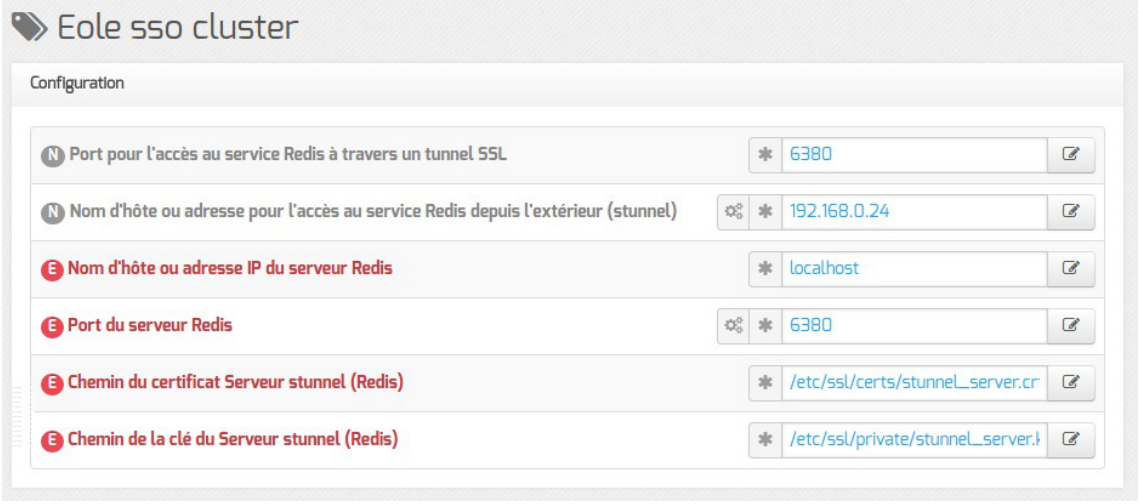
Sur un module Eole, il faut installer le paquet dédié à l'aide de la commande suivante :

```
# apt-eole install eole-sso-cluster-server
```

Celui-ci va installer un serveur Redis et configurer une instance spécifique sur le port `6380` (service redis-eolesso), ainsi qu'un service stunnel4 permettant de sécuriser l'accès à l'aide d'un tunnel SSL.

Dans l'interface de configuration du module apparaît le nouvel onglet `Eole sso cluster`.

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



Tous les paramètres sont renseignés pour une utilisation par défaut, mais il est possible d'effectuer les réglages suivants :

- `Port pour l'accès au service Redis à travers un tunnel SSL` : Permet de modifier le port sur lequel les clients se connecteront pour accéder à la base de données.
- `Nom d'hôte ou adresse pour l'accès au service Redis depuis l'extérieur (stunnel)` : Permet de définir l'adresse sur laquelle le tunnel sera disponible. Par défaut, l'adresse IP de l'interface 0 est utilisée.
- `Chemin du certificat Serveur stunnel (Redis)` et `Chemin de la clé du Serveur stunnel (Redis)` : Permettent de renseigner un certificat serveur spécifique pour le tunnel SSL. Par défaut, un certificat est généré automatiquement (`/etc/ssl/certs/stunnel_client.crt`).
- `Nom d'hôte ou adresse IP du serveur Redis` et `Port du serveur Redis` : Permettent de modifier le port sur lequel l'instance de Redis écoute, ou d'accéder à un autre serveur Redis. Si le nom d'hôte est différent de 127.0.0.1 ou localhost, le service local redis-eolesso est désactivé.



En cas d'utilisation d'un serveur Redis non local, il faut être conscient que les échanges circuleront en clair, ce qui est déconseillé en dehors d'un réseau sécurisé.

Installation et configuration en mode client

Sur un module Eole dont le service EoleSSO doit être utilisé en mode cluster il faut installer le paquet adéquat à l'aide de la commande suivante :

```
# apt-eole install eole-sso-cluster-client
```

Celui-ci va installer les librairies nécessaires à l'accès Redis par EoleSSO, ainsi qu'un service stunnel4 configuré en mode client.

Dans l'interface de configuration du module apparaît le nouvel onglet `Eole sso cluster`.

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



- `Port pour l'accès au service Redis à travers un tunnel SSL` : Permet de spécifier le port sur lequel le service stunnel4 va se connecter. Il doit correspondre à la valeur configurée sur la machine en mode serveur.
- `Nom d'hôte ou adresse IP d'accès au service Redis distant (stunnel)` : Renseigner l'adresse choisie pour l'accès à Redis sur la machine en mode serveur.
- Les variables chemin du certificat et de la clé du client stunnel permettent d'utiliser un certificat spécifique pour le service stunnel local. Attention, ce certificat doit être un certificat client (nsCertType = client). par défaut, un certificat est généré automatiquement (`/etc/ssl/certs/stunnel_client.crt`)

Installation et configuration des 2 modes sur la même machine

Il est possible d'installer les paquets `eole-sso-cluster-server` et `eole-sso-cluster-client` sur une seule machine.

Dans ce cas, le service EoleSSO de cette machine accédera directement à la base Redis.

Le service *stunnel* sera configuré en mode serveur pour permettre l'accès à la base par d'autres instances d'EoleSSO.

Tunnel SSL

Échange des clés

Une fois la configuration renseignée, reconfigurer le serveur et générer les certificats à l'aide de la commande reconfigure sur chaque machine utilisée.

Il faut ensuite procéder à un échange des certificats entre le serveur et le client pour que la connexion par tunnel soit possible :

- Exécuter `reconfigure` sur chaque machine après avoir copié les fichiers.

Sur la machine en mode serveur il faut recopier dans le répertoire `/etc/stunnel/eole/` les fichiers `/etc/ssl/certs/ca_local.crt` et `/etc/ssl/certs/stunnel_client.crt` de chaque serveur en mode client. Il faut les renommer afin de ne pas les écraser au fur et à mesure de l'ajout de clients.

```
# scp root@<adresse_client> :/etc/ssl/certs/ca_local.crt /etc/stunnel/eole/ca_[adresse_client].crt
# scp root@<adresse_client> :/etc/ssl/certs/stunnel_client.crt
```


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

`/etc/stunnel/eole/stunnel_[nom_client].crt`

Sur chaque machine en mode client il faut recopier dans le répertoire `/etc/stunnel/eole/` les fichiers `/etc/ssl/certs/ca_local.crt` et `/etc/ssl/certs/stunnel_server.crt` de chaque serveur en mode serveur.

```
# scp root@<adresse_client> :/etc/ssl/certs/ca_local.crt /etc/stunnel/eole/
# scp root@<adresse_client> :/etc/ssl/certs/stunnel_server.crt /etc/stunnel/eole/
```

Utilisation de certificats spécifiques

En cas d'utilisation d'un autre certificat que celui généré par défaut, les fichiers à échanger sont :

- le fichier du certificat utilisé pour le service *stunnel* ;
- toute les autorités de certification permettant de valider celui-ci (autorité racine et éventuels certificats intermédiaires).

Vérifier le bon fonctionnement du tunnel

Une fois les machines configurées, il faut se connecter sur un des serveurs en mode client, se placer dans le répertoire `/usr/share/sso/`, exécuter l'interpréteur `python` et saisir le code suivant :

```
>>> import config, redis
>>> r = redis.Redis(host=config.REDIS_HOST, port=config.REDIS_PORT)
>>> r.ping()
```

La dernière commande doit retourner `True`.

Si la commande renvoie un message d'erreur se terminant par `Error while reading from socket: (104, 'Connection reset by peer')` , cela indique généralement un problème de validation des certificats (par le serveur ou le client), ou une interdiction d'accès au port du tunnel par le serveur (pare-feu, TCP Wrapper[p.780]...).

6.8. Répartition de charge EoleSSO en mode cluster

Cette documentation a pour but de décrire la mise en place d'une configuration HAProxy afin de pouvoir mettre plusieurs services EoleSSO en cluster et de gérer la répartition de charge.

https://www.haproxy.com/fr/

Cette documentation décrit également la mise en place de 2 services pour suivre les métriques d'EoleSSO :

- Prometheus : https://prometheus.io/
- Grafana : https://grafana.net/

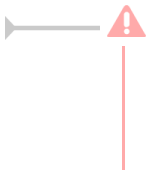
On suppose l'existence de 3 serveurs EoleSSO qui écoutent sur le port 443 dont les DNS sont les suivants :

- `sso-1.ac-academie.fr` ;
- `sso-2.ac-academie.fr` ;

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

- `sso-3.ac-academie.fr`.

Un quatrième serveur doit héberger le service ha-proxy avec pour nom DNS `sso-ha.ac-academie.fr`.



Le serveur hébergeant le service ha-proxy du cluster doit avoir un nom de domaine différent de celui du cluster de serveur web même si les 2 noms de domaine pointent sur la même adresse IP.

Pour maintenir et déployer la configuration (certificats pour stunnel, metadata, filtres, thèmes, CSS, attributs calculés) sur les différents serveurs EoleSSO il est possible d'utiliser Ansible.

Installation d'HAProxy

Sur le serveur `sso-ha.ac-academie.fr` :

```
# apt-eole install haproxy
```

Configuration d'HAProxy

Procéder à la configuration basique d'HAProxy (non détaillée ici).

Éditer le fichier de configuration /etc/haproxy/haproxy.cfg et ajouter les lignes suivantes :

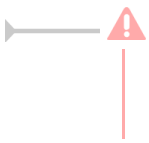
```
global
  ...
   # Les serveurs étant gérés par vous, la vérification ssl peut être désactivée
  ssl-server-verify none

frontend https-in
     bind <IP DU SERVEUR SSO-HA>:443 ssl crt <CHEMIN DU CERTIFICAT PEM>
     option   forwardfor
     redirect scheme https if !{ ssl_fc }
     default_backend    sso_servers

backend sso_servers
     balance         roundrobin
     cookie SSONAME  insert indirect nocache
     server sso-1.ac-academie.fr   sso-1.ac-academie.fr:443 ssl cookie sso1 check
     server sso-2.ac-academie.fr   sso-2.ac-academie.fr:443 ssl cookie sso2 check
     server sso-3.ac-academie.fr   sso-3.ac-academie.fr:443 ssl cookie sso3 check
```


<IP DU SERVEUR SSO-HA> : est à remplacer par l'adresse IP de votre serveur HAProxy

<CHEMIN DU CERTIFICAT PEM> : chemin du certificat + key



Penser à redémarrer le service haproxy :

```
# service haproxy restart
```

Mise en place de Prometheus et de Grafana

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

Il faut mettre en place un serveur Prometheus qui sera chargé de collecter les données fournies par nos serveurs EoleSSO et mettre en place Grafana pour avoir un visuel des métriques.

Pour des raisons de simplicité, des micro-services docker sont utilisés pour fournir ces deux applications, aussi il faut installer les paquets `docker` et `docker-compose`.

Il peut être intéressant de dissocier ces services du serveur HAPproxy, car il pourrait servir à d'autres serveurs, ce serveur de monitoring porte le nom DNS `monitoring.ac-academie.fr`.

Exemple de configuration de Prometheus

Exemple de configuration, contenu dans le fichier `/shared/prometheus/monitoring-compose.yml` :

```
prometheus:
  image: prom/prometheus
  ports:
    - 9090:9090
  volumes:
    - /shared/prometheus/etc/:/etc/prometheus/
    - /shared/prometheus/data/:/prometheus

grafana:
  image: grafana/grafana:4.1.1
  ports:
    - 3000:3000
  volumes:
    - /shared/prometheus/grafana/:/var/lib/grafana/
  env_file:
    - /shared/prometheus/grafana.config.monitoring
```

Configuration de Prometheus

Le fichier de configuration de prometheus `/shared/prometheus/etc/prometheus.yml` contient :

```
global:
  scrape_interval: 60s

scrape_configs:
  - job_name: "eole_sso"
    metrics_path: /metrics
    scheme: https
    tls_config:
      insecure_skip_verify: true
    static_configs:
        - targets:
            - sso-1.ac-academie.fr
            - sso-2.ac-academie.fr
            - sso-3.ac-academie.fr
```

Configuration de Grafana

Configuration de Grafana dans le fichier `/shared/prometheus/grafana.config.monitoring`

```
GF_SECURITY_ADMIN_PASSWORD=VOTRE_MOT_DE_PASSE_ADMIN
GF_USERS_ALLOW_SIGN_UP=false
http_proxy=PROXY_HOST:PROXY_PORT
https_proxy=PROXY_HOST:PROXY_PORT
```


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

Modifier les valeurs de :
VOTRE_MOT_DE_PASSE_ADMIN
PROXY_HOST
PROXY_PORT

La documentation de Grafana décrit les paramètres possibles :
http://docs.grafana.org/installation/configuration/

JSON pour le tableau de bord Grafana

```
{
  "annotations": {
    "list": []
  },
  "editable": true,
  "gnetId": null,
  "graphTooltip": 0,
  "hideControls": false,
  "id": 16,
  "links": [],
  "refresh": "1m",
  "rows": [
    {
      "collapse": false,
      "height": 237,
      "panels": [
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 7,
          "grid": {},
          "id": 9,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 0,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
```


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

```
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 4,
          "stack": true,
          "steppedLine": false,
          "targets": [
            {
              "expr": "eolesso_login_gauge",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_login_gauge",
              "refId": "A",
              "step": 120
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "Nombre de tickets de login (TicketCache)",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        },
        {
          "bars": true,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 10,
          "grid": {},
          "id": 4,
```


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

```
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": false,
          "linewidth": 0,
          "links": [],
          "nullPointMode": "null as zero",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 4,
          "stack": true,
          "steppedLine": true,
          "targets": [
            {
              "expr": "(rate(eolesso_sessions_new_counter[10m]))*60*2",
              "intervalFactor": 2,
              "legendFormat": "{{host}} [{{authclass}}]",
              "metric": "eolesso_sessions_new_counter",
              "refId": "A",
              "step": 120
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "Nb connexions/s",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "individual"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
```


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

```
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      },
      {
        "aliasColors": {
          "sso-3": "#82B5D8",
          "sso-1": "#7EB26D",
          "sso-2": "#EAB839"
        },
        "bars": false,
        "datasource": null,
        "editable": true,
        "error": false,
        "fill": 3,
        "grid": {},
        "id": 2,
        "legend": {
          "avg": false,
          "current": false,
          "max": false,
          "min": false,
          "show": true,
          "total": false,
          "values": false
        },
        "lines": true,
        "linewidth": 1,
        "links": [],
        "nullPointMode": "null",
        "percentage": false,
        "pointradius": 5,
        "points": false,
        "renderer": "flot",
        "seriesOverrides": [],
        "span": 4,
        "stack": true,
        "steppedLine": false,
        "targets": [
          {
            "expr": "eolesso_sessions_nb_gauge",
            "intervalFactor": 1,
            "legendFormat": "{{host}}",
            "metric": "eolesso_sessions_gauge",
            "refId": "A",
            "step": 60
          }
        ],
        "thresholds": [],
        "timeFrom": null,
        "timeShift": null,
        "title": "Nombre de tickets de sessions (auth)",
        "tooltip": {
          "msResolution": false,
          "shared": true,
          "sort": 0,
          "value_type": "cumulative"
```


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

```
        },
        "type": "graph",
        "xaxis": {
          "mode": "time",
          "name": null,
          "show": true,
          "values": []
        },
        "yaxes": [
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      }
    ],
    "repeat": null,
    "repeatIteration": null,
    "repeatRowId": null,
    "showTitle": false,
    "title": "Row",
    "titleSize": "h6"
  },
  {
    "collapse": false,
    "height": "250px",
    "panels": [
      {
        "aliasColors": {
          "sso-3": "#82B5D8",
          "sso-1": "#7EB26D",
          "sso-2": "#EAB839"
        },
        "bars": false,
        "datasource": null,
        "editable": true,
        "error": false,
        "fill": 7,
        "grid": {},
        "id": 7,
        "legend": {
          "avg": false,
          "current": false,
          "max": false,
          "min": false,
          "show": true,
          "total": false,
          "values": false
```


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

```
        },
        "lines": true,
        "linewidth": 1,
        "links": [],
        "nullPointMode": "connected",
        "percentage": false,
        "pointradius": 5,
        "points": false,
        "renderer": "flot",
        "seriesOverrides": [],
        "span": 6,
        "stack": true,
        "steppedLine": true,
        "targets": [
          {
            "expr": "eolesso_calcdata_gauge",
            "intervalFactor": 2,
            "legendFormat": "{{host}}",
            "metric": "eolesso_calcdata_gauge",
            "refId": "A",
            "step": 60
          }
        ],
        "thresholds": [],
        "timeFrom": null,
        "timeShift": null,
        "title": "taille du cache des attributs calculés",
        "tooltip": {
          "msResolution": false,
          "shared": true,
          "sort": 0,
          "value_type": "cumulative"
        },
        "type": "graph",
        "xaxis": {
          "mode": "time",
          "name": null,
          "show": true,
          "values": []
        },
        "yaxes": [
          {
            "format": "decbytes",
            "label": "Octets",
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      },
      {
```


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

```
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 5,
          "grid": {},
          "id": 8,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 6,
          "stack": true,
          "steppedLine": false,
          "targets": [
            {
              "expr": "eolesso_userdata_gauge",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_userdata_gauge",
              "refId": "A",
              "step": 60
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "taille du cache des attributs ldap",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
```


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

```
        "yaxes": [
          {
            "format": "decbytes",
            "label": "Octets",
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          }
        ]
      }
    ],
    "repeat": null,
    "repeatIteration": null,
    "repeatRowId": null,
    "showTitle": false,
    "title": "New row",
    "titleSize": "h6"
  },
  {
    "collapse": false,
    "height": "250px",
    "panels": [
      {
        "aliasColors": {
          "sso.ac-reunion.fr:4430": "#82B5D8",
          "sso.ac-reunion.fr:4431": "#E5A8E2",
          "sso.ac-reunion.fr:4432": "#AEA2E0"
        },
        "bars": false,
        "datasource": null,
        "editable": true,
        "error": false,
        "fill": 0,
        "grid": {},
        "id": 3,
        "legend": {
          "alignAsTable": true,
          "avg": false,
          "current": true,
          "max": false,
          "min": false,
          "rightSide": true,
          "show": true,
          "total": false,
          "values": true
        },
        "lines": true,
        "linewidth": 1,
        "links": [],
        "nullPointMode": "null as zero",
        "percentage": false,
```


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

```
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 6,
          "stack": false,
          "steppedLine": false,
          "targets": [
            {
              "expr": "process_virtual_memory_bytes{job='eole_sso'}",
              "intervalFactor": 2,
              "legendFormat": "{{instance}}",
              "refId": "A",
              "step": 60
            }
          ],
          "thresholds": [
            {
              "colorMode": "critical",
              "fill": true,
              "line": true,
              "op": "gt",
              "value": 1517522817
            }
          ],
          "timeFrom": null,
          "timeShift": null,
          "title": "Mémoire utilisée",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "individual"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
          },
          "yaxes": [
            {
              "format": "bytes",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        },
```


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

```
        {
          "aliasColors": {
            "sso-3": "#82B5D8",
            "sso-1": "#7EB26D",
            "sso-2": "#EAB839"
          },
          "bars": false,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 4,
          "grid": {},
          "id": 1,
          "legend": {
            "avg": false,
            "current": false,
            "max": false,
            "min": false,
            "show": true,
            "total": false,
            "values": false
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "points": false,
          "renderer": "flot",
          "seriesOverrides": [],
          "span": 6,
          "stack": true,
          "steppedLine": false,
          "targets": [
            {
              "expr": "eolesso_appticket_gauge{job='eole_sso'}",
              "intervalFactor": 2,
              "legendFormat": "{{host}}",
              "metric": "eolesso_appticket_gauge",
              "refId": "A",
              "step": 60
            }
          ],
          "thresholds": [],
          "timeFrom": null,
          "timeShift": null,
          "title": "Nombre de Tickets applicatifs (AppTicket)",
          "tooltip": {
            "msResolution": false,
            "shared": true,
            "sort": 0,
            "value_type": "cumulative"
          },
          "type": "graph",
          "xaxis": {
            "mode": "time",
            "name": null,
            "show": true,
            "values": []
```


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

```
          },
          "yaxes": [
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            },
            {
              "format": "short",
              "label": null,
              "logBase": 1,
              "max": null,
              "min": null,
              "show": true
            }
          ]
        }
      ],
      "repeat": null,
      "repeatIteration": null,
      "repeatRowId": null,
      "showTitle": false,
      "title": "New row",
      "titleSize": "h6"
    }
  ],
  "schemaVersion": 14,
  "style": "dark",
  "tags": [],
  "templating": {
    "list": []
  },
  "time": {
    "from": "now-12h",
    "to": "now"
  },
  "timepicker": {
    "refresh_intervals": [
      "5s",
      "10s",
      "30s",
      "1m",
      "5m",
      "15m",
      "30m",
      "1h",
      "2h",
      "1d"
    ],
    "time_options": [
      "5m",
      "15m",
      "1h",
      "6h",
      "12h",
      "24h",
      "2d",
```


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

```
      "7d",
      "30d"
    ]
  },
  "timezone": "browser",
  "title": "SSO Copy",
  "version": 0
}
```

Monitoring

Lancer l'environnement de monitoring

```
# cd /shared/prometheus/
```

```
# docker-compose -f prometheus-compose.yml start
```

Par défaut Grafana écoute sur le port 3000 et Prometheus sur le port 9090

Pour accéder à Grafana :

http://monitoring.ac-academie.fr:3000

Pour accéder à Prometheus :

http://monitoring.ac-academie.fr:9090

6.9. Compléments de configuration EoleSSO

6.9.1. Résumé des fichiers et liens

Fichiers de configuration

Fichiers de base

- `/usr/share/sso/config.py` : fichier de configuration principal de l'application (sur un module Eole, la configuration est gérée via Creole)
- `/usr/share/sso/app_filters/*_apps.ini` : définition des applications et spécification du filtre à utiliser
- `/usr/share/sso/app_filters/*.ini` : fichiers de description des filtres d'attributs
- `/usr/share/sso/user_infos/*.py` : fonctions de calcul d'attributs supplémentaires
- `/usr/share/sso/interface/theme` : répertoire pour personnalisation de la CSS des pages d'authentification

Fichiers spécifiques au fonctionnement en mode SAML

- `/usr/share/sso/metadata/*.xml` : fichiers metadata des entités partenaires (doit contenir le certificat utilisé pour la signature des requêtes)
- `/usr/share/sso/metadata/attributes.ini` : définition des attributs requis/optionnels en tant que fournisseur de service (obsolète)
- `/usr/share/sso/attribute_sets/*.ini` : description de jeux d'attributs pour la fédération via SAML
- `/usr/share/sso/attribute_sets/associations*.ini` : fichiers de configuration des associations avec des fournisseurs d'identité

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

URL principales

Toutes les URL du service EoleSSO décrites ci-dessous commencent par https://addresse_serveur:8443 (port par défaut, peut être différent suivant la configuration du service).

URL Générales

- `/ (sans paramètres)` : Page d'accueil, le formulaire d'authentification est présenté et une session SSO est créée après validation. Si l'utilisateur est déjà authentifié il est redirigé sur la page `/loggedin` ou une liste des fédérations établies et des applications ayant un ticket est affichée
- `/logout` : adresse de déconnexion de la session actuelle (gestion du Single Logout pour les protocoles le supportant)

URL spécifiques à CAS

- `/?service=X` : Adresse d'obtention d'un ticket CAS pour les applications clientes (à utiliser comme URI de base dans la configuration des clients CAS)
  - `service` est l'URL de l'application désirant obtenir un ticket. Une fois la validité de la session SSO vérifiée, le service EoleSSO redirige l'utilisateur sur cette URL en passant le ticket en paramètre (nom du paramètre : `ticket`)
- `/validate?service=X&ticket=Y` (ou `/serviceValidate`) : adresse de validation des tickets d'application CAS ;
  - `service` est l'URL du service pour lequel le ticket a été délivré
  - `ticket` est le ticket a vérifier (de type ST)
- `/proxyValidate?service=X&ticket=Y&pgtUrl=Z` : adresse de validation des tickets d'application CAS en mode proxy
  - `ticket` est le ticket à vérifier (de type ST ou PT) ;
- `/samlValidate` : adresse de validation des tickets CAS au format SAML 1. Les paramètres doivent être passés par méthode POST (méthode supportée par les client CAS java 3.1.X, phpCAS 1.1.0 et .NET CAS Client). Pour plus de détail sur, se reporter à la page http://en.wikipedia.org/wiki/SAML_1.1
  - `TARGET` : URL à laquelle la réponse doit être envoyée
  - Le corps de la requête doit contenir la requête SAML dans une enveloppe SOAP. Le ticket à valider est fourni comme valeur de l'élément AssertionArtifact
- `/proxy?pgt=X?targetService=Y` : adresse d'obtention d'un ticket de type proxy

URL spécifiques à SAML 2

- `/saml/metadata` : adresse de récupération des méta-données SAML du serveur (fournisseur d'identité et fournisseur de services)
- `/saml?sp_ident=X&RelayState=Y&index=Z` : adresse à utiliser pour envoyer une assertion d'authentification SAML à un fournisseur de services
  - `sp_ident` est l'identifiant de ce partenaire (ou le nom de son fichier metadata sans l'extension .xml)
  - `RelayState` est une information (URL ou autre) indiquant au partenaire où l'utilisateur doit être

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

redirigé après la validation de l'assertion ;

- `index` permet de forcer l'utilisation d'un binding particulier (voir le fichier de méta données pour les valeurs possibles)

- `/saml/acs` : adresse de traitement des assertions reçues en tant que fournisseur de services
- `/discovery?idp_ident=X&return_url=Y` : adresse permettant d'envoyer un demande d'authentification à un fournisseur d'identité
  - `idp_ident` est l'identifiant de ce partenaire (ou le nom de son fichier metadata sans l'extension .xml)
  - `return_url` est le service de destination sur lequel rediriger après authentification

6.9.2. Astuces d'exploitation

Journalisation du service

Le fichier de journalisation du service EoleSSO est `/var/log/rsyslog/local/eolesso/eolesso.info.log`.

Il est possible d'activer un mode `debug` affichant beaucoup plus d'informations dans le fichier de log.

Pour l'activer, ouvrez le fichier `/usr/share/sso/config.py` et remplacer la ligne

```
DEBUG_LOG = False
```

par

```
DEBUG_LOG = True
```

Cette option de debug est à utiliser temporairement pour éviter de rendre les logs illisibles (et limiter l'espace disque utilisé). En cas de mise à jour du paquet eole-sso, elle sera réinitialisée à sa valeur par défaut.

Quand ce mode est activé, il est également possible d'afficher certaines requêtes SAML dans le navigateur en ajoutant un paramètre `show=1` aux urls gérant leur envoi.

Cela est possible dans les cas suivants :

- envoi d'une assertion d'authentification (ex : `/saml?sp_ident=X&show=1`)
- envoi d'une requête d'authentification (ex : `/discovery?idp_ident=X&show=1`)

Rechargement de la configuration du service

Il est possible de recharger le service EoleSSO (au lieu de le redémarrer) afin de prendre en compte de nouvelles données de configuration. Pour cela utilisez la commande suivante :

```
CreoleService eole-sso reload
```

L'avantage de cette méthode par rapport à `CreoleService eole-sso restart` est que les sessions des utilisateurs en cours sont conservées.

Les données suivantes sont prises en compte lors du rechargement :

- filtres d'attributs et description d'applications (situés dans `/usr/share/sso/app_filters`) ;
- jeu d'attributs et fichier de configuration d'associations (situés dans `/usr/share/sso/attribute_sets`) ;
- fichiers metadata des entités partenaires (situés dans `/usr/share/sso/metadata`) ;
- définitions d'attributs calculés (situés dans `/usr/share/sso/user_infos`).

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

6.9.3. Exemple de Fédération avec RSA/FIM

Préparation de la configuration FIM

Les données suivantes sont nécessaires pour configurer l'association dans FIM :

- Les méta-données du serveur EoleSSO : `wget https://<ip_serveur_sso>:8443/saml/metadata --no-check-certificate --outputfile=eolesso.xml`
- le certificat du serveur EoleSSO : `/etc/ssl/certs/eole.crt` (fichier par défaut, peut varier selon la configuration)

Si le certificat est au format PEM (c'est le cas du certificat par défaut sur un module EOLE), il faut le convertir au format DER : `openssl x509 -inform PEM -outform DER -in eole.crt -out eole_der.crt`

Une fois converti, utiliser la commande keytool pour intégrer le certificat à un truststore du serveur RSA/FIM (ou créer un truststore spécifique à cette occasion). Sur notre serveur de test, ils sont situés dans `/appli/federation/rsa-fim-config/keystores`

Par exemple : `<chemin vers jdk>/bin/keytool -import -alias fs-ac-mon_acad-et-mon_etab-1.0 -keystore mon_truststore-trust.jks -file eole_der.crt`

Configuration du fournisseur d'identité :

- aller dans Quick Setup -> add New Partner ;
- importer le fichier de méta-données `eolesso.xml` et donner un nom d'entité ;
- sauver dans la page suivante (association), choisir le fournisseur de service (FIM) ;
- cliquer sur l'onglet `general settings` et choisir les réglages suivants :
  - Encrypting/Signature truststores : sélectionner le truststore créé ci dessus ;
  - cocher la case `Transient Plug-in` ;
  - le greffon 'dictao cleartrust transient plugin' doit être sélectionné ;
  - attribute plugin : ajouter DictaoDumbAttributePluginRP ;
  - laisser les autres valeurs par défaut et sauver.

Configuration du serveur EoleSSO

La première étape est de récupérer le fichier de méta-données du fournisseur de service dans FIMConfig :

- Entities -> local entities -> manage existing ;
- cliquer sur le fournisseur, puis sur 'Export' dans le menu déroulant ;
- valider avec les valeurs par défaut, et copier le contenu affiché dans un fichier sur votre machine locale.

Placer ce fichier dans le répertoire `/usr/share/sso/metadata` (dans cet exemple, `fim_sp.xml`) du serveur EoleSSO et redémarrer le service.

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



Le fichier de méta-données doit être un fichier XML valide. Si l'entête suivant n'est pas présent, ajoutez le au début du fichier :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

Test du lien de fédération

Pour accéder à une ressource au moyen de la fédération, il faut utiliser une adresse de ce type :

https://<adresse_FI>:8443/saml?sp_ident=<id_FS>&RelayState=<adresse_service>

6.9.4. Fédération entre 2 serveurs EoleSSO

Synopsis

On considère la situation suivante :

Un serveur Scribe en établissement (adresse : `Scribe FI`) propose l'accès à des ressources protégé par un serveur Seshat (adresse : `Seshat FS`) à travers son portail local.

Une réplication d'annuaire est en place entre les 2 serveurs (le serveur Seshat répliquant les annuaires de plusieurs établissements).

On souhaite que l'utilisateur se connecte sur le portail établissement du serveur Scribe, et accès à un application web du serveur Seshat (en saisissant une seule fois ses identifiants lors de la connexion au portail).

Pour permettre de retrouver les utilisateurs sur le fournisseur de service, on décide d'utiliser comme clé de jointure le champ FederationKey de l'annuaire de Scribe. Ce champ étant unique au niveau national, il n'y aura pas de problème



Se reporter à la partie traitant de la gestion des identifiants ENT dans la documentation Scribe pour plus d'informations sur la mise en place de l'attribut FederationKey

Configuration du fournisseur d'identité (module Scribe)

La première étape est de définir un filtre pour définir les attributs à envoyer au fournisseur de service dans l'assertion SAML.

Par défaut, le serveur EoleSSO utilise le filtre défini dans le fichier `/usr/share/sso/app_filters/saml.ini` si aucun filtre n'est spécifié pour l'adresse du fournisseur de service (pour information, cette adresse est https://Seshat_FS:8443/saml/acs).

Il n'y a ici rien à modifier car ce filtre envoie l'attribut FederationKey.

Configuration du fournisseur de service (Seshat)

Sur le fournisseur de service, il faut indiquer le jeu d'attributs à utiliser pour établir la correspondance entre les attributs donnés dans l'assertion SAML et les attributs présents dans l'annuaire de Seshat.

Ici aussi, la configuration par défaut convient. Si aucun jeu d'attribut n'est défini pour l'identifiant du

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

fournisseur d'identité, le jeu par défaut est `FederationKey=FederationKey`, ce qui correspond à notre cas d'utilisation.

Ce filtre est défini dans le fichier `/usr/share/sso/attribute_sets/default.ini`.

Mise en oeuvre du lien de fédération

Une fois les 2 serveurs configurés, on échange les fichiers de méta données pour établir le lien. Une méthode simple est de le faire par les commandes suivantes :

- sur le module Scribe : `wget --no-check-certificate -O /usr/share/sso/metadata/seshat.xml https://seshat_FS:8443/saml/metadata`
- sur le module Seshat : `wget --no-check-certificate -O /usr/share/sso/metadata/scribe.xml https://scribe_FI:8443/saml/metadata`
- redémarrer le service `eole-sso` sur les 2 serveurs : `CreoleService eole-sso restart`

Pour tester le fonctionnement de la fédération, taper l'URL suivante dans un navigateur :

https://scribe_FI:8443/saml?sp_ident=seshat

Après validation du formulaire pour confirmer l'accès, le navigateur doit être redirigé sur l'URL https://seshat_FS:8443/loggedin. Des informations sur la session établie par le serveur Seshat sont affichées sur cette page

une fois le lien de fédération fonctionnel, ajouter un lien dans le portail du serveur Scribe pour accéder à l'application sur Seshat:

https://scribe_FI:8443/saml?sp_ident=seshat&RelayState=https://seshat_FS/mon_application

6.9.5. Mise en place de l'authentification OTP

Le service EoleSSO est capable de valider une authentification par clé OTP auprès d'un serveur RSA Authentication Manager (protocole SecurID).

Pour permettre ce fonctionnement, il est nécessaire d'installer sur le serveur un module PAM fourni par EMC.

Ce module est disponible à l'adresse suivante :

http://france.emc.com/security/rsa-securid/rsa-authentication-agents/pam-7-1.htm

La dernière version testée est la version 7.1.0.1. elle nécessite au minimum un serveur RSA Authentication Manager version 6.1 ou 7.1

Ce client n'est pas certifié pour fonctionner sur le système GNU/Linux Ubuntu, il peut être nécessaire de modifier le script d'installation présent dans l'archive pour qu'il s'exécute correctement sur un serveur EOLE (voir ci-dessous).



Adaptation du fichier `install_pam.sh` pour une installation sur un serveur EOLE :

- Remplacer les occurrences de `chmod 755` par `chmod 644` pour appliquer les permissions préconisées par la distribution.
- Rechercher la section concernant le paramétrage pour Linux (ligne 362 dans la version testée) :

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

```
'Linux' ) LNX_VERS=`uname -i`
   if [ `getconf LONG_BIT` = "32" ] ; then
        ARCH=32bit
        MODULE_DIR_PRIMARY="/lib/security"
        MODULE_DIR_SECONDARY=""
   else
        ARCH=64bit
        MODULE_DIR_PRIMARY="/lib/security"
        MODULE_DIR_SECONDARY="/lib64/security/"
   fi
```

Dans le bloc `else` (serveur 64 bits), remplacer `MODULE_DIR_SECONDARY="/lib64/security/"` par `MODULE_DIR_SECONDARY="/lib/x86_64-linux-gnu/security/"`.

La même modification doit être effectuée sur le fichier `uninstall_pam.sh` si vous souhaitez désinstaller l'agent.

Cette modification concerne la dernière version testée du client (v7.1.0.1.16.05_06_13_02_04_01), si besoin voir la documentation EoleSSO 2.3 si vous utilisez des versions plus anciennes.

Un fichier de configuration est livré avec EoleSSO pour utiliser le module fourni (`/etc/pam.d/rsa_securid`)

Le module nécessite également les étapes suivantes :

- enregistrement du serveur hébergeant EoleSSO en tant qu'agent dans la configuration du serveur Authentication Manager ;
- copie du fichier `sdconf.rec` présent sur le serveur RSA dans le répertoire `/var/ace` (serveur EoleSSO) ;
- activer la gestion de l'authentification OTP dans EoleSSO (dans l'interface de configuration du module, onglet `Eole sso` puis redémarrer le service). Se reporter à la section Configuration pour le détail des options de configuration disponibles.

Deux utilitaires sont livrés avec le module PAM pour tester le fonctionnement :

- `/opt/pam/bin/32bit/acestatus` : affiche les informations sur le serveur présentes dans `sdconf.rec`
- `/opt/pam/bin/32bit/acetest` : permet de valider l'authentification d'un utilisateur

Sur un serveur 64 bits, les utilitaires livrés avec le module PAM se trouvent dans le répertoire `/opt/pam/bin/64bit`.

Versions 32 ou 64 bits

Les scripts d'installation fournis n'installent pas toujours correctement le module PAM. En cas de dysfonctionnement, vérifier que la version installée de la librairie correspond bien à l'architecture de la machine (voir complément ci dessus sur le script d'installation).

Vous pouvez comparer le fichier `pam_securid.so` installé avec les version 32 ou 64 bits qui peuvent être trouvées dans l'archive `sd_pam_agent.tar` du répertoire `/lnx` du répertoire d'installation de l'agent.

La librairie doit être installée dans le répertoire `/lib64/security/` dans le cas d'une version

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

> d'EOLE inférieure à 2.5.0 ou dans le répertoire `/lib/x86_64-linux-gnu/security/` dans le cas contraire.

6.9.6. Application de redirection : Eole-dispatcher

Dans le cadre de l'utilisation du module Seshat en tant que point d'entrée d'un ENT centralisé, l'application Eole-dispatcher permet de rediriger les utilisateurs vers leur établissement d'origine. Elle se base sur les informations remontées lors de la mise en place de la réplication des serveurs Scribe.

Elle est également prévue pour gérer le cas de l'affectation multiple pour les enseignants et les responsables :

- un enseignant qui aurait des services sur plusieurs établissements se verrait proposer le choix de l'établissement sur lequel il souhaite se connecter ;
- un parent d'élève qui aurait plusieurs enfants dans des établissements différents se verrait également proposer le choix de l'établissement. Il est à noter que la problématique de la l'affectation multiple pour un élève ne se pose pas, puisque ce dernier ne peut pas être scolarisé dans deux établissements.

Eole-dispatcher est capable (au travers de ses filtres d'attributs) de gérer les sources d'authentification suivantes :

- LDAP Académique pour les agents de l'Éducation nationale ;
- LDAP Téléservices pour les parents et élèves ;
- LDAP local (réplicat des serveurs Scribe) pour l'authentification des élèves et parents (si les téléservices ne sont pas déployés).

> Le terme affectation est à prendre au sens large, il désigne l'appartenance d'une personne à un établissement.

Pré-requis

Cette application nécessite :

- la mise en place de la réplication LDAP des serveurs Scribe sur le serveur Seshat ;
- l'alimentation des annuaires des serveurs Scribe avec des extractions AAF **EXCLUSIVEMENT** ;
- la bonne saisie des numéros et libellés établissement sur les serveurs Scribe et Zéphir ;
- la configuration d'une fédération entre chaque serveur Scribe et le serveur Seshat (voir documentation EoleSSO au chapitre : Fédération entre 2 serveurs EoleSSO).

Installation

Le dispatcher est à installer sur le module Seshat, afin d'utiliser son portail EoleSSO comme portail unique d'authentification vers les ENT (Envole).

L'application n'est pas installée par défaut. Via l'interface de configuration du module, configurer le serveur pour recevoir les applications web :

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

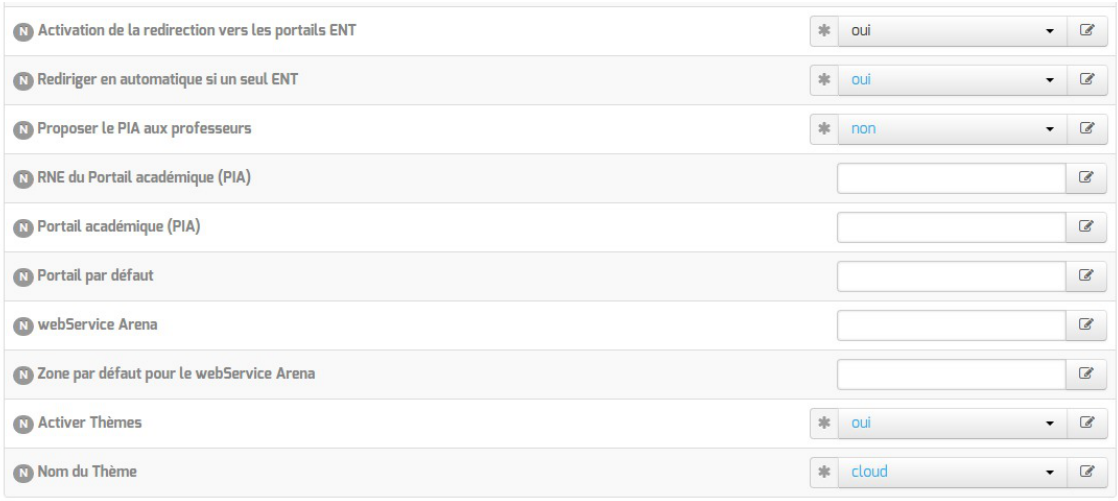
- en mode normal dans l'onglet `Services`, passer `Activer le serveur web Apache` à `oui` ;
- dans l'onglet `Applications web`, saisissez le nom de domaine des applications web dans `Nom de domaine des applications web (sans http://)` ;
- enregistrer la configuration et quitter l'interface de configuration du module.

Puis saisir les commandes suivantes sur le module Seshat pour installer le paquet `eole-dispatcher` :

```
# Query-Auto
# apt-eole install eole-dispatcher
```

Configuration

Une fois les paquets installés, il faut de nouveau se rendre dans l'onglet `Application web` de l'interface de configuration du module et passer `Activation de la redirection vers les portails ENT` à `oui`. Des paramètres supplémentaires s'affichent.



- `Rediriger en automatique si un seul ENT` ;
- `Proposer le PIA aux professeurs` : permet de proposer le portail académique aux enseignants ;
- `RNE du Portail académique (PIA)` : permet de saisir l'UAI du portail académique ;
- `Portail académique (PIA)` : portail sur lequel seront redirigés les personnels académiques ;
- `Portail par défaut` : adresse du site Internet dédié à l'ENT si aucun portail d'établissement n'est disponible pour l'utilisateur ;
- `webService Arena` : URL complète du webService ARENA pour la récupération des ressources ;
- `Zone par défaut pour le webService Arena` : zone par défaut du portail ARENA.

Il est possible de changer ou de désactiver le thème.

Une fois l'application paramétrée, il est nécessaire de reconfigurer le serveur à l'aide de la commande `reconfigure`.

Une fois le serveur reconfiguré, l'application est accessible à l'adresse : `http://<adresse_serveur>/edispatcher/`

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

Il est possible de rendre l'application directement accessible depuis l'adresse `http://<adresse serveur>/`, en renseignant `/edispatcher` en tant qu'`Application web par défaut (redirection)` dans la famille Applications web

Fonctionnement

L'installation du dispatcher va mettre en place sur le serveur SSO les filtres d'attributs nécessaires afin de rediriger correctement la personne.

Extrait du fichier /usr/share/sso/app_filters/dispatcher.ini :

```
[user]
rne=ecs_rne
user=uid
uid=uid
source=SourceAuth
FederationKey=DispatcherKey
displayName=displayName
profils=DispatcherProfils
auth=auth
```

L'attribut calculé `ecs_rne`, va permettre de récupérer les codes RNE en fonction des établissements d'affectation de l'utilisateur.

Lors de la connexion d'une personne, Eole-dispatcher va prendre tous les RNE reçus de EoleSSO et présenter tous les liens de fédération pour l'accès aux portails Envole le concernant.

Exemple d'URL de fédération

`https://<domaineSeshatSSO>/saml?sp_ident=<id_fs>&RelayState=https:/`
Cette URL effectue une fédération vers le fournisseur de service `<id_fs>` et redirige vers l'`<URL du portail Établissement>` du client en fournissant un identifiant de session.

Eole-dispatcher et EoleSSO

RNE : `id_fs`

`id_fs` est :

- soit l'identifiant du fournisseur de service (entityID tel que défini dans son fichier de méta-données) ;
- soit le nom de son fichier de méta-données placé dans /usr/share/sso/metadata/ (sans l'extension `.xml`).

Par simplicité il est possible de nommer le fichier metadata de nos entités partenaires (Serveur Scribe des établissements) par <RNE>.xml ; `id_fs` est alors le code RNE de l'établissement.

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

Libellé et adresse du portail des établissements : URL_du_portail_Établissement

EoleSSO va générer automatiquement, à chaque redémarrage du service `eole-sso`, un fichier dans `/var/www/html/edispatcher/utils/etabs.ini` qui va contenir les entrées nécessaires pour chaque établissement :

```
[9740091F]
libelle = COLLEGE LECONTE DE LISLE
portail = https://portail.college-lecontedelisle.re
...
```

Ces entrées sont récupérées depuis Zéphir, il est donc nécessaire que les serveurs Scribe soient enregistrés sur le serveur Zéphir. Dans le cas contraire, ou si des informations sont incorrectes ou manquantes, il faudra remplir ce fichier à la main (voir le chapitre : Gestion des sources d'authentification multiples).

Vous pouvez vous baser sur le fichier d'exemple : `/var/www/html/edispatcher/utils/etabs.ini.sample`.

Message d'erreur : `aucun portail trouvé`



Il manque une section pour le code RNE dans le fichier `/var/www/html/edispatcher/utils/etabs.ini`.

Description de liens vers des applications web ou vers des portails.

Fichier `/var/www/html/edispatcher/applications.ini` :

- Format des sections :

```
[<identifiant du lien>]
url="<adresse du lien>"
piwik=<identifiant piwik>
```

- Paramétrage des URLs : il est possible d'insérer des étiquettes dynamiques dans les URLs

```
[SSO] : adresse du serveur SSO de Seshat
[PORTAILHOST] : portail dépendant de la zone d'accès du client (configuré dans portails.ini)
[TICKET] : identifiant de session
```

Configuration de l'accès à un portail en fonction de la plage IP du client

Eole-dispatcher est également utilisé dans certaines académies comme portail d'authentification unique pour l'accès aux portails ARENA[p.753].

Il peut exister plusieurs portails en fonction de l'endroit où se trouve l'utilisateur. Par exemple, dans l'académie de la Réunion il existe au moins trois portails d'accès aux application ARENA :

- `portail.ac-reunion.fr` (accessible en externe) ;
- `scoens.ac-reunion.fr` (depuis le réseau pédagogique des établissements) ;
- `scoweb.ac-reunion.fr` (depuis le réseau administratif).

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

Chaque portail, en fonction de sa zone de confinement, ne présentera pas les mêmes ressources et l'utilisation d'une clé OTP[p.773] sera proposée ou non.

Il faut donc permettre à l'utilisateur d'obtenir le bon portail en fonction de la zone où il se trouve.



La fonction `GetPortailHost` du fichier `/var/www/html/edispatcher/inc.php` du dispatcher permet, en fonction de l'adresse IP du client, de rediriger l'utilisateur vers le bon portail. La récupération de l'adresse IP du client se base sur le champ `HTTP_X_FORWARDED_FOR` des headers HTTP.

Les différentes associations réseau / portail sont définies dans le fichier `/var/www/html/edispatcher/utils/portails.ini`.

Créer le fichier `/var/www/html/edispatcher/utils/portails.ini` et ajouter des sections décrivant une plage IP et l'adresse du portail correspondant :

```
[<adresse IP>]
mask=<masque IP>
portail="<adresse du portail pour cette plage IP>"
```

Un exemple de fichier est présent dans : `/var/www/html/edispatcher/utils/portails.ini.sample`.



```
[172.16.0.0]
mask=13
portail="scoens.ac-reunion.fr"
arena="rev-proxy-peda"
[172.31.190.64]
mask=26
portail="portail.ac-reunion.fr"
arena="rev-proxy-id"
[172.31.16.0]
mask=16
portail="portail.ac-reunion.fr"
arena="rev-proxy-id"
[10.205.0.0]
mask=16
portail="scoweb.ac-reunion.fr"
arena="rev-proxy-agr"
```



Dans cet exemple, tout utilisateur se présentant avec une adresse IP du réseau 10.205.0.0/16, se verra renvoyé vers l'URL du portail académique https://scoweb.ac-reunion.fr.

La variable `arena`, permet de spécifier la zone ClearTrust associée au portail. Elle est

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

utilisée si vous souhaitez intégrer les ressources ARENA dans le bureau Envole.
Plus d'informations : https://envole.ac-dijon.fr/wordpress/2014/02/19/integration-de-arena-dans-le-bureau-envole.

Voir aussi...

Gestion des sources d'authentification multiples

6.9.7. Configuration du fournisseur d'identité France Connect

Pour mettre en place la relation de confiance entre EoleSSO et France Connect, il faut effectuer une demande d'enregistrement auprès de France Connect : https://franceconnect.gouv.fr/inscription

Le fournisseur d'identité France Connect renvoi un identifiant client (Client ID) et une clé privée secrète (Client secret) utilisé pour valider les échanges. Il met à disposition un certain nombre d'URLs nécessaires à la configuration du client.

Pour l'inscription il est demandé les informations suivantes:

- le nom du service ;
- une adresse électronique de contact ;
- un logo représentant le fournisseur de service (logo EOLE, logo de l'académie...) qui apparaîtra sur la page d'authentification de France Connect ;
- une adresse dite de callback : adresse sur laquelle est renvoyé l'utilisateur après authentification.
  Dans le cas d'EoleSSO cette adresse est :
  `https://<adresse_serveur_eolesso>:8443/oidcallback`

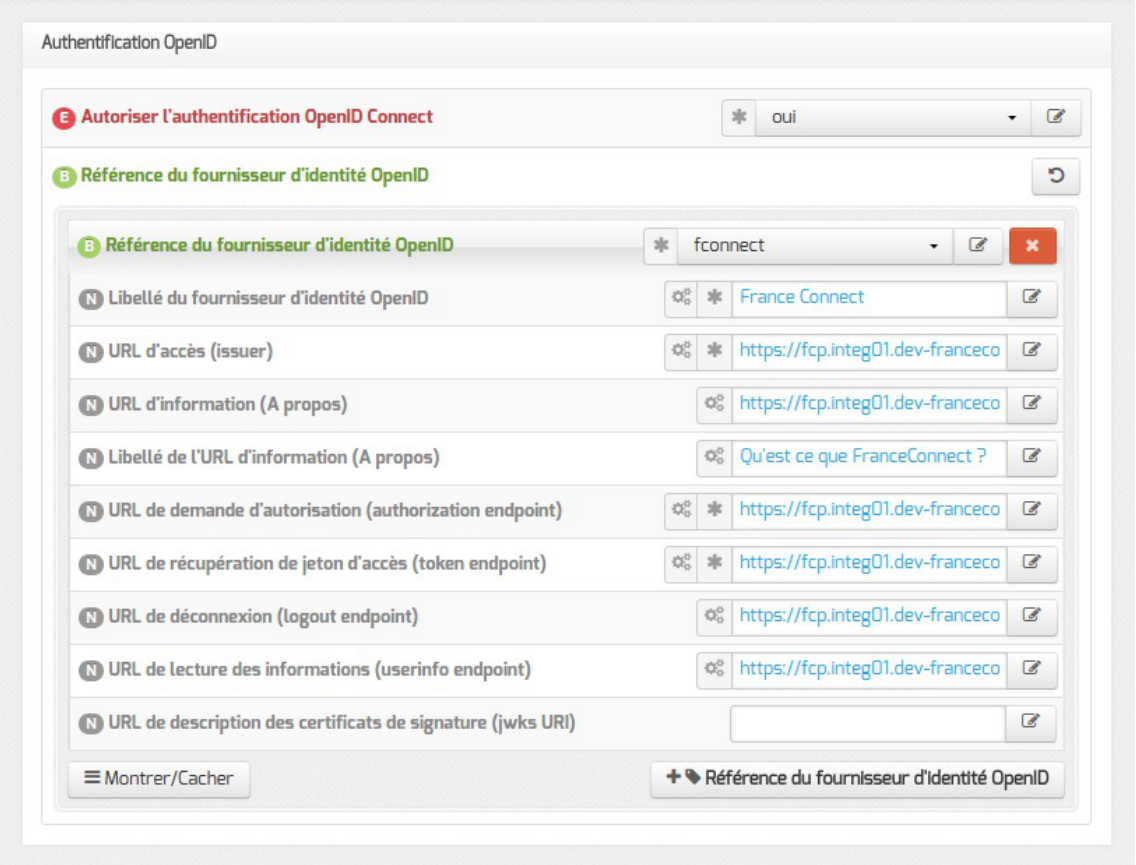
Les logos et bouton de connexion France Connect sont déjà fournis avec EoleSSO.



Pour plus d'informations sur le fonctionnement et la configuration, se reporter à : https://franceconnect.gouv.fr/fournisseur-service
Les conditions d'utilisation de France Connect et le processus de raccordement sont décrites dans le document PDF suivant :
https://franceconnect.gouv.fr/files/CGU FS - Annexe Processus d'implementation de FC par FS V2.1.pdf [https://franceconnect.gouv.fr/files/CGU%20FS%20-%20Annexe%20Processus%20d'implementation%20de%20FC%20par%20FS%20V2.1.pdf]
À noter que parmi les conditions, une **déclaration CNIL** simplifiée est disponible et une **recette de la solution technique** mise en œuvre doit être effectuée par le SGMAP[p.778].

Une configuration prédéfinie est fournie pour France Connect.

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



Pour l'activer, choisissez `fconnect` dans la liste déroulante de la variable `Référence du fournisseur d'identité OpenID`, ne pas oublier de valider le choix pour faire apparaître les différentes variables.



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

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

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

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

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

Voir aussi...

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

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

6.9.8. Configuration du fournisseur d'identité Google (Google APIs).

Déclaration d'EoleSSO comme fournisseur de service

Pour récupérer votre Client ID / Client Secret, vous devez créer un compte développeur depuis cette adresse : https://developers.google.com/

Rendez-vous dans la console développeur de Google afin de déclarer votre service EoleSSO comme application : https://console.developers.google.com

- Créez un nouveau projet (barre supérieure de la console -> `select a project` -> `create a project`) ;
- Une fois le projet créé, cliquez sur la barre de menu gauche (3 barres horizontales), puis sur `API Manager`. Cliquez ensuite sur `Credentials` (à gauche) ;
- Cliquer sur `Oauth Consent Screen` et renseigner au minimum le champ `Product name shown to users` (par exemple 'établissement xxx') ;
- Sauvegarder et dans Credentias, cliquer sur `Create credentials`, *Oauth Client ID" ;
- Choisir `Web application` et renseigner les champs suivants :
  - Name : au choix
  - Authorized JavaScript origins : https://[adresse_serveur_sso]:8443
  - Authorized redirect URIs : https://[adresse_serveur_sso]:8443/oidcallback
- Cliquer sur Create et recopier l'identifiant et la clé secrète fournis ;

Configuration du fournisseur d'identité (Google) dans l'interface de configuration du module

Une fois les identifiants récupérés, vous pouvez configurer les paramètres d'EoleSSO (gen_config, onglet Eole SSO en mode expert)

- Passer à `oui` la variable `Autoriser l'authentification OpenID Connect` ;
- ajouter un forunisseur en cliquant sur `+Référence du fournisseur d'identité OpenID` ;
- `Référence du fournisseur d'identité OpenID` : google (des logos sont présents et utilisés automatiquement en choisissant ce libellé) ;
- `Libellé du fournisseur d'identité OpenID` : Google (ou autre description de votre choix) ;
- `issuer` : https://accounts.google.com ;
- `authorization endpoint` : https://accounts.google.com/o/oauth2/v2/auth ;
- `token endpoint` : https://www.googleapis.com/oauth2/v4/token ;
- `userinfo endpoint` : https://www.googleapis.com/oauth2/v3/userinfo ;
- `jwks uri` : https://www.googleapis.com/oauth2/v3/certs .

En cas de problème, les paramètres en cours de validité sont décrits ici : https://accounts.google.com/.well-known/openid-configuration

Pour plus d'informations sur le support d'OpenID de Google : https://developers.google.com/identity/protocols/OpenIDConnect

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

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

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

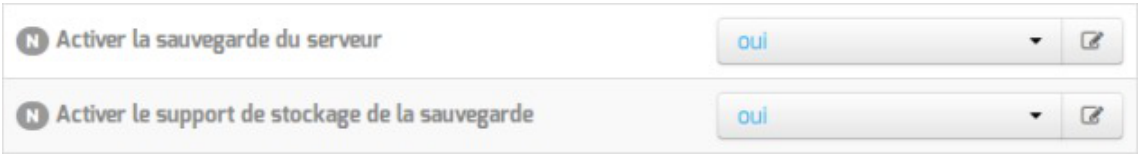
```
<nom_fournisseur> = "<client id> :<client secret>"
```

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

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

7. Activation et configuration de Bareos

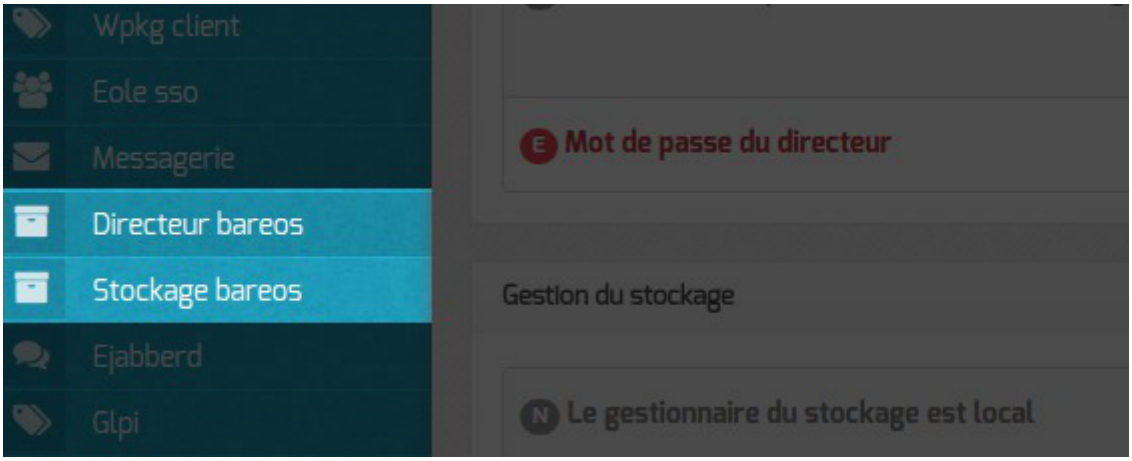
La sauvegarde du serveur et le support de stockage de la sauvegarde sont activés par défaut sur certains modules, il peuvent être activés/désactivés dans l'onglet `Services` de l'interface de configuration du module.



Activation de la sauvegarde Bareos dans l'onglet Services de l'interface de configuration

- L'activation du support de stockage de la sauvegarde permet d'accueillir des sauvegardes locales ou distantes.
- L'activation de la sauvegarde permet d'activer la sauvegarde du serveur, celle-ci peut être locale si le support de stockage est activé ou déportée à condition d'avoir un serveur sur lequel est activé le support de stockage.

Cette fonctionnalité permet de mettre en place des sauvegardes croisées.



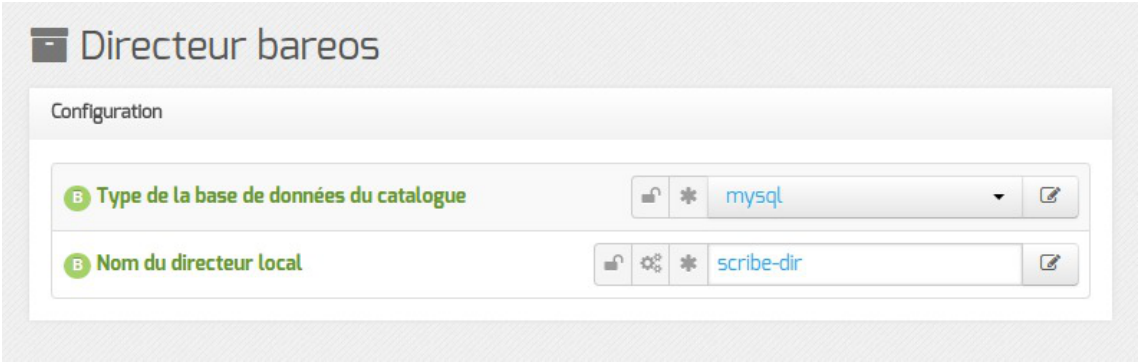
Si le support de stockage de la sauvegarde est activé (`Activer le support de stockage de la sauvegarde` à `oui`) un onglet `Stockage bareos` apparaît dans l'interface de configuration du module.

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

L'onglet permet de configurer le nom du serveur de stockage et d'autoriser des directeurs à se connecter au stockage.

Suite à l'activation de la sauvegarde du serveur (`Activer la sauvegarde du serveur` à `oui`) l'onglet `Directeur bareos` apparaît dans l'interface de configuration du module. Il permet de configurer le nom du directeur et les périodes de rétention et de définir si le serveur de stockage est distant ou local.

Onglet Directeur bareos



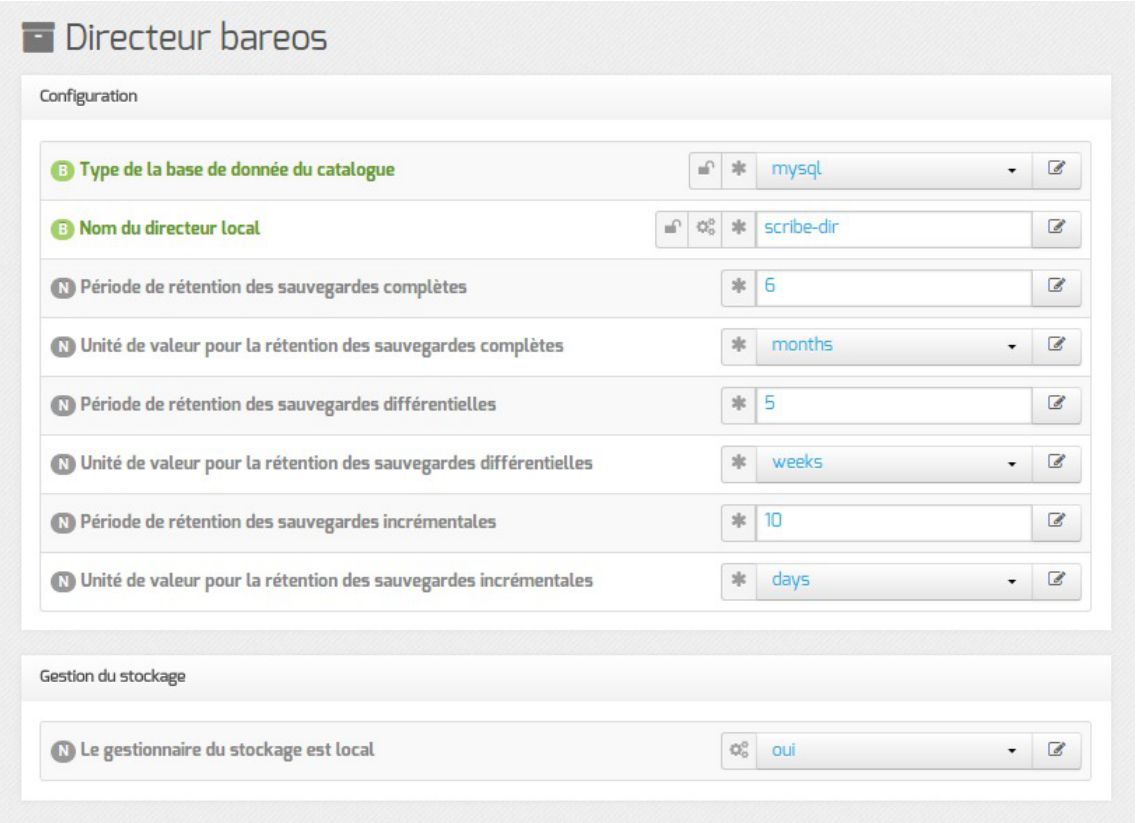
Le type de base de données permet de choisir si l'enregistrement du catalogue se fait dans MySQL ou dans SQLite. Il ne sera plus possible de modifier ce paramètre après l'enregistrement de la configuration.

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.759] 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.

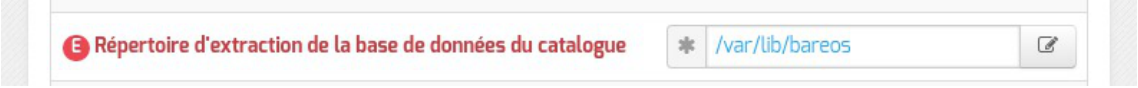
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

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.

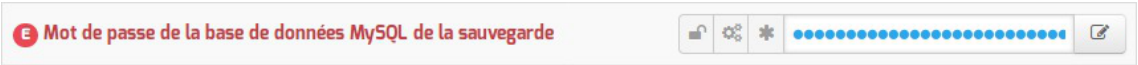
En mode expert, il est possible de modifier le répertoire utilisé par défaut pour l'extraction de la base de données du catalogue. Ce changement permet éventuellement de ne pas surcharger l'espace occupé

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

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



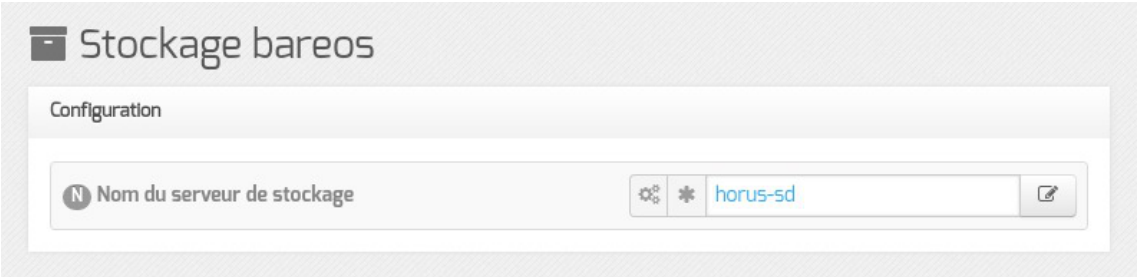
Type de compression et délai alloué

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 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.

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.

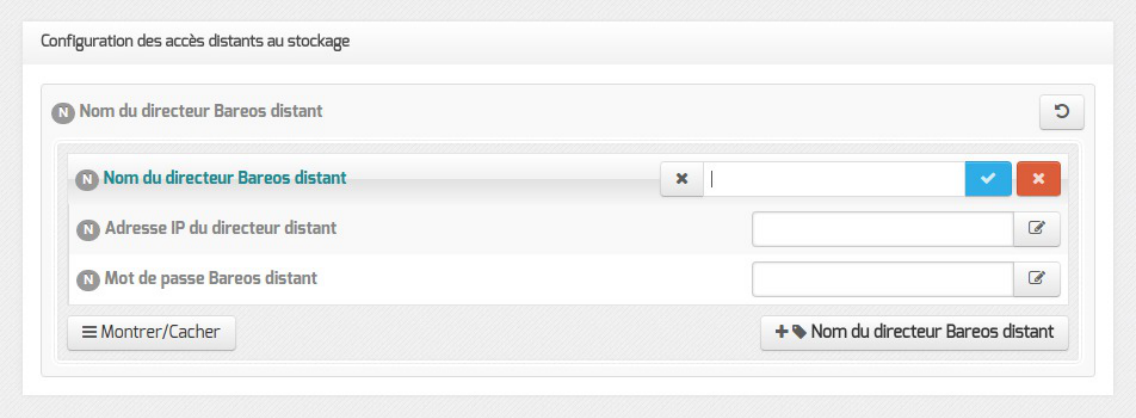


Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur `Nom du directeur Bareos distant`, le détail de l'autorisation s'affiche.

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

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

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



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.

Pour que les modifications soient prises en compte, une reconfiguration du module est nécessaire avec la commande : `reconfigure`.

Voir aussi...

- Les mots de passe
- bareos-webui : outil d'administration pour Bareos [p.486]

8. Gestion des bases de données avec EoleDB

EoleDB est disponible depuis la version 2.5.2 d'EOLE. C'est une re-implémentation de l'ancien gestionnaire des bases de données EOLE (eole-sql) dont les objectifs principaux sont :

- n'utiliser qu'un seul fichier de configuration ;
- supporter nativement plusieurs types de bases de données (MySQL, PostgreSQL, SQLite, ...) ;
- supporter nativement l'externalisation des bases de données sur d'autres serveurs ;
- ne plus avoir à fournir des scripts python dans les paquets d'application web du projet EOLE pour pouvoir générer ou mettre à jour des bases de données (cf eole-sql : `/usr/share/eole/applications/gen/` , `/usr/share/eole/applications/passwords/` , `/usr/share/eole/applications/updates/`).

EoleDB rend possible l'externalisation des bases de données d'un module EOLE.

Pour le moment, la version publiée d'EoleDB gère uniquement les bases de données MySQL et PostgreSQL.

Installation d'EoleDB

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

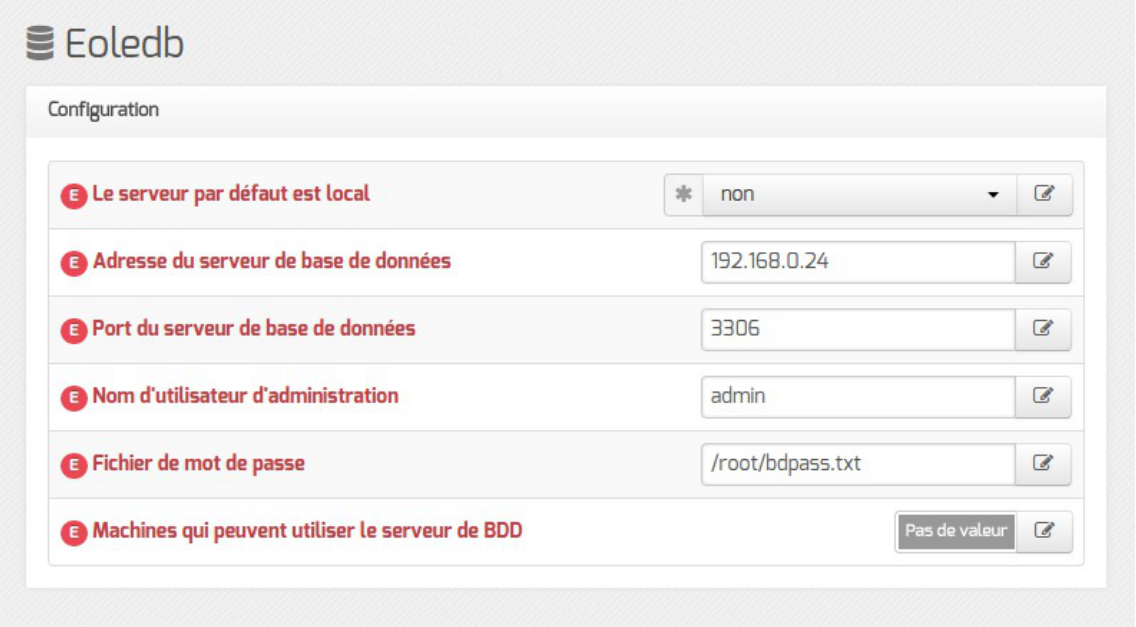
L'installation d'EoleDB se fait manuellement sur le serveur qui héberge l'application web avec la commande `apt-eole` :

```
# apt-eole install eole-db
```

Le paquet `eole-db` est pré-installé sur le module Scribe depuis la version 2.6.0.

Configuration d'EoleDB

Par défaut le serveur est paramétré comme étant local. Dans le cas où le serveur est distant quelques variables sont à renseigner.



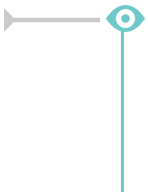
- `Adresse du serveur de base de données` : adresse IP, nom de machine ou nom de domaine du serveur de base de données distant. Cette valeur est utilisée pour toutes les applications web qui ne définiront pas elles-mêmes un serveur de base de données.
- `Port du serveur de base de données` : port du serveur de base de données utilisé, par exemple `3306` pour le serveur MySQL fourni par EOLE.
- `Nom d'utilisateur d'administration` : identifiant du gestionnaire de la base de données distante.
- `Fichier de mot de passe` : chemin d'accès vers le fichier qui contient le mot de passe du gestionnaire, par exemple `/root/bdpass.txt`. Ce fichier doit être accessible par EoleDB, idéalement le fichier doit avoir les droits 600.
- `Machines qui peuvent utiliser le serveur de BDD` : permet d'autoriser des machines à accéder à l'administration des bases distantes #fixme [https://dev-eole.ac-dijon.fr/issues/15456] , si rien n'est renseigné l'adresse IP du serveur utilisant EoleDB est ajoutée automatiquement dans le fichier de configuration.

EoleDB dispose d'un fichier de configuration principal, `/etc/eole/eole-db.conf`, géré par Creole.

Ce fichier est au format YAML[p.785], il définit le comportement par défaut d'EoleDB si aucune

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

configuration spécifique n'est définie par l'application web.



```
dbhost: 192.168.0.24
dbport: 3306
dbroot: root
client_hosts: ['192.168.0.26']
dbrootpwd: /root/bdpass.txt
```

Le fichier `/root/bdpass.txt` est un fichier à créer, il contient le mot de passe en clair du gestionnaire. Ce fichier doit être accessible par EoleDB, idéalement le fichier doit avoir les droits 600.

Configuration d'une application web

Les applications web disponibles sur les modules EOLE fournissent un fichier de configuration au format YAML[p.785] qui surcharge le fichier de configuration principal d'EoleDB.

Ces fichiers de configuration spécifiques aux applications redéfinissent le comportement par défaut d'EoleDB, ils sont stockés dans `/etc/eole/eole-db.d/`.

Pour des raisons pratiques, EoleDB réalise le changement de mots de passe dans les fichiers de configuration des applications.

Les mots de passe sont changés à chaque lancement des commandes `eole_db_gen` et `reconfigure`.

Pour utiliser EoleDB il faut mettre en place un fichier de configuration portant l'extension `.yml` dans le répertoire `/etc/eole/eole-db.d/` en utilisant :

- **dbhost** : définition de l'adresse du serveur de base de données utilisé par l'application (surcharge la valeur par défaut définie dans `/etc/eole/eole-db.conf`) ;
- **dbport** : définition du port d'écoute du serveur de base de données utilisé par l'application (surcharge la valeur par défaut définie dans `/etc/eole/eole-db.conf`) ;
- **dbroot** : définition du nom de l'utilisateur ayant des droits "Administrateur" sur le serveur de base de données utilisé par l'application (surcharge la valeur par défaut définie dans `/etc/eole/eole-db.conf`) ;
- **dbrootpwd** : définition du mot de passe par défaut de l'utilisateur défini par l'option dbroot (surcharge la valeur par défaut définie dans `/etc/eole/eole-db.conf`) ;
- **dbtype** : définition du type de base de données par défaut du serveur de base de données (mysql, pgsql, sqlite, ...) ;
- **dbname** : nom de la base de données de l'application ;
- **dbuser** : nom de l'utilisateur utilisé par l'application pour accéder à la base définie dans **dbname** ;
- **dbpass** : mot de passe utilisé par l'application pour l'utilisateur défini dans **dbuser** ;
- **createscript** : script SQL de création de la base de données définie dans **dbname** ;
- **sqlscripts** : scripts SQL a lancer après le script de création défini dans **createscript** ;
- **updatescripts** : scripts de mise à jour exécutés sur la base définie dans **dbname** (exécutés uniquement si la base existe déjà) ;

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

- **pwd_files** : définition des fichiers à mettre à jour après le changement du mot de passe de l'utilisateur défini dans **dbuser**.

```
dbtype: mysql
dbname: taskfreak
dbuser: taskfreak
dbpass: "53nrgk>as="
createscript: "/usr/share/eole/db/taskfreak/gen/taskfreak-create.sql"
pwd_files:
    - {file: '/var/www/html/taskfreak/include/config.php',
       pattern: '$dbpass="',
       owner: 'www-data:www-data',
       mod: '600' }
```

L'option **pwd_files** accepte une liste de dictionnaires au format python.

```
pwd_files:
    - {file: '/var/www/html/posh/includes/config.inc.php',
       container: 'web',
       pattern: 'define("__PASS","',
       end_pattern: ');',
       owner: 'root:www-data',
       mod: '660' }
    - {file: '/usr/share/envole/eoledb/posh',
       pattern: 'dbpassPOSH="',
       owner: 'root:root',
       mod: '600' }
```

Liste des options possibles d'un dictionnaire **pwd_files** :

- **file** : chemin complet du fichier à modifier (option obligatoire) ;
- **pattern** : modèle de ligne qui contient le mot de passe entre **"** (option obligatoire) ;
- **end_pattern** : permet de définir le ou les caractères à ajouter après le **pattern** ;
- **owner** : propriétaire au format "user:group", à définir après la modification du mot de passe ;
- **mod** : droits au format Unix (ex: 600) à définir après la modification du mot de passe ;
- **container** : conteneur ou se trouve le fichier à modifier.

L'option **pattern** permet de définir le modèle de ligne qui contient le mot de passe, il est important de définir la totalité de ce qui précède le mot de passe dans la ligne.

Ligne à changer dans le fichier de configuration `/chemin/monFichier.conf` :

`password: "JeSuiSunMauvaisPassowrd"`

La valeur de l'option pattern doit être `password: "`

Extrait du fichier YAML :

`pwd_files:`

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

```
- {file: "/chemin/monFichier.conf",
pattern: 'password: "'
```

EoleDB détermine automatiquement qu'il faut faire suivre, après remplacement, la valeur de **pattern** par le caractère **"**. Aussi si le caractère ouvrant est **'** il faut préférer le format suivant :

```
pattern: "password: '"
```

EoleDB détermine automatiquement qu'il faut faire suivre la valeur de pattern par le caractère **'**.

EoleDB détecte également si le caractère **;** est requis en fin de ligne et l'ajoute après le **pattern**.



L'option **end_pattern** permet de maîtriser des cas non gérés par EoleDB, exemple

```
define('DBPASS': 'JeSuisUnMauvaisPassword');
pattern : "define('DBPASS': '"
end_pattern: ");",
```

Pour une application 3 modes de gestion de la base de données sont possibles et sont fonctions de la configuration :

- mode **default** : l'application utilise la configuration globale d'EoleDB ;
- mode **local** : l'application force l'utilisation d'un serveur de base de données local ;
- mode **externe** : l'application force l'utilisation d'un serveur de base de données et définit complètement la configuration.

Le mode default

Dans le mode **default**, l'application ne prend donc aucune liberté et sa configuration repose exclusivement sur la configuration d'EoleDB saisie dans l'onglet `Eoledb` de l'interface de configuration du module.



```
1  dbtype: mysql
2  dbname: taskfreak
3  dbuser: taskfreak
4  dbpass: "53nrgk>as="
5  createscript: "/usr/share/eole/db/taskfreak/gen/taskfreak-create.sql"
6  pwd_files:
7      - {file: '/var/www/html/taskfreak/include/config.php',
8         pattern: '$dbpass="',
9         owner: 'www-data:www-data',
10        mod: '600' }
```



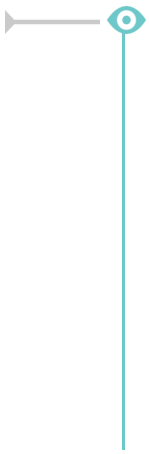
Si le comportement d'EoleDB est changé, celui-ci impactera l'application.

Le mode local

Dans le mode **local** la configuration de l'application à utiliser un serveur de base de données local, il faut donc ajouter dans la configuration **dbhost** et **client_hosts**.

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

La configuration d'EoleDB saisie dans l'onglet `Eoledb` de l'interface de configuration du module est ignorée.

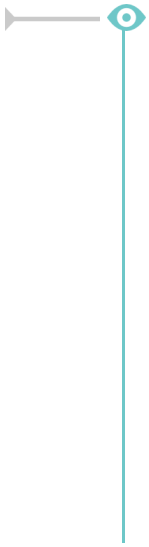


```
---
dbhost: 127.0.0.1
dbtype: mysql
dbname: taskfreak
dbuser: taskfreak
dbpass: "task;Freak"
client_hosts: ["127.0.0.1", "localhost"]
createscript: "/usr/share/eole/mysql/taskfreak/gen/taskfreak-create.sql"
pwd_files:
    - {file: '/var/www/html/taskfreak/include/config.php',
       pattern: '$dbpass="',
       owner: 'www-data:www-data',
       mod: '600' }
```

Le mode externe

Dans le mode **externe** l'application définie complètement le serveur externe de base de données à utiliser, il faut donc ajouter dans la configuration, en plus de **dbhost** et **client_hosts** ajouté dans le mode local, **dbroot** et **dbrootpwd**.

La configuration d'EoleDB saisie dans l'onglet `Eoledb` de l'interface de configuration du module est ignorée.



```
---
dbhost: 192.168.45.34
dbport: 3309
dbroot: adminDB
dbrootpwd: /root/.secrets-mydb
dbtype: mysql
dbname: taskfreak
dbuser: taskfreak
dbpass: "task;Freak"
client_hosts: ["127.0.0.1", "localhost", "192.168.0.14" ]
createscript: "/usr/share/eole/mysql/taskfreak/gen/taskfreak-create.sql"
pwd_files:
    - {file: '/var/www/html/taskfreak/include/config.php',
       pattern: '$dbpass="',
       owner: 'www-data:www-data',
       mod: '600' }
```

Mode conteneur

Pour fonctionner dans un conteneur EOLE, sur le module AmonEcole par exemple, l'application doit utiliser le mode **local** avec une configuration adaptée.

Configuration du serveur distant

Tester la connexion distante au serveur de base de données

```
# mysql -u admin -h <adresseDuServeur> -p<motDePasse>
```


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

Serveur Eolebase

Le serveur EOLE peut être l'un des modules ou un Eolebase.

Installer le paquet `eole-phpmyadmin`, le système de dépendance se charge d'installer les paquets nécessaires `eole-web` et `eole-mysql` :

```
root@eolebase:~# apt-eole install eole-phpmyadmin
```

Éditer le configuration du serveur à l'aide de la commande de l'interface de configuration du serveur :

```
root@eolebase:~# gen_config
```

Dans l'onglet t `Applications web`, la variable minimum à renseigner est `Nom de domaine des applications web (sans http://)`, il est possible d'activer l'application phpMyAdmin et de la choisir comme application web par défaut.

Reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
root@eolebase:~# reconfigure
```

Vérifier dans un navigateur web que le serveur répond.

Modifier le mot de passe par défaut du compte root mysql avec la commande `mysql_pwd.py` :

```
root@eolebase:~# mysql_pwd.py
## Réinitialisation des mots de passe Mysql ##
 Nouveau mot de passe root mysql : eole21
Voulez-vous que les autres mots de passe soient modifiés ? [oui/non] [non] : non
root@eolebase:~#
```

Se connecter à MySQL avec l'utilisateur root :

```
root@eolebase:~# mysql -u root -h localhost -peole21
```

Créer un utilisateur autre que `root` (le mot de passe du compte `root` est généré à chaque `reconfigure`) et lui donner les privilèges et l'autorisation de se connecter depuis le serveur hébergeant EoleDB :

```
mysql> grant all privileges on *.* to admin@<IPServeurEoleDB> identified by "eole21";
mysql> quit
```

Pour ouvrir le port il faut faire un dictionnaire personnalisé `00_mysql.xml` à placer dans `/usr/share/eole/creole/dicos/local/`

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <creole>
3      <files>
4          <service_access service='mysql'>
5          <port>3306</port>
6          <tcpwrapper>mysqld</tcpwrapper>
7          </service_access>
8      </files>
9      <variables />
10     <constraints />
11     <help />
12 </creole>
```


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

```
<!-- vim: ts=4 sw=4 expandtab
-->
```

Pour qu'il soit pris en compte il faut procéder à la reconfiguration du serveur :

```
root@eolebase:~# reconfigure
```

Vérifier la connexion entre le serveur hébergeant EoleDB et le serveur Eolebase :

```
root@scribe:~# mysql -u admin -h <IPServeurEoleDB> -peole21
mysql>
```


À partir de la version 2.6.1 il n'est plus nécessaire de procéder à l'ouverture de port à l'aide d'un dictionnaire. En effet, depuis cette version, l'onglet expert `Mysql` permet de déclarer des adresses IP ou des réseaux autorisés à accéder à MySQL.

Serveur non EOLE

Exemple d'une distribution GNU/Linux supportant le système de paquet debian.

Installation du serveur de base de données :

```
# apt-get install mysql-server
```

Se connecter à MySQL avec l'utilisateur root :

```
# mysql -u root -h localhost -p<motDePasse>
```

Créer un utilisateur autre que `root` (le mot de passe du compte `root` est généré à chaque `reconfigure`) et lui donner les privilèges et l'autorisation de se connecter depuis le serveur hébergeant EoleDB :

```
mysql> grant all privileges on *.* to admin@<IPServeurEoleDB> identified
by "<motDePasse>";
mysql> quit
```

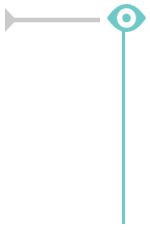
Vérifier la connexion entre le serveur hébergeant EoleDB et le serveur hébergeant la base de données :

```
root@scribe:~# mysql -u admin -h <IPServeurEoleDB> -peole21
mysql>
```

Appliquer la configuration EoleDB

Pour que les changements soient pris en compte il faut exécuter la commande `eole_db_gen`.

L'appel de cette commande `eole_db_gen` doit au minimum préciser le répertoire utilisé pour sauvegarder les fichiers modifiés par EoleDB avec l'option **-b**.



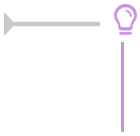
```
root@scribe:~# eole_db_gen -b /var/backup/eole-db
TASKFREAK :
  >>> Passwords    [OK]
  >>> Create       [OK]
  >>> Update       [OK]
root@scribe:~#
```

La commande utilise les fichiers de configuration par défaut d'eoleDB, mais il est possible de préciser

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

d'autres fichiers de configuration :

- **-c** : permet de définir un fichier de configuration a utiliser à la place de `/etc/eole/eole-db.conf`
- **-d** : permet de définir un répertoire différent de `/etc/eole/eole-db.d/` et qui contient les fichiers de configuration des applications



Pour connaître les différents paramètres de la commande `eole_db_gen` :

```
# eole_db_gen --help
```

9. Configuration du module Eclair avec un module Horus

Le module Eclair a été conçu pour fonctionner conjointement avec les serveurs de fichiers EOLE : Scribe, Horus et AmonEcole.

Afin de simplifier sa mise en place dans un environnement existant, nous préconisons de conserver (ou de mettre en place) le service DHCP sur le serveur de fichiers et que celui-ci diffuse l'adresse du serveur TFTP du serveur Eclair.

Utiliser le module Eclair conjointement avec le module Horus permet :

- d'utiliser l'annuaire utilisateurs présent sur le module Horus pour authentifier les utilisateurs sur le module Eclair ;
- d'utiliser les répertoires utilisateur présents sur le module Horus (protocole NFS) ;
- d'utiliser le service DHCP du module Horus.

Configuration du module Horus

Exports NFS

Installer le paquet eole-nfs :

```
# apt-eole install eole-nfs
```

Autoriser le module Eclair à monter les export NFS.

Se rendre dans l'interface de configuration du module, dans l'onglet `Nfs` et saisir l'adresse IP du module Eclair dans le champ : `Adresse IP autorisée à monter les exports NFS`.

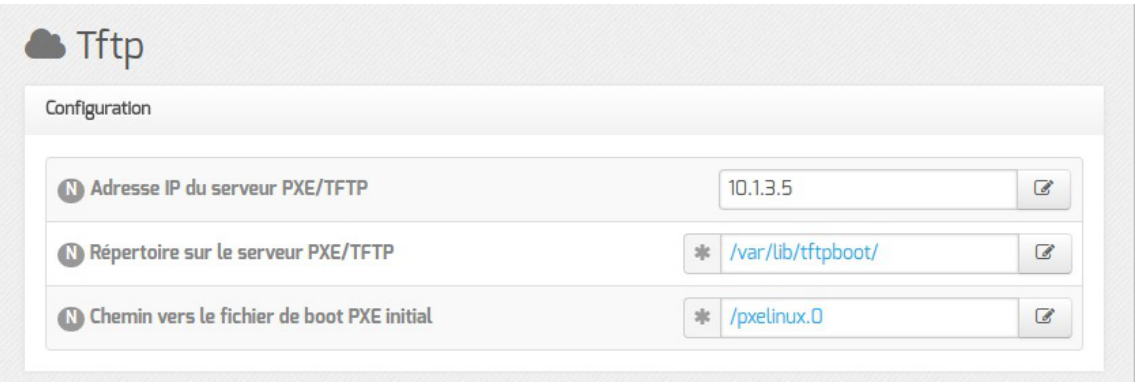


Services DHCP et TFTP

Pré-requis : le module Horus est déjà configuré en tant que DHCP.

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

En mode expert, dans l'onglet `Services`, passer la variable `Activer l'utilisation d'un serveur PXE/TFTP` à `oui` puis dans l'onglet Tftp, renseigner l'adresse IP du serveur Eclair dans le champ : `Adresse IP du serveur PXE/TFTP`.



Vue de l'onglet Tftp

Reconfiguration

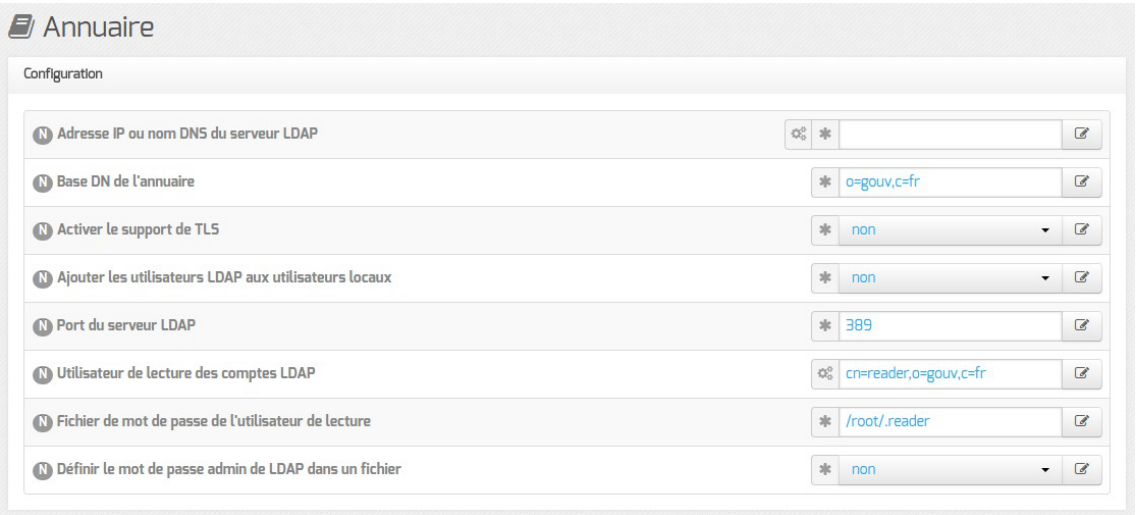
Reconfigurer le serveur à l'aide de la commande `reconfigure`.



Si ce n'est pas déjà fait, pensez à attribuer un shell valide aux utilisateurs susceptibles d'utiliser les clients légers.

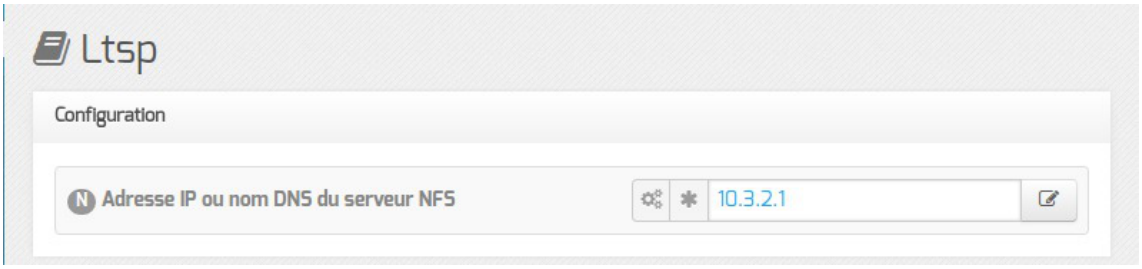
Configuration du module Eclair

Dans l'onglet `Annuaire`, renseigner l'adresse IP du serveur Horus dans le champ : `Adresse IP ou nom DNS du serveur LDAP`.



Dans l'onglet `Ltsp`, vérifier que le champ : `Adresse IP ou nom DNS du serveur NFS` contient bien l'adresse du serveur Horus.

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



10. 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.752] s'effectue en déclarant au minimum deux interfaces réseau dans la variable experte `Nom de l'interface réseau` dans un onglet `Interface-n`.



L'utilisation de l'agrégation de liens Ethernet[p.752] nécessite de disposer d'un Commutateur réseau[p.755] 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.755] parmi :

- balance-rr ;
- active-backup ;

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

- 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.

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

Un SAN[p.777], tout comme un NAS[p.770] usant des protocoles NFS[p.770] ou SMB[p.778], permet de partager de l'espace disque via une image disque simulant un disque dur ou d'un disque complet, via le protocole iSCSI[p.766].

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

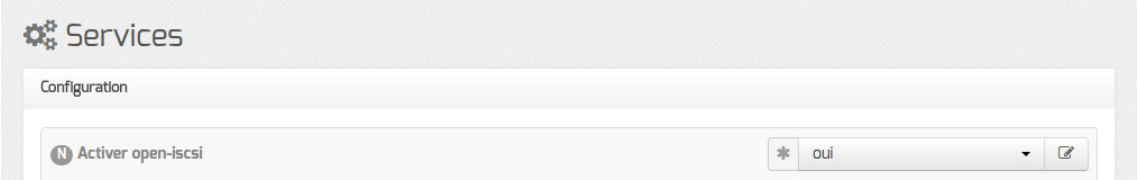
Le paquet `eole-open-iscsi` s'installe manuellement sur un module EOLE :

```
# 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`.



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

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.

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.770] 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...

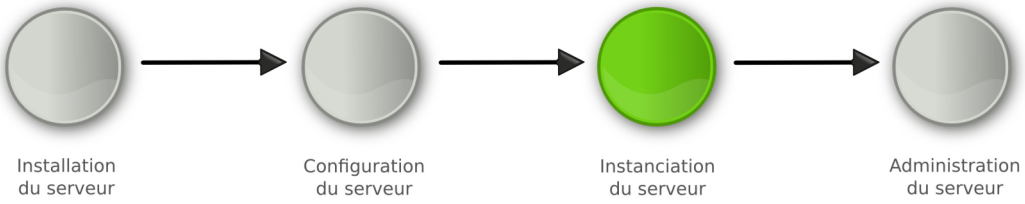
Onglet Réseau avancé [p.170]

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.781] 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.774] 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.616]

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.754] 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.

```
1 Créer un nouvel administrateur eole2 ? [oui/non]
2 [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.667]

2.4. Le redémarrage

Il est possible qu'un redémarrage soit proposé à la fin de l'instanciation.

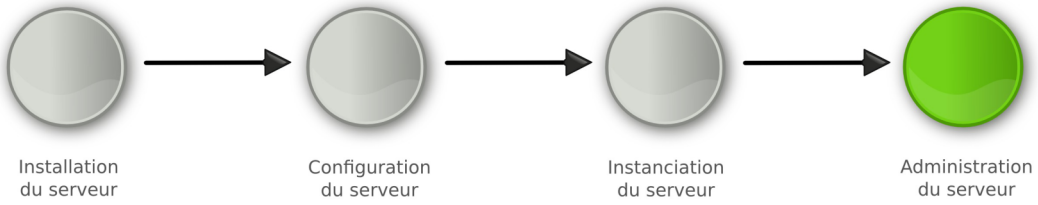
Si le noyau (kernel) a été mis à jour, le serveur doit redémarrer pour pouvoir l'utiliser. Dans ce cas, la question suivante apparaîtra :

```
Un redémarrage est nécessaire
Faut-il l'effectuer maintenant ? [oui/non]
```


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

Chapitre 8

Administration du module Horus

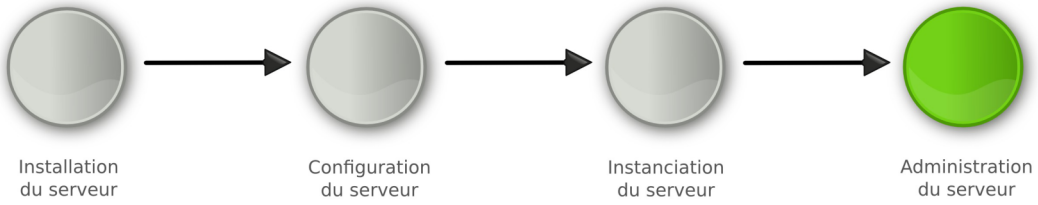


Administration

- 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.767]
- des outils périphériques = GNU [p.763]
- 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.

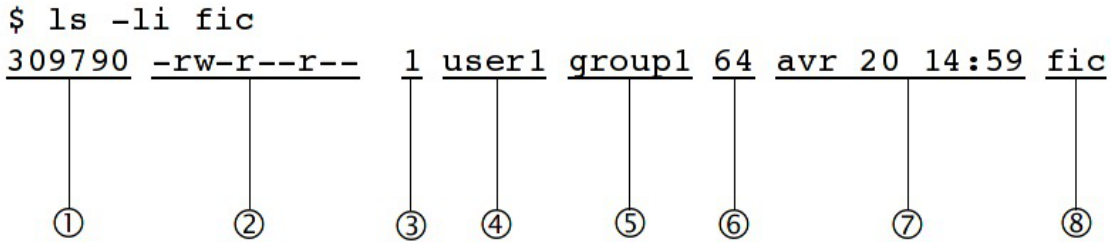
Droits essentiels :

- 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.779] (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.763]. 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 :

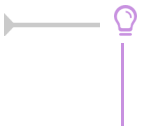
```
scp utilisateur@ip_serveur:/repertoire/source/nom_du_fichier /repertoire/de/destination/
```

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.780] et SSH[p.779] 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.

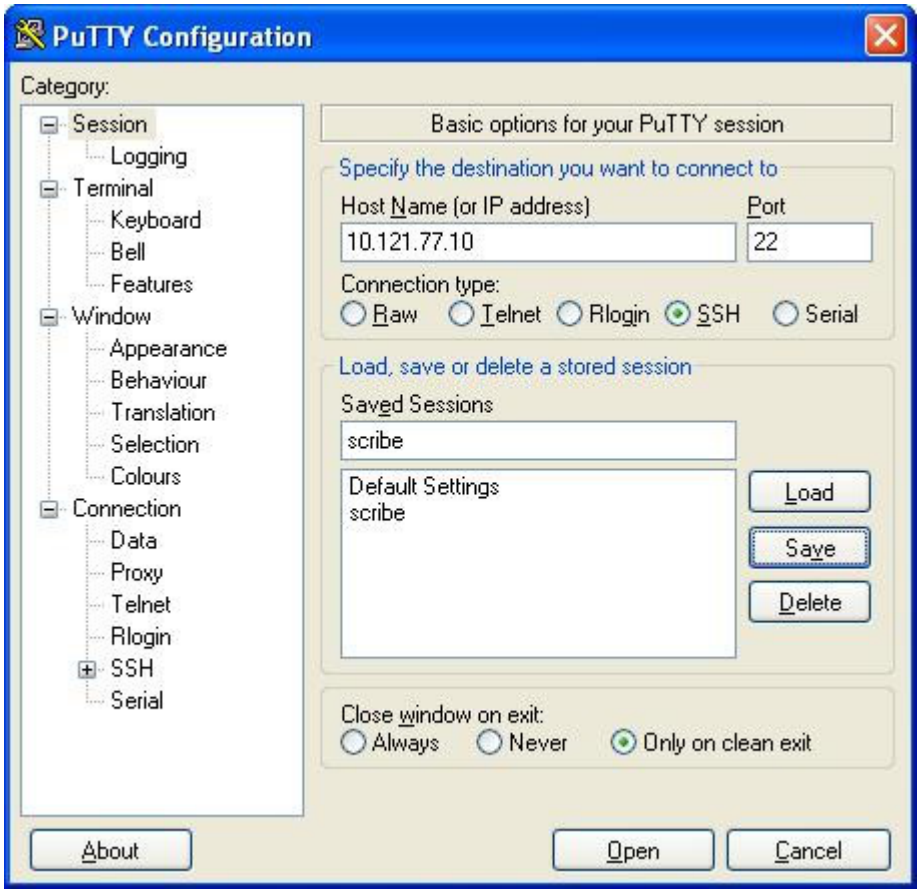
La connexion avec Putty au serveur se fait en utilisant le protocole SSH.

Sur le module Scribe, Putty est pré-installé dans le répertoire personnel d'*admin* (`U:\client\putty.exe`).

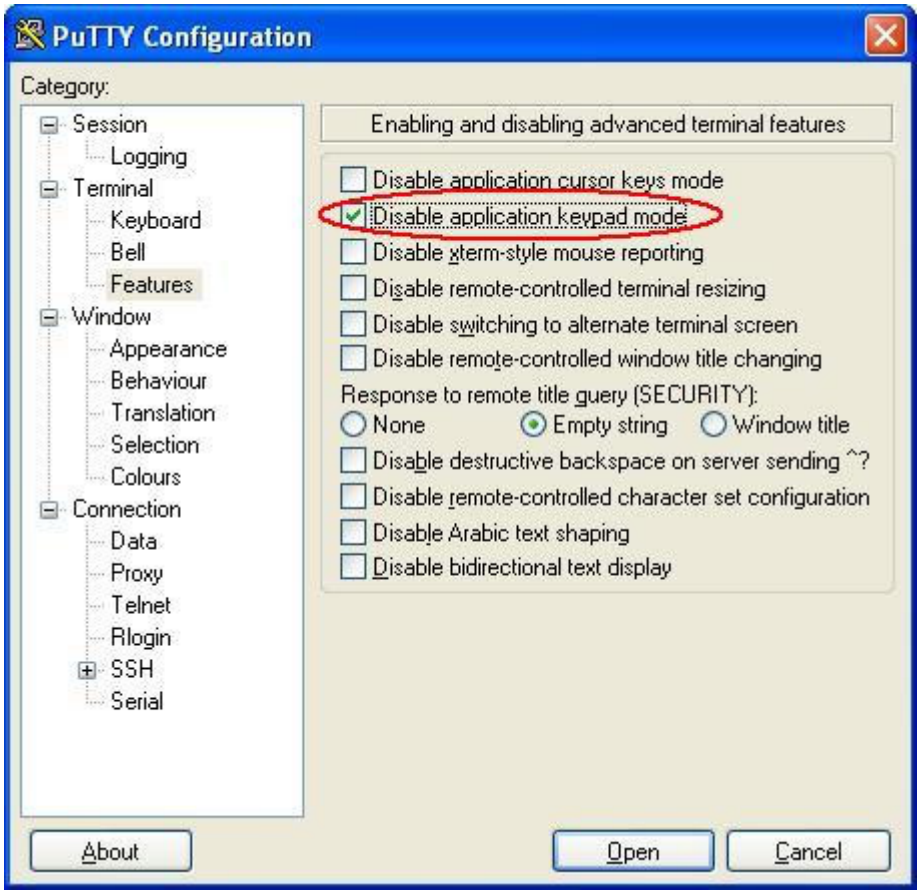
Configuration pour les serveurs EOLE

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)

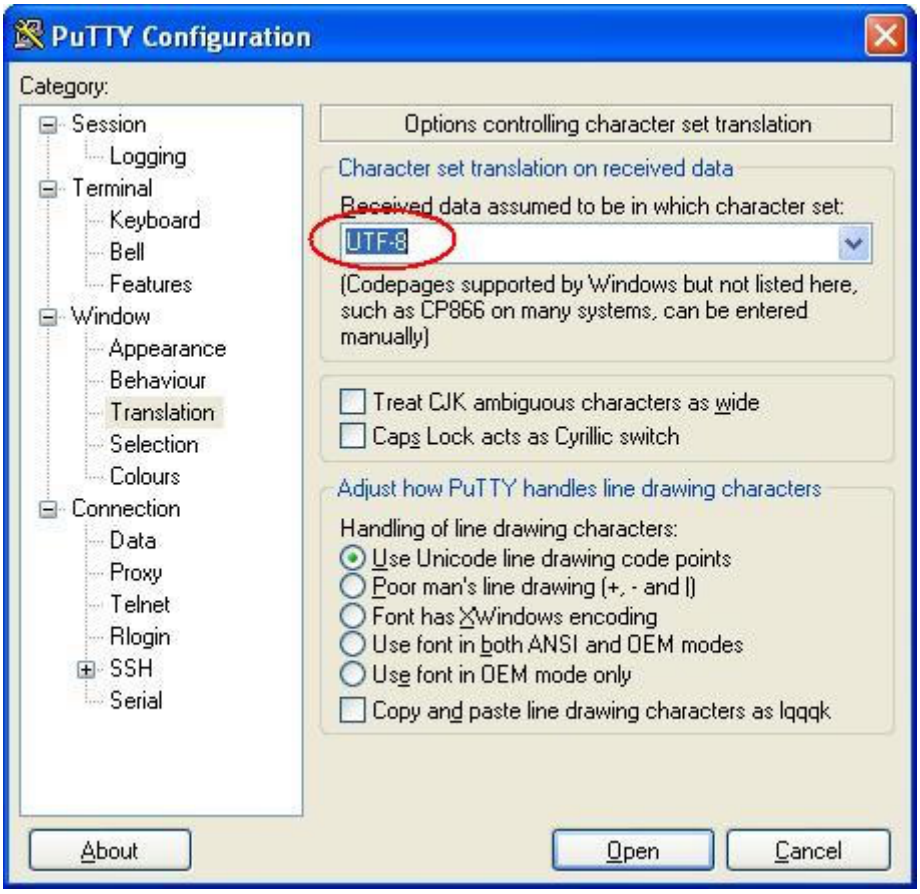


Fenêtre principale

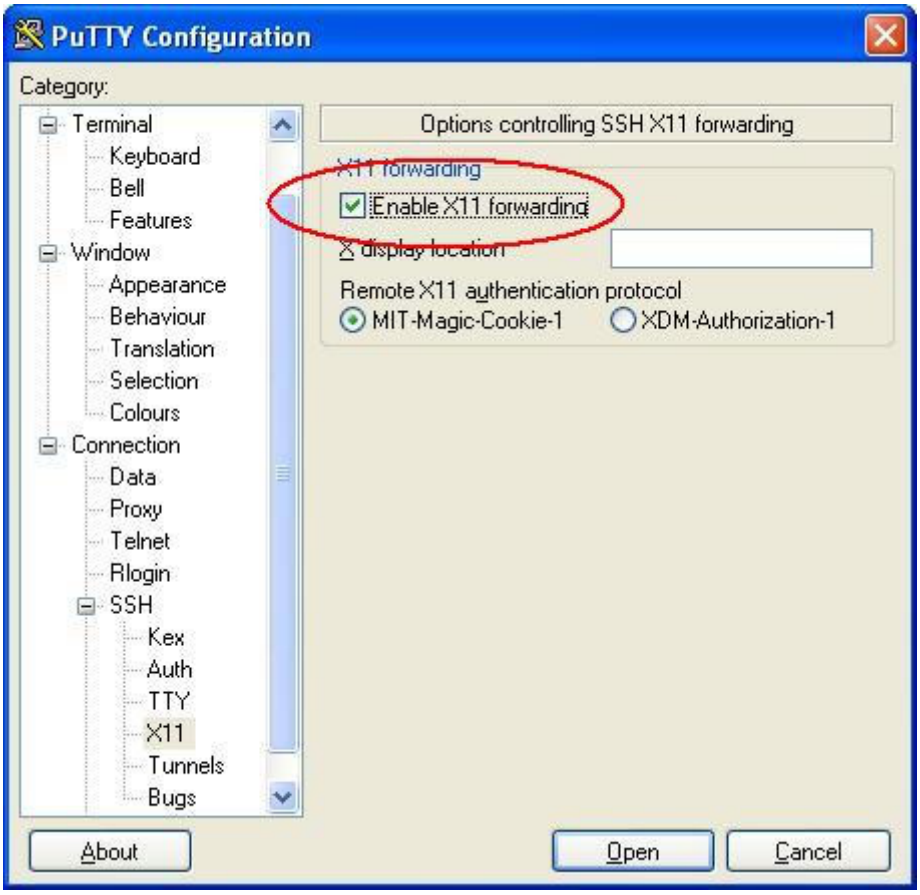


Permettre au pavé numérique de fonctionner correctement (dans "vim" par ex.)

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



Permettre aux accents de s'afficher normalement



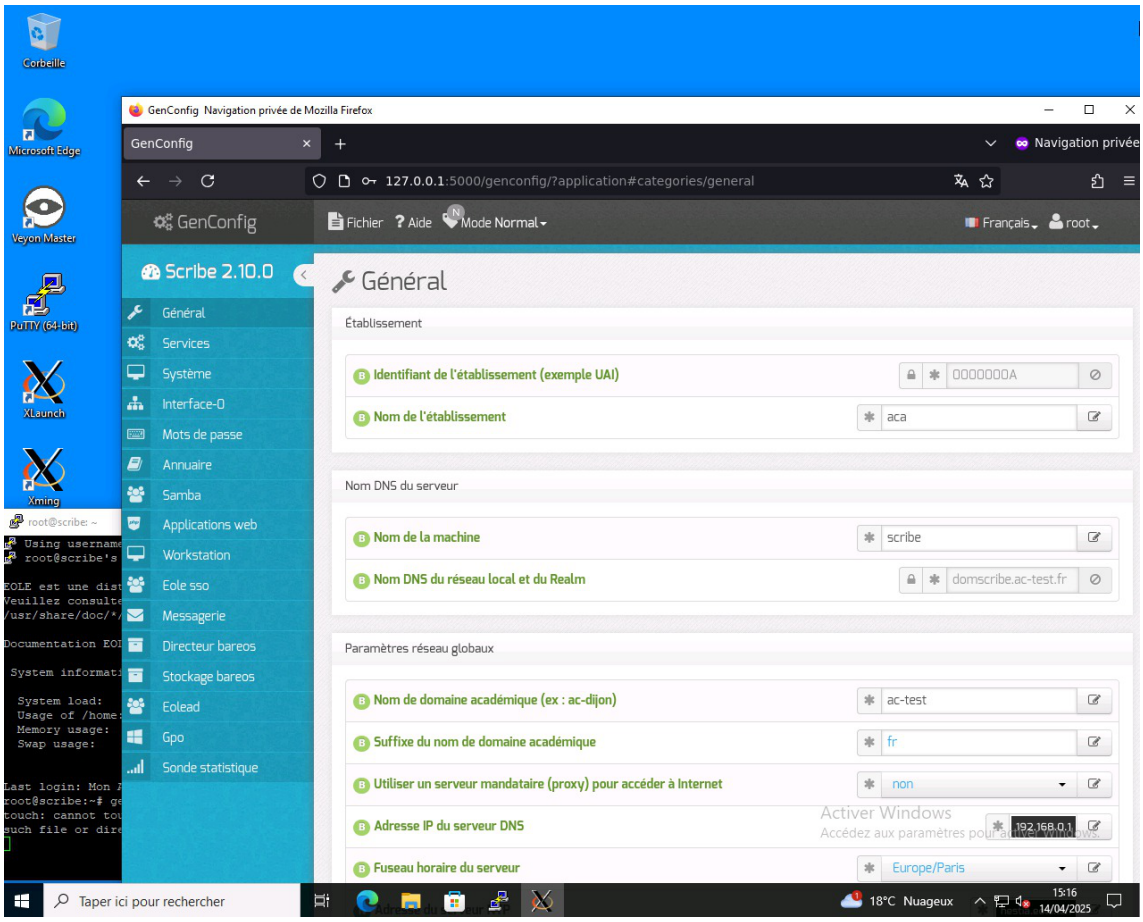
Pouvoir lancer des applications graphique du serveur depuis la station (Ex. "gen_config")

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.766] 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.778] 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.774] 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.759], `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.764] 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.

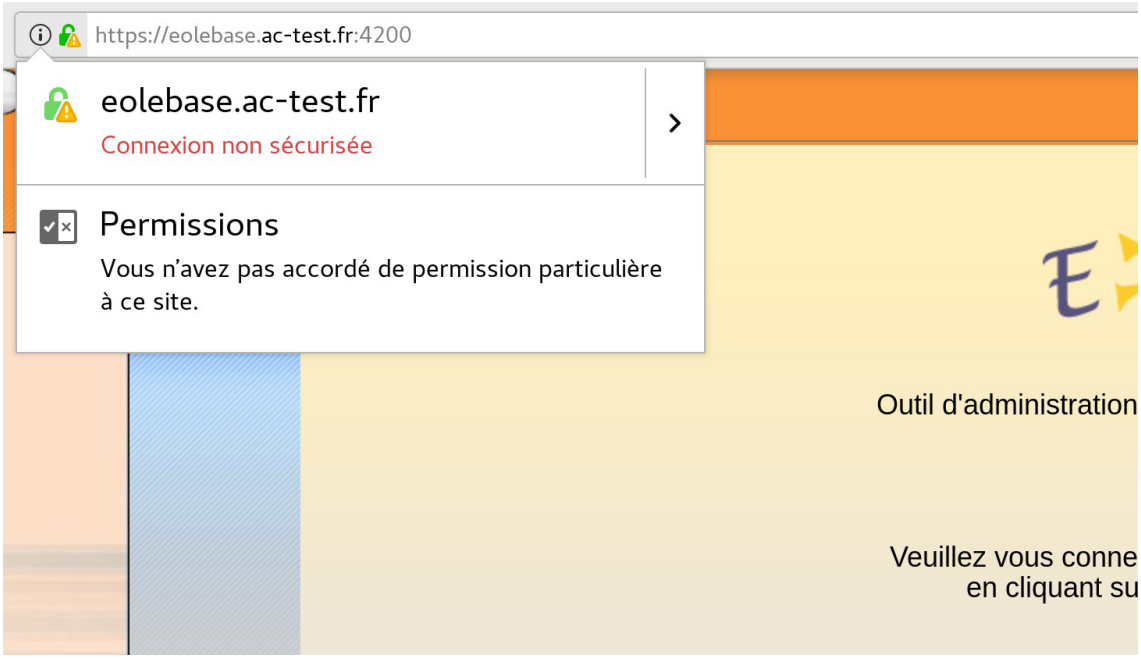
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

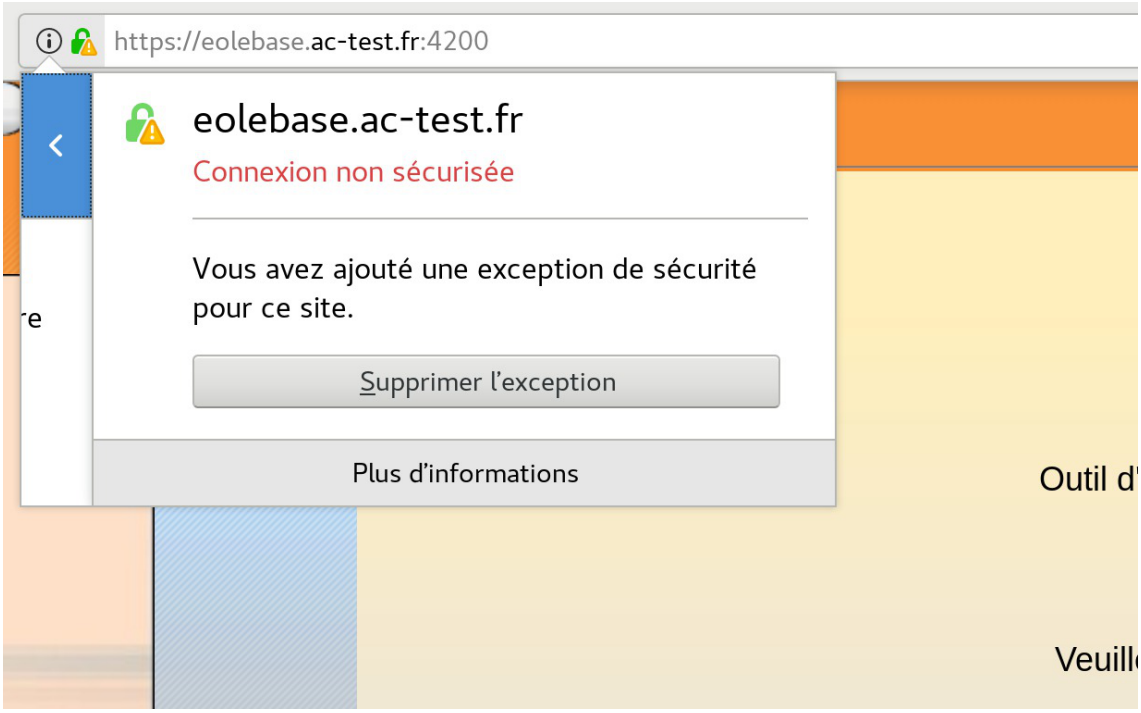
Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

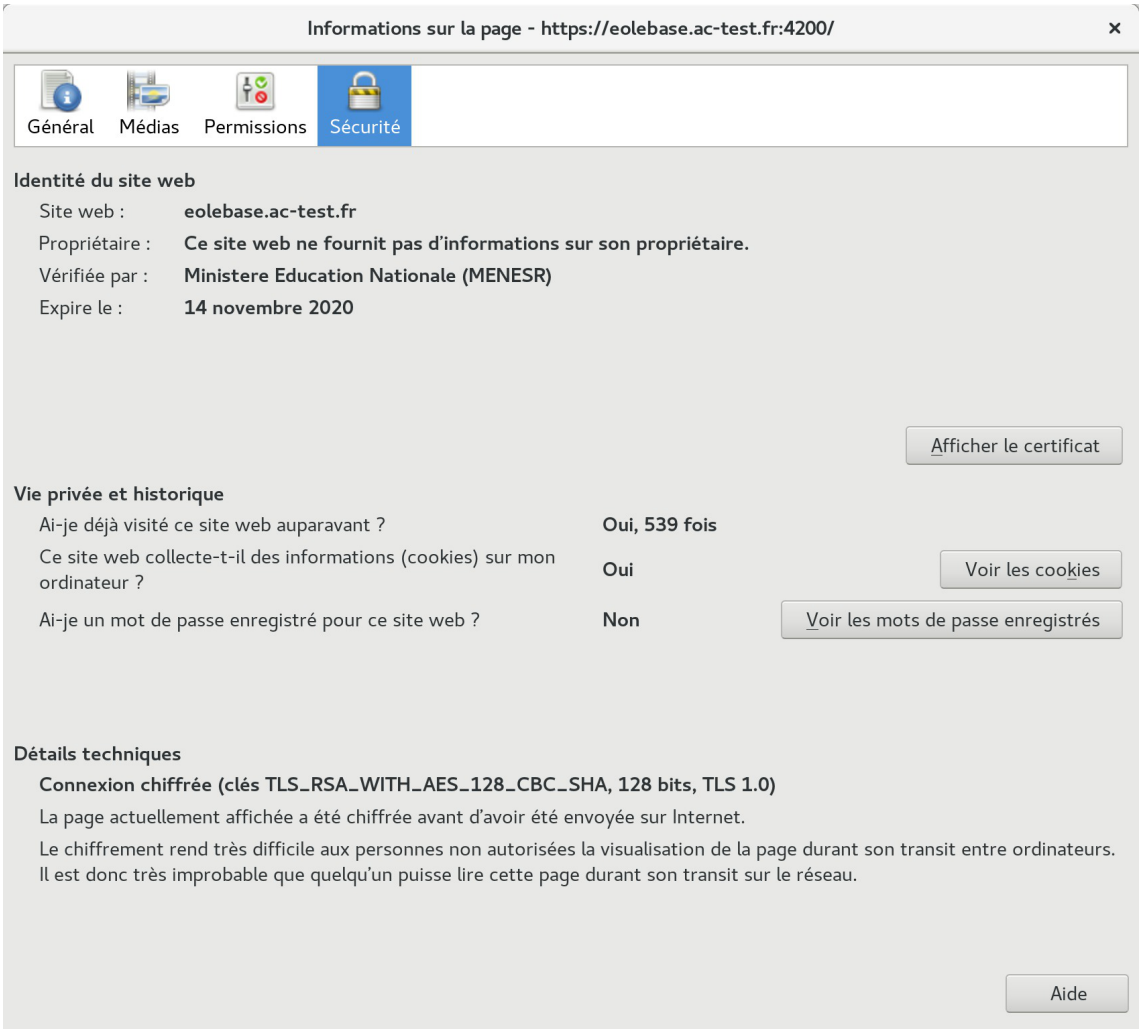


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion



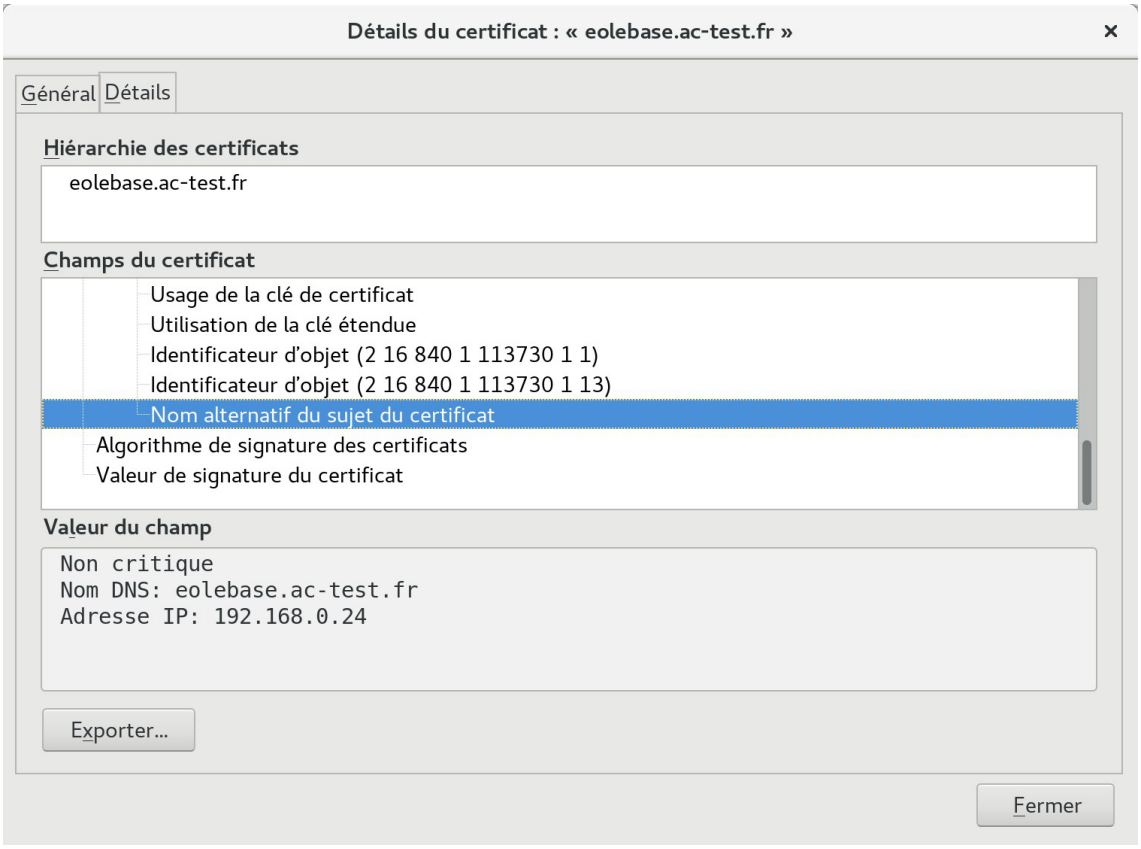
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`

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).

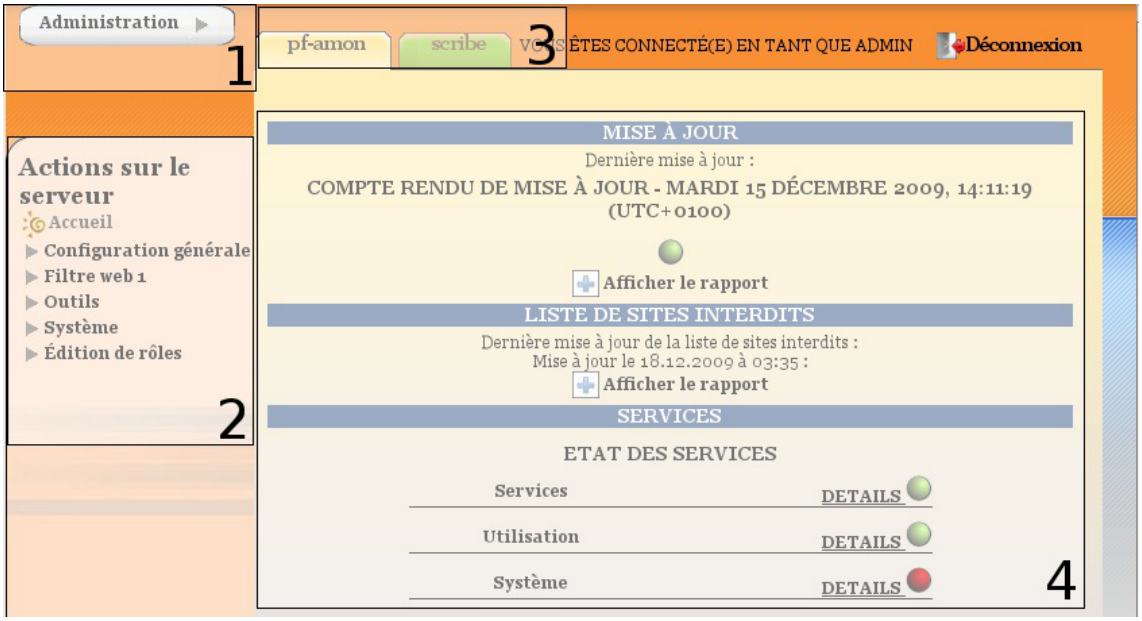
```
# reconfigure
# /usr/share/creole/gen_certif.py -f ou #
```


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`

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.379]

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.758] : `ead scribe`.

Voir aussi...

Onglet Ead-web : EAD et proxy inverse [p.224]

Onglet Reverse proxy : Configuration du proxy inverse [p.137]

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.764] 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.

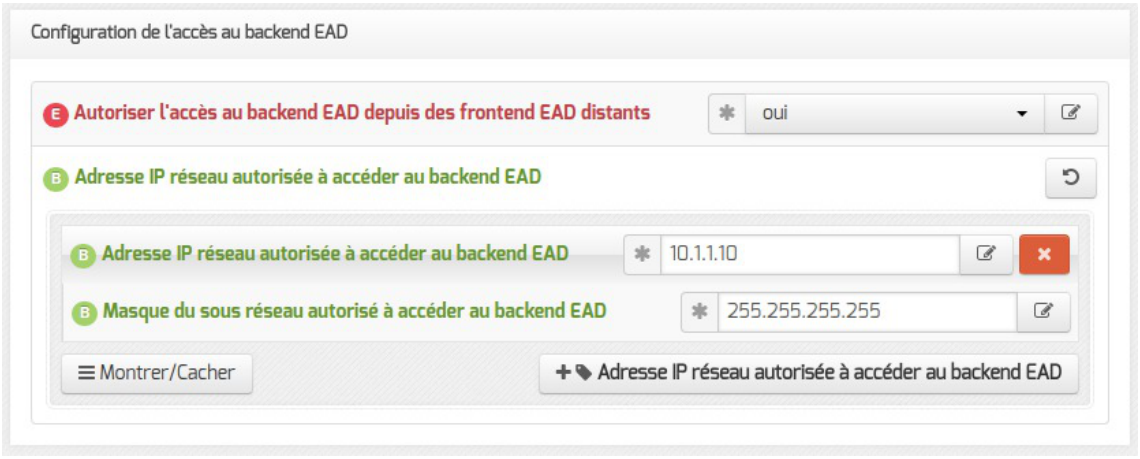
Il est possible d'enregistrer plusieurs serveurs EOLE sur l'interface.

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.

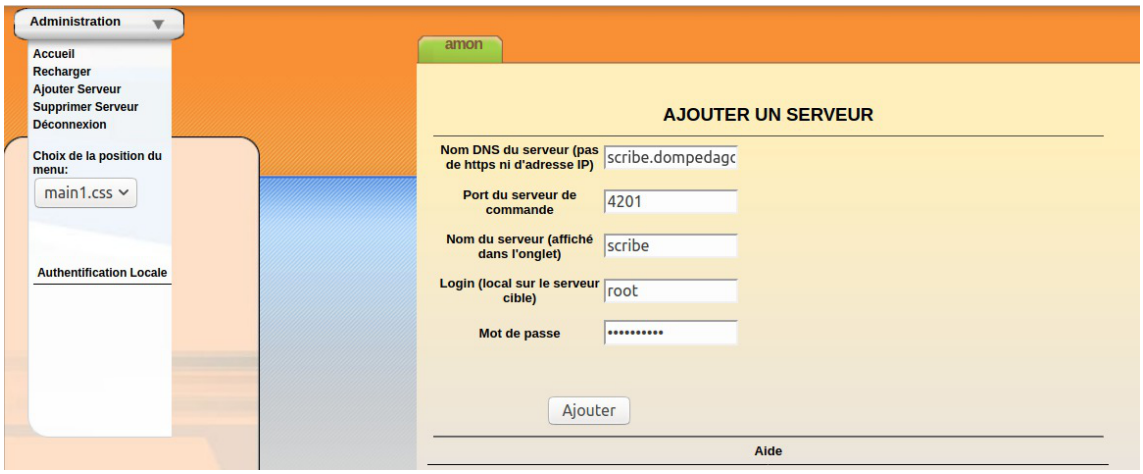
Ajout de serveur

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.753] 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.769] 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.758].

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

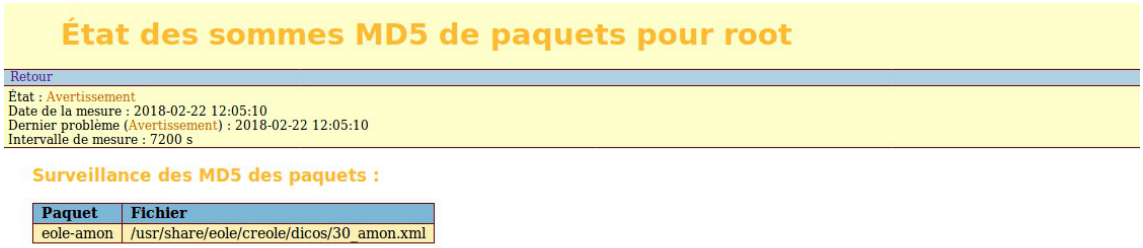
Ignored by eole
---------------

```

Un agent[p.752] 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.779]) ;
- 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`.

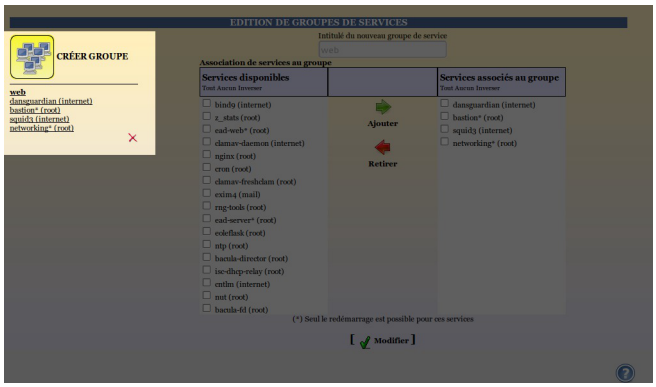


Création d'un groupe de services (1)



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`

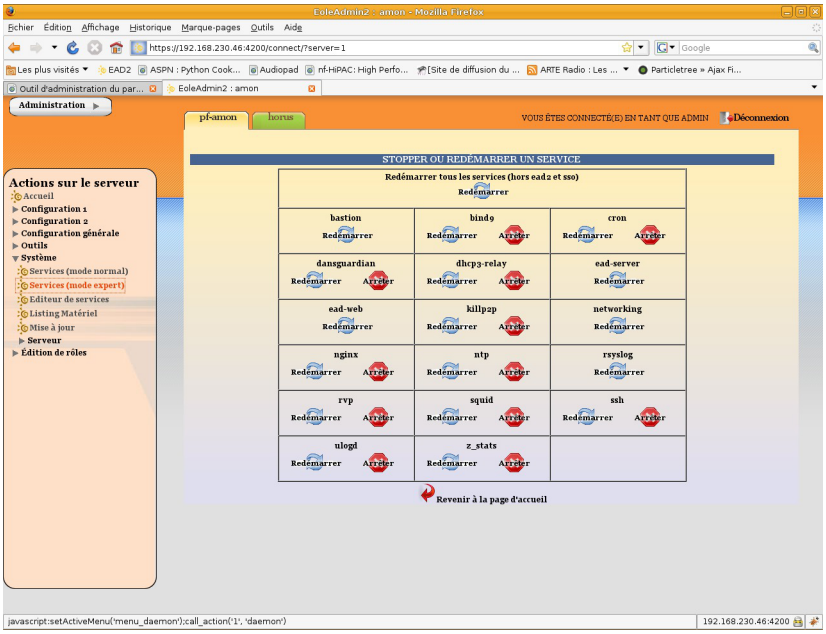
`[amon]`

`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

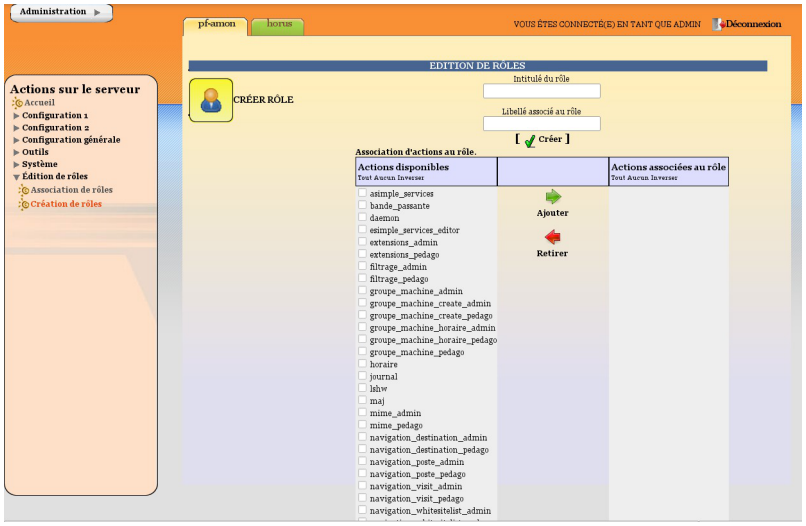
Pour créer un nouveau rôle cliquer sur :

- 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)

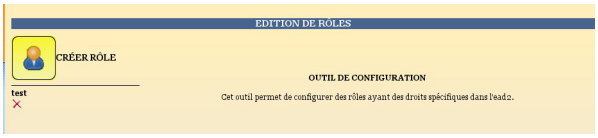
- **printers** : action de gestion des imprimantes.

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.765] 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.

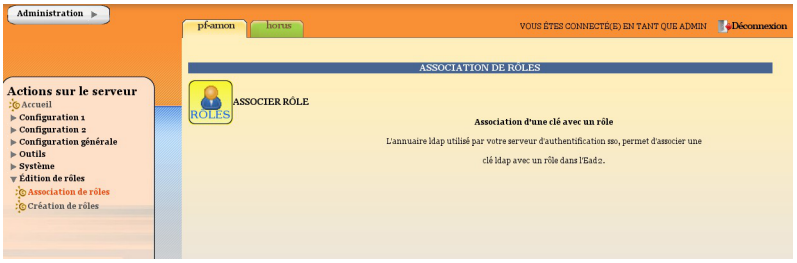
Création d'association via l'EAD

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

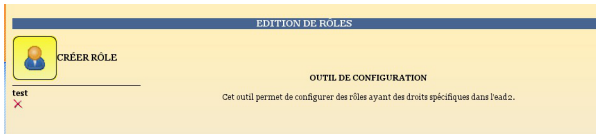
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

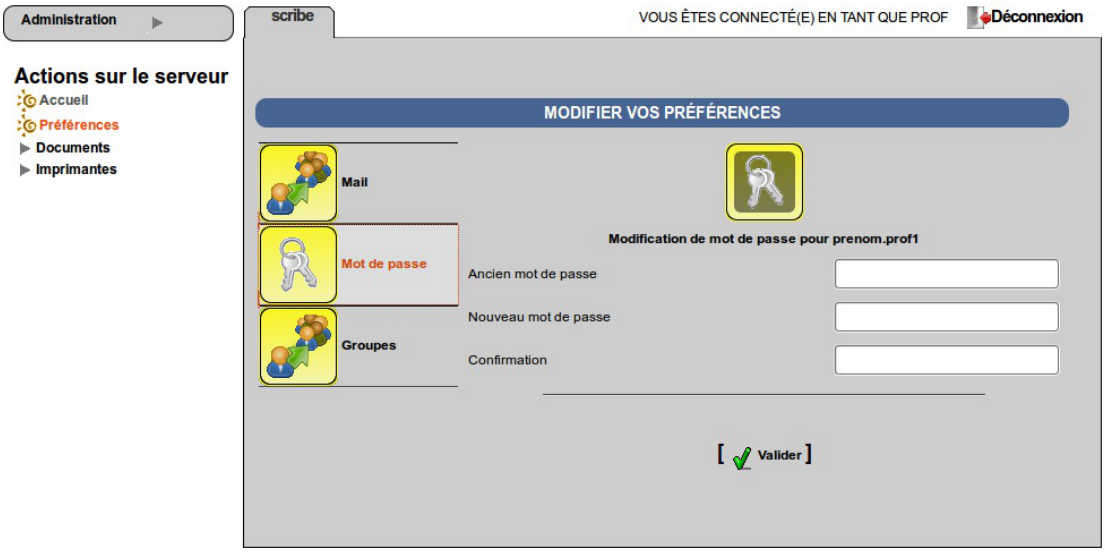


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

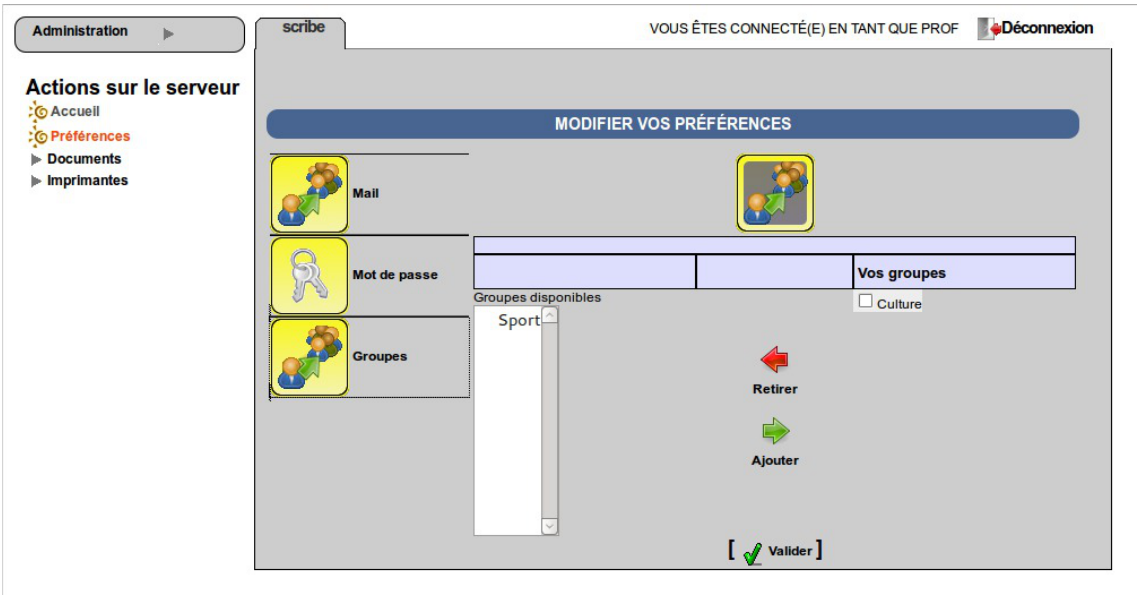
- modifier son mot de passe ;

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



EAD vue enseignant avec thème Envole, changement de mot de passe

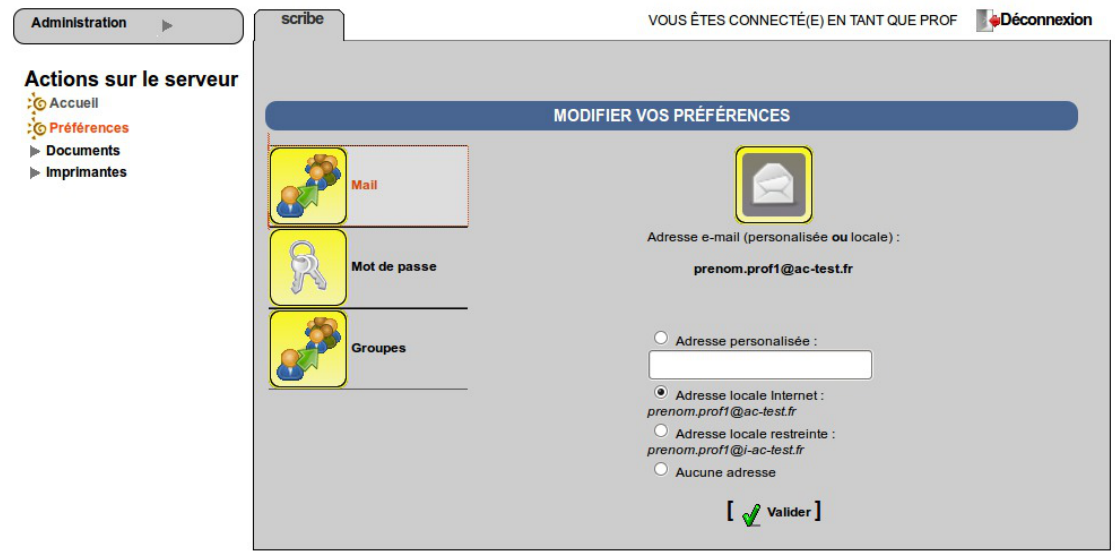
- s'inscrire/se désinscrire d'un groupe ;



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)

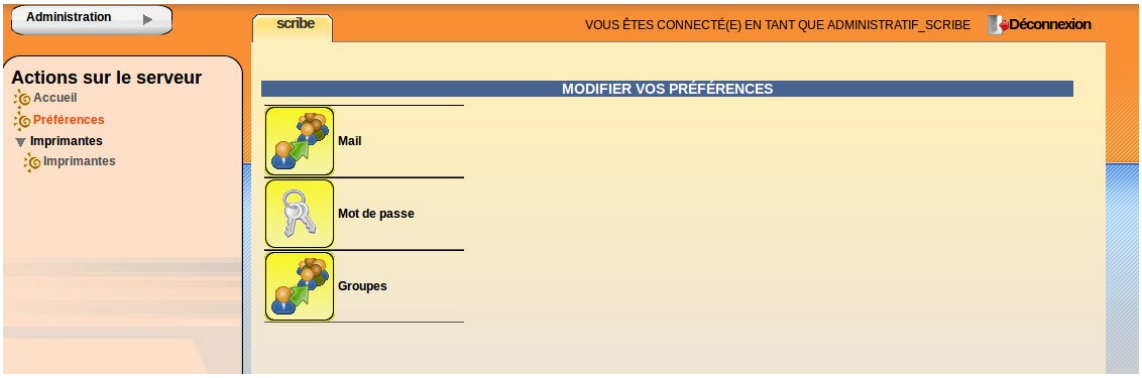
Un professeur peut être responsable de plusieurs classes.

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.

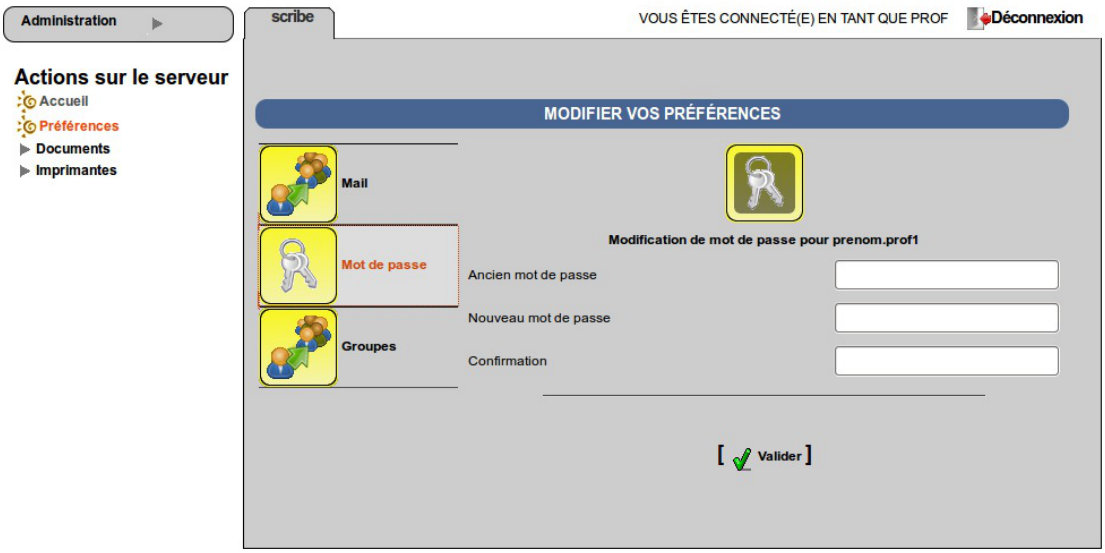
Accès "Administratif du Scribe"

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 :

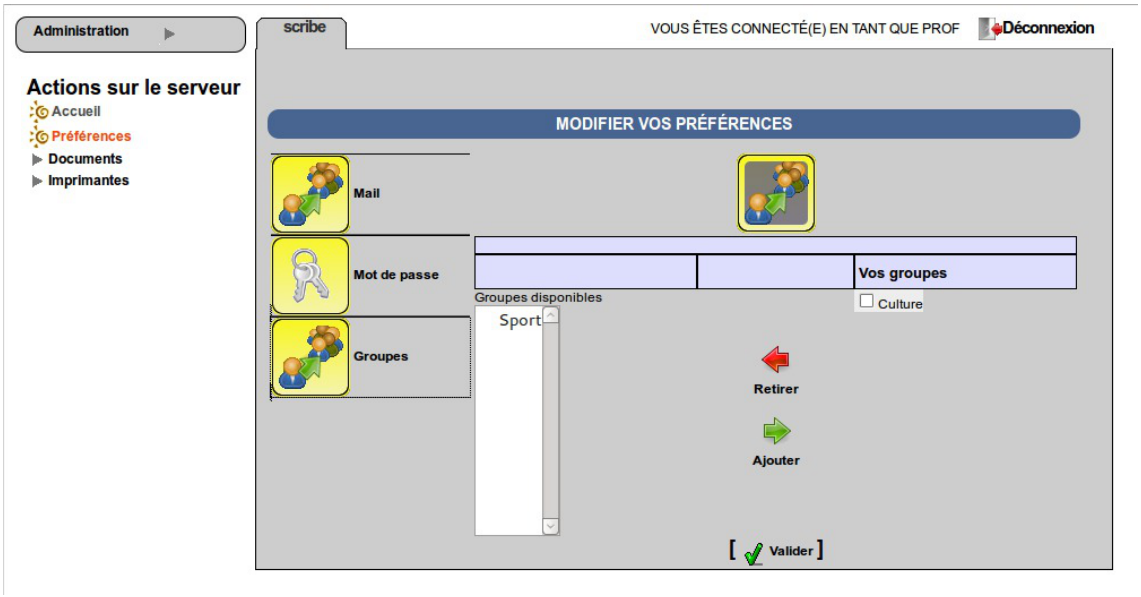
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

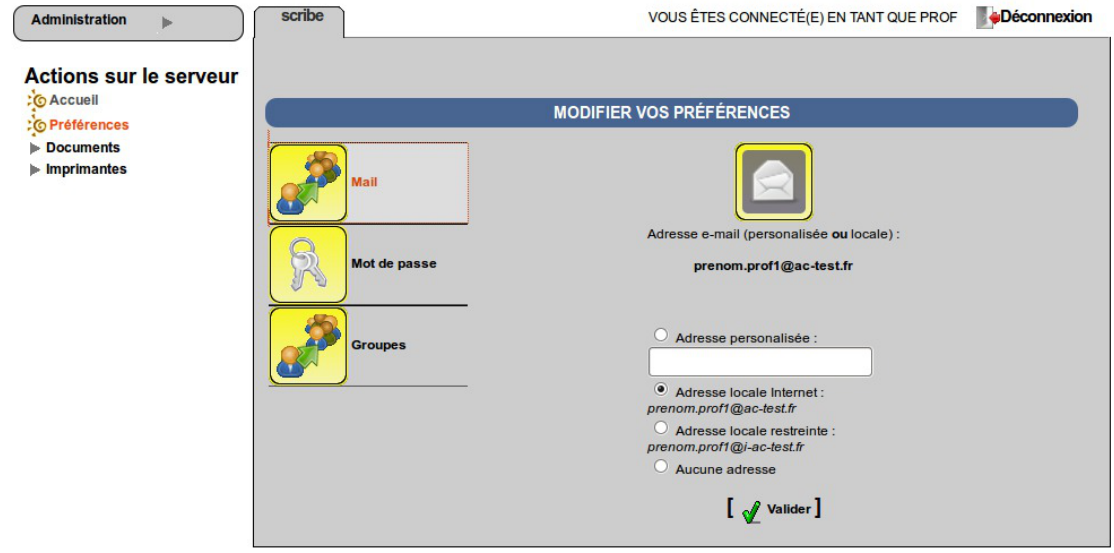
- s'inscrire/se désinscrire d'un groupe ;

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.

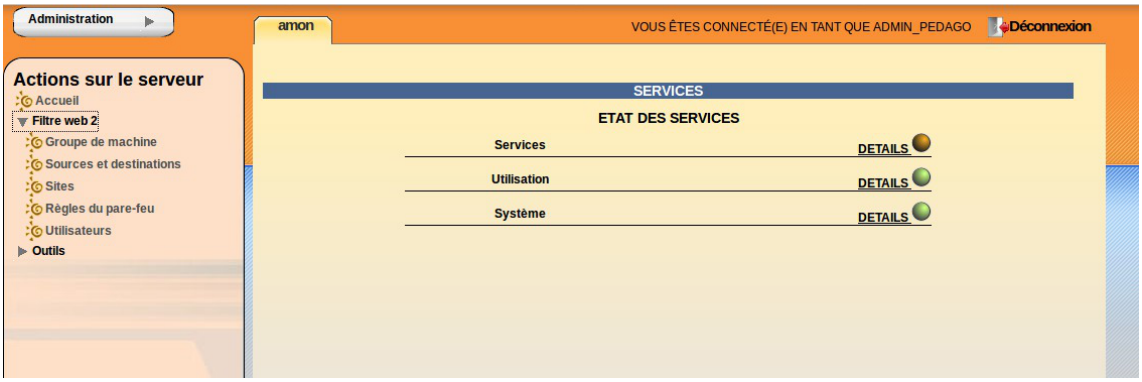
Fonctionnalités Amon

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 :

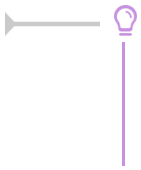
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

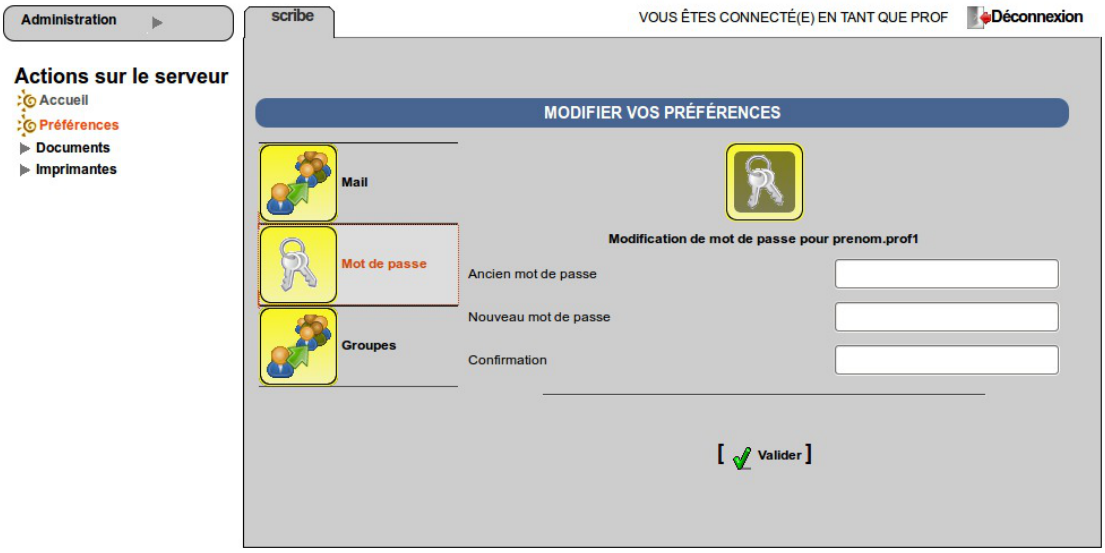


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

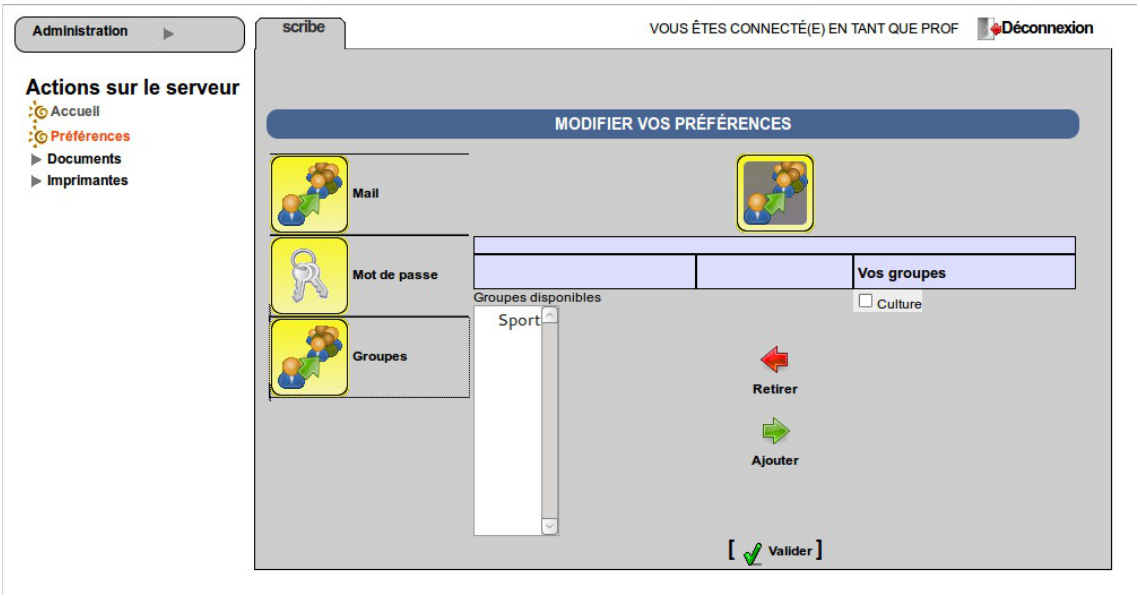
- modifier son mot de passe ;

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



EAD vue enseignant avec thème Envole, changement de mot de passe

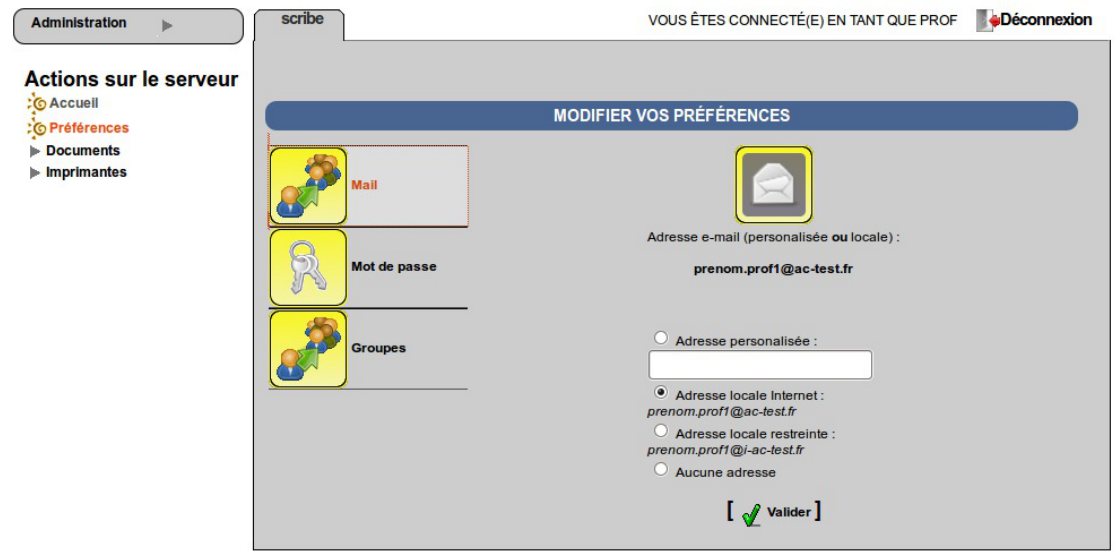
- s'inscrire/se désinscrire d'un groupe ;



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)

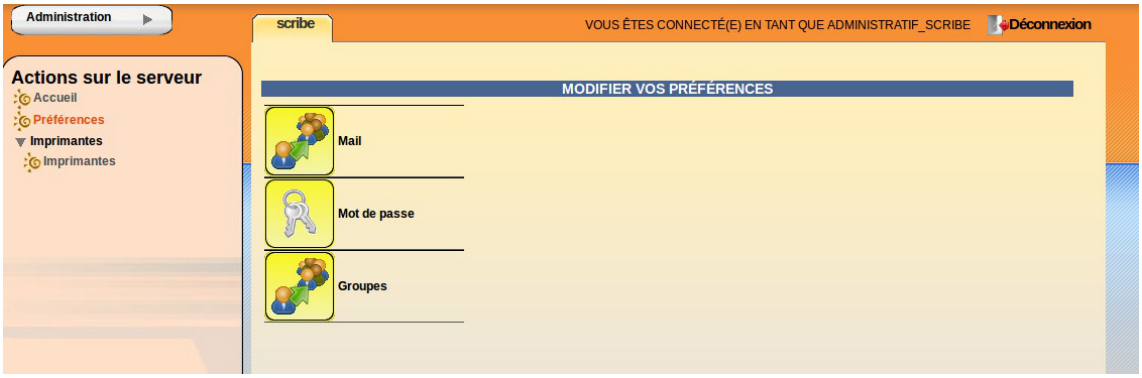
Un professeur peut être responsable de plusieurs classes.

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.

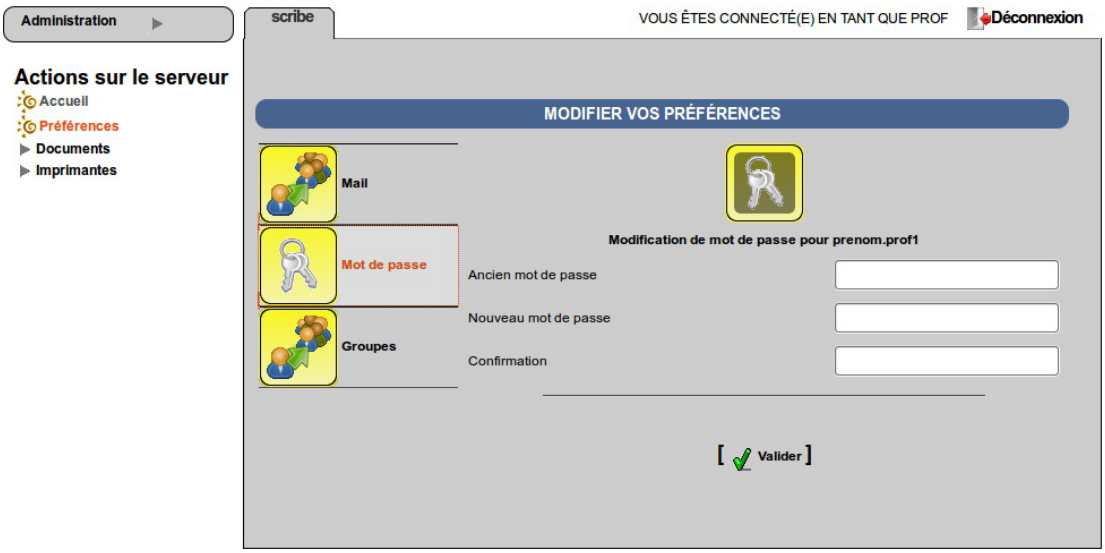
Accès "Administratif du Scribe"

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 :

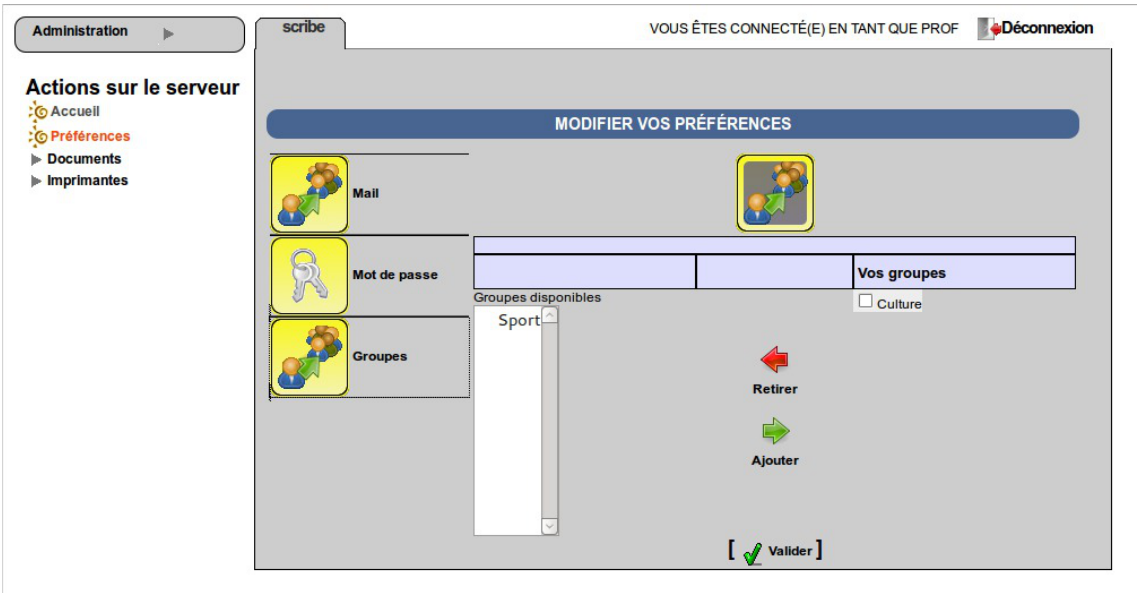
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

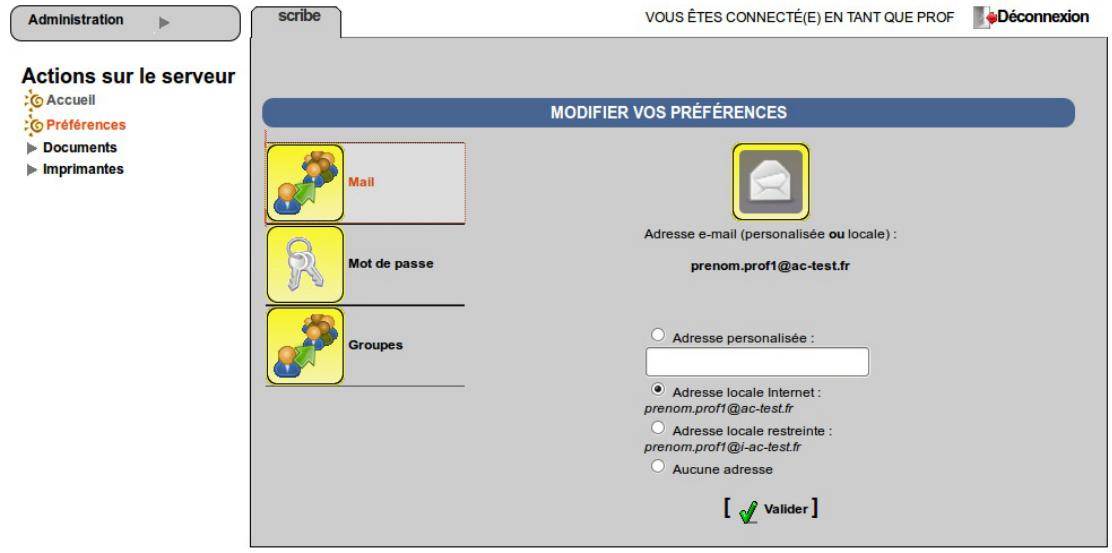
- s'inscrire/se désinscrire d'un groupe ;

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

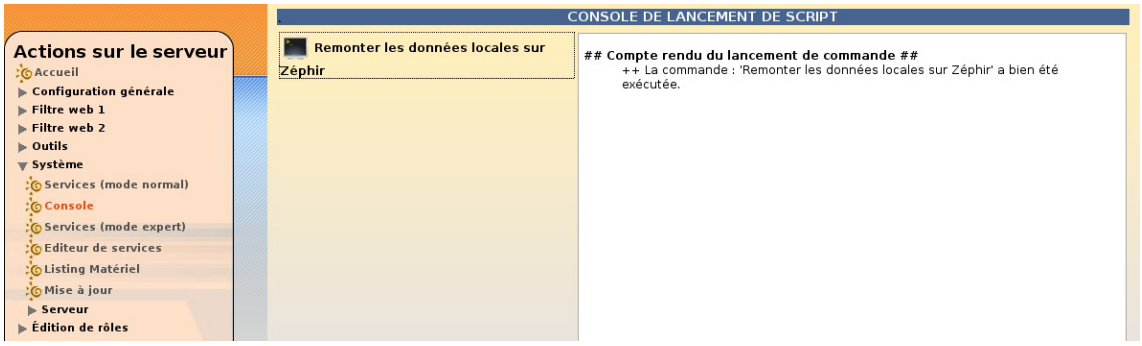
L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- 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

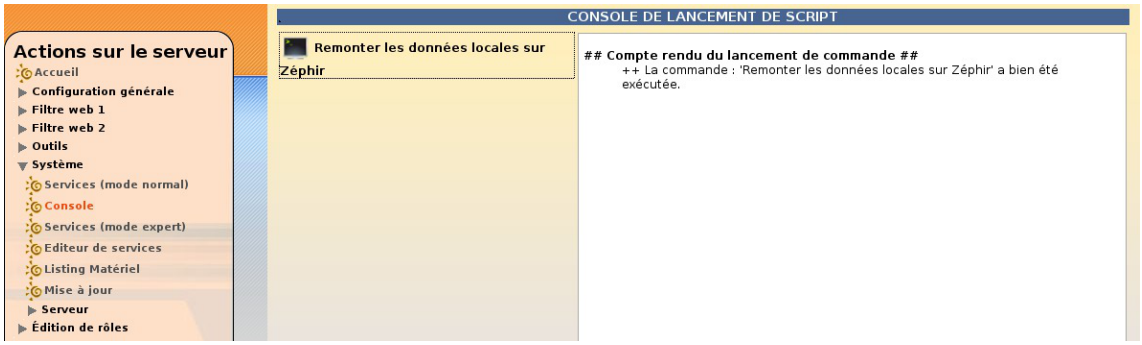
Seul le script Remonter les données locales sur Zéphir est fourni par défaut.



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 :

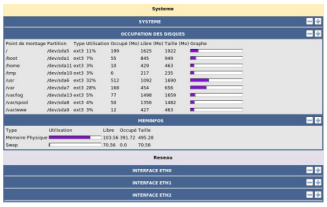
```
++ La commande : 'Occupation disque' a bien été exécutée.
```

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)

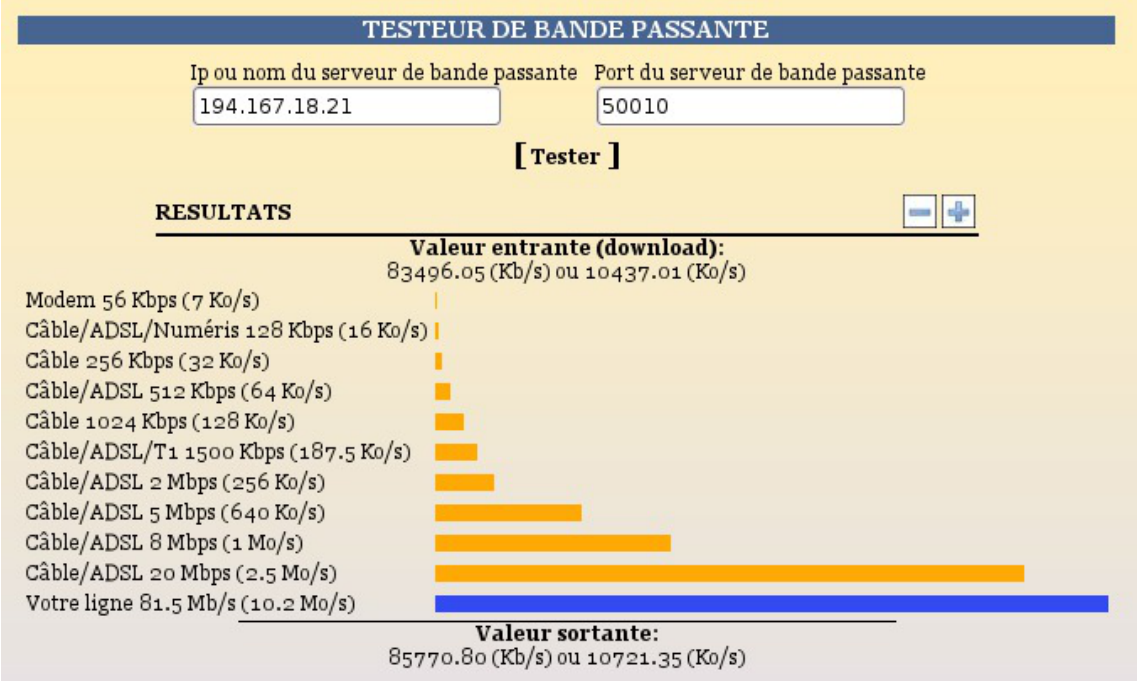
Le noyau Linux[p.767] utilise un système de cache mémoire pour limiter les accès disque. Le chiffre "mémoire physique" comprend ce cache. Cela signifie qu'il n'est pas inquiétant de voir une valeur proche de 100%.

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.

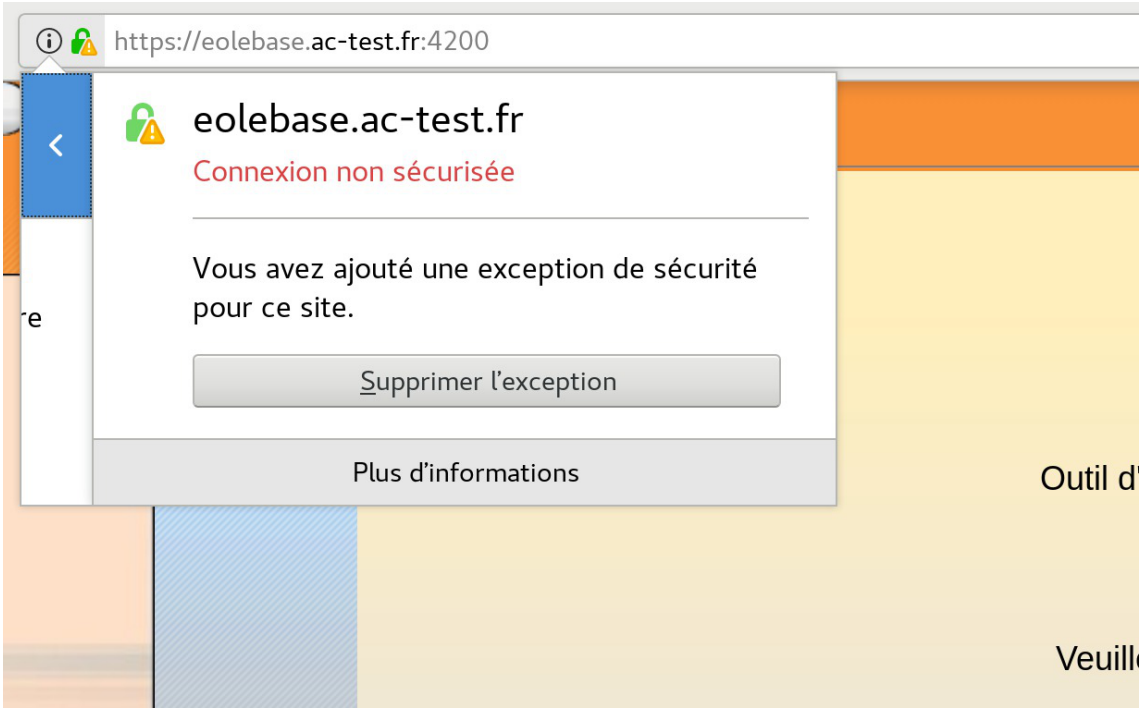
Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

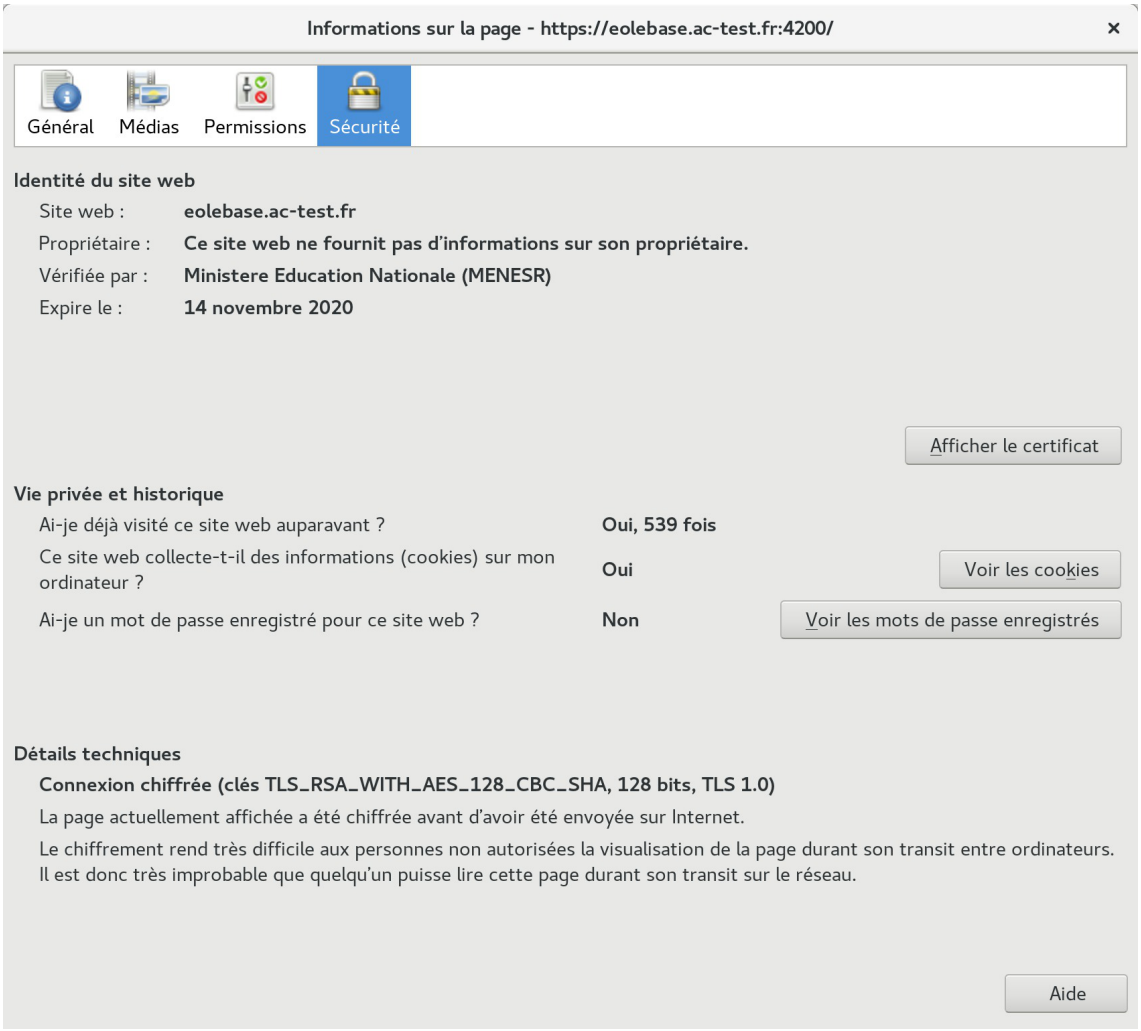


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion



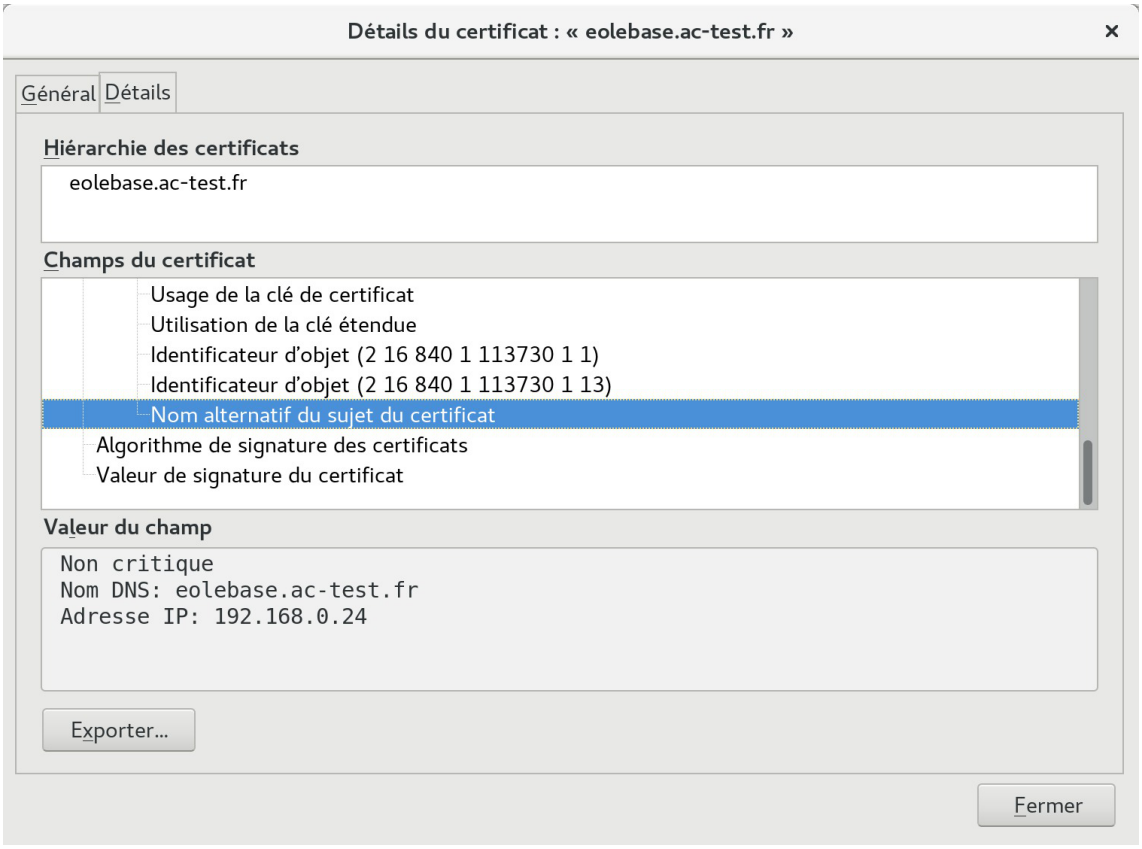
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`

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`

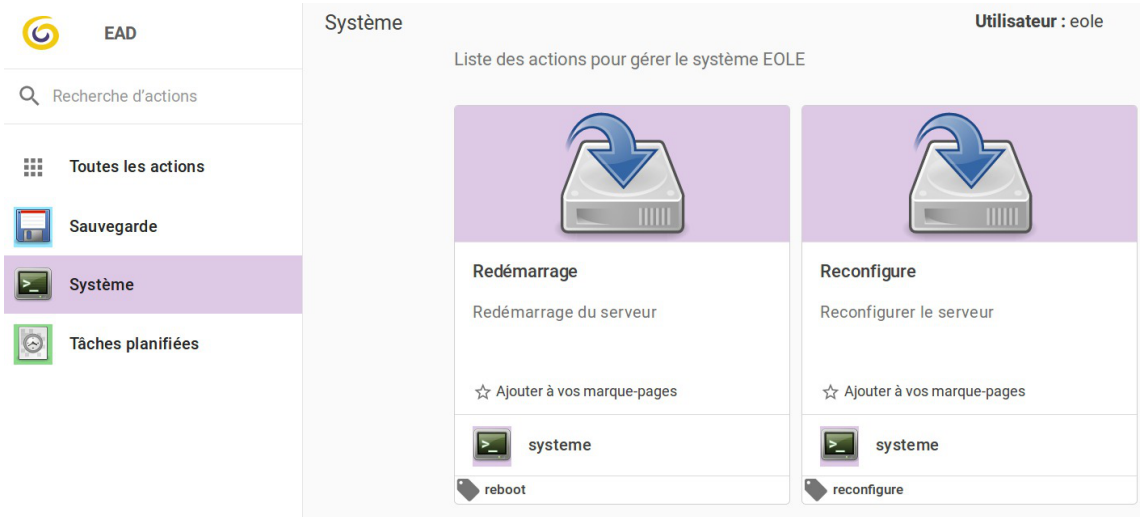
```
[1]
url = https://127.0.0.1
port = 4201
comment = amon
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

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/

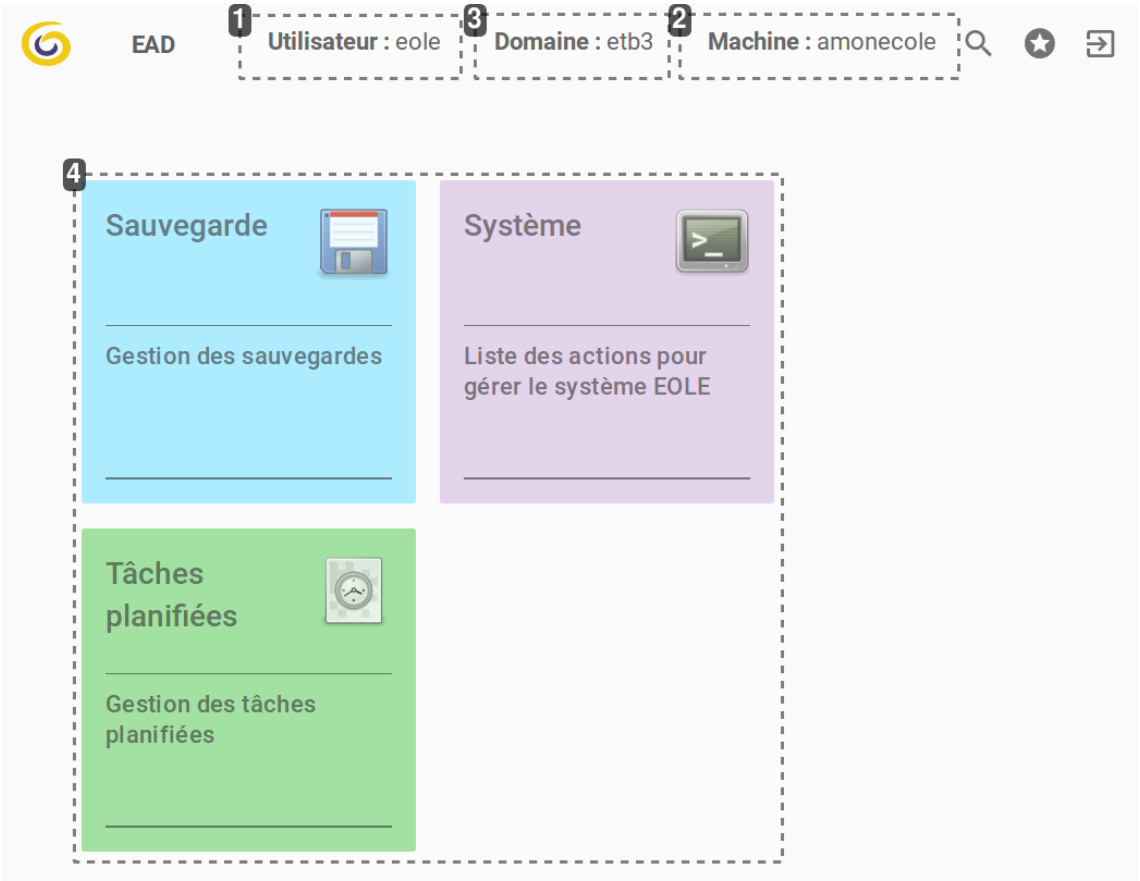
Une mire d'authentification apparaît. Saisir le compte et la clé secrète associée.

Pour le moment l'authentification est réalisée avec PAM[p.773], 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)

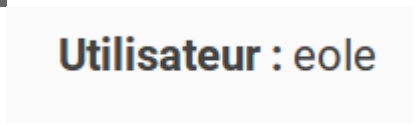


Description des éléments de la page principale



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)

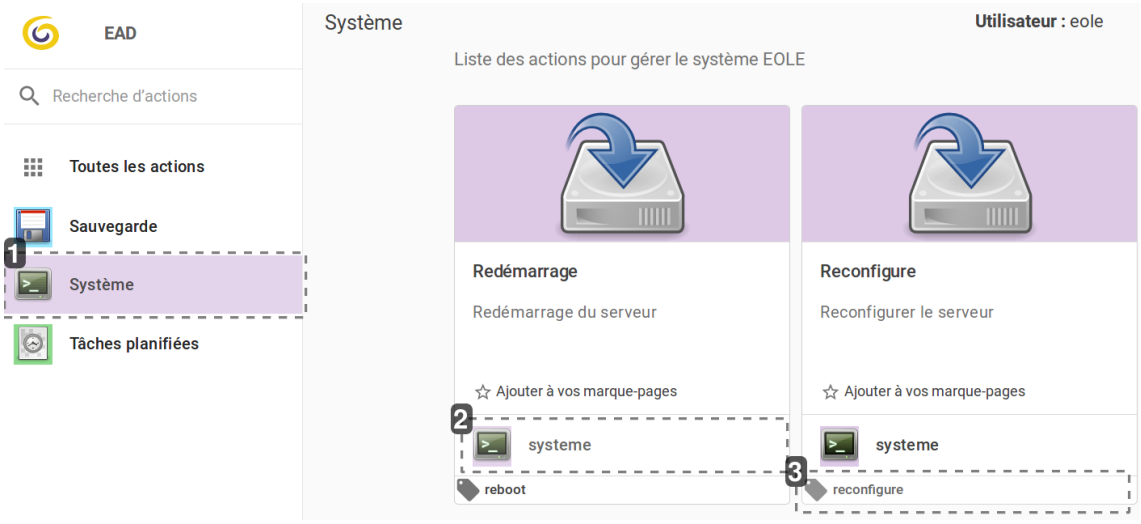
4



Catégories d'actions (exemple : sauvegarde, système…)

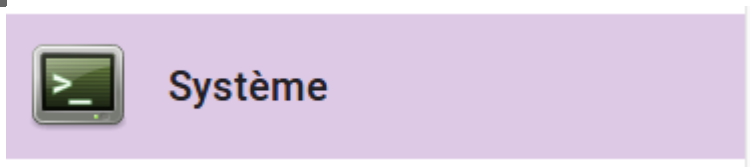
Cliquer sur une catégorie particulière permet d'afficher une vue propre à la catégorie.

Description de la vue par catégorie



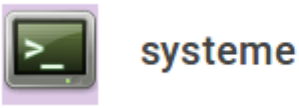
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1



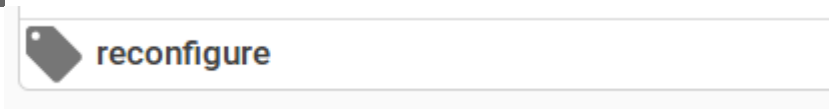
La catégorie choisie est en surbrillance.

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.757] 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.777] (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.766].

Dans ce cas, l'accès aux variables Creole se fait via les pillars[p.777].

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']*.

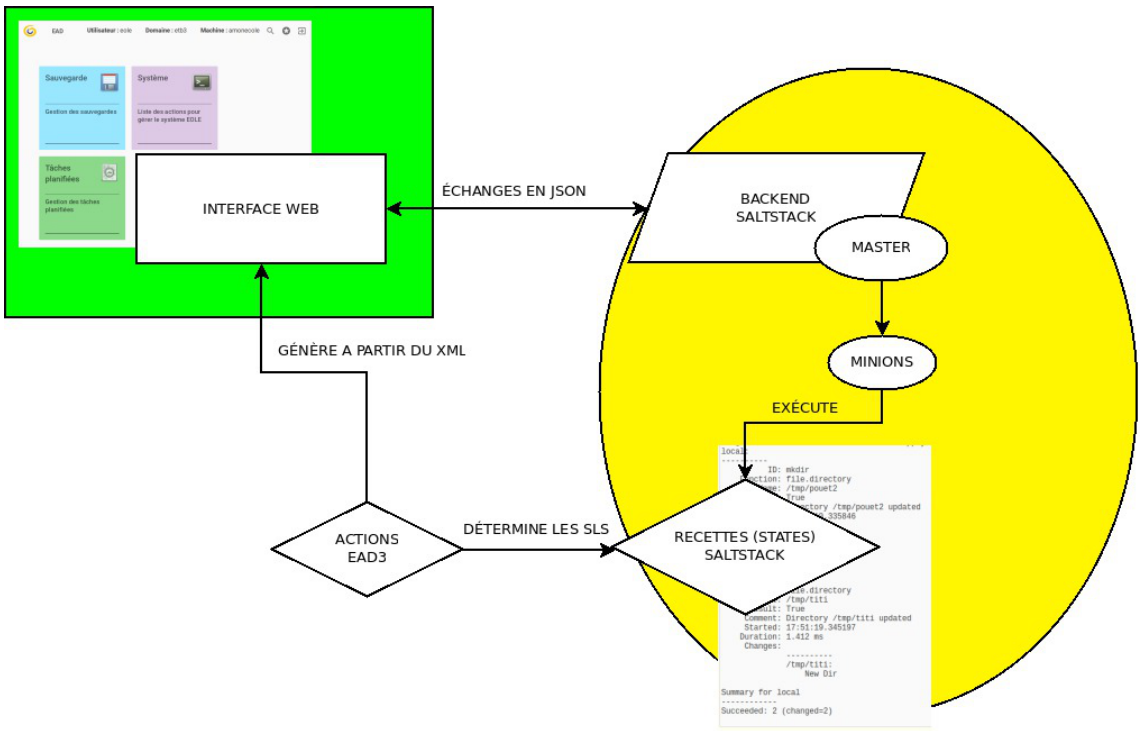


Diagramme de fonctionnement

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

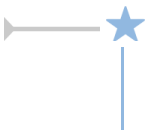
```
<creole>
<creole>
    <family_action name="Test"
     <family_action name="Mise à jour"
                   description="Test"
                    description="Gestion de la mise à jour"
                   color="#0000dd"
                    color="#fca474"
                   image="icons/mail-attachment.svg">
                    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
```



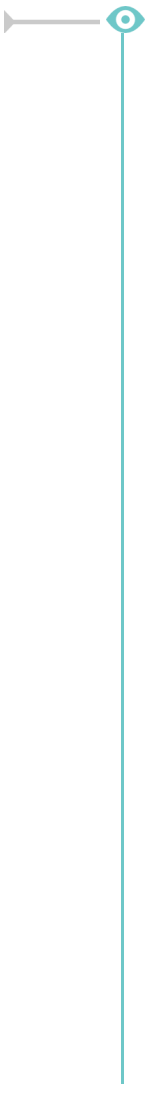
Dans un cas comme dans l'autre il est préférable de se déconnecter et se reconnecter à l'EAD.

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 :

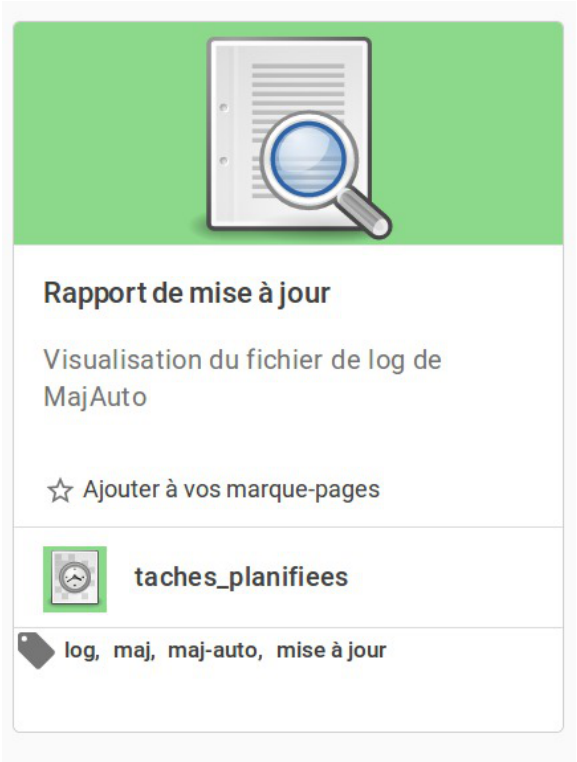
- *<family_action>* et *<action>* : permettent de définir l'action d'une manière générique ;

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.

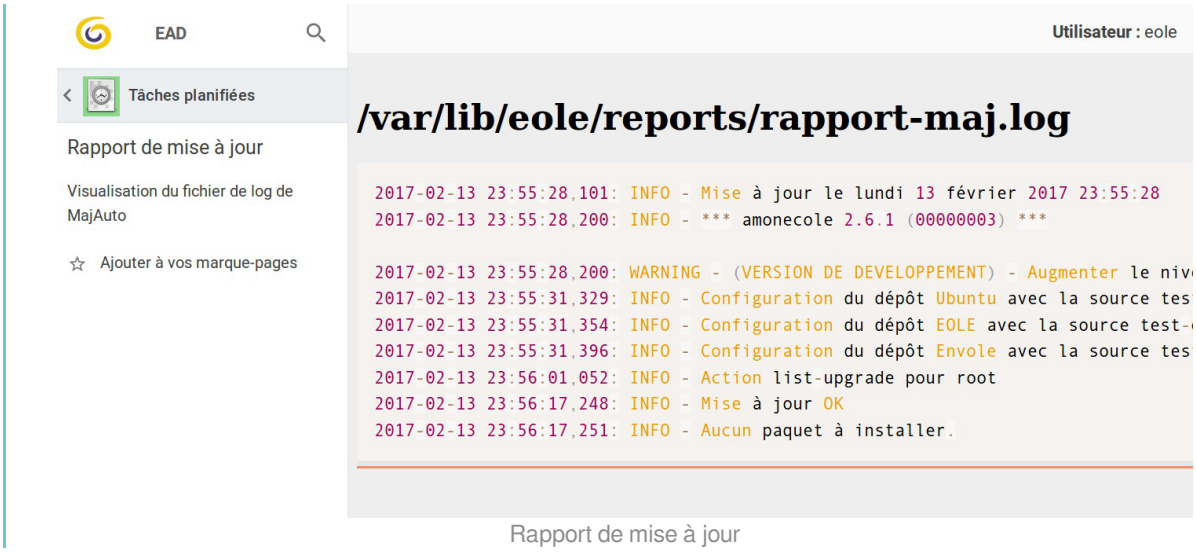
Ces variables sont des variables Creole chargée en mémoire vives, si on veut qu'elles soient enregistrées il faut renseigner l'attribut *save=True* et elles leurs nouvelles valeurs seront stockées dans un `config.eol` (qui n'est pas le `/etc/config.eol` principal de Creole).

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.

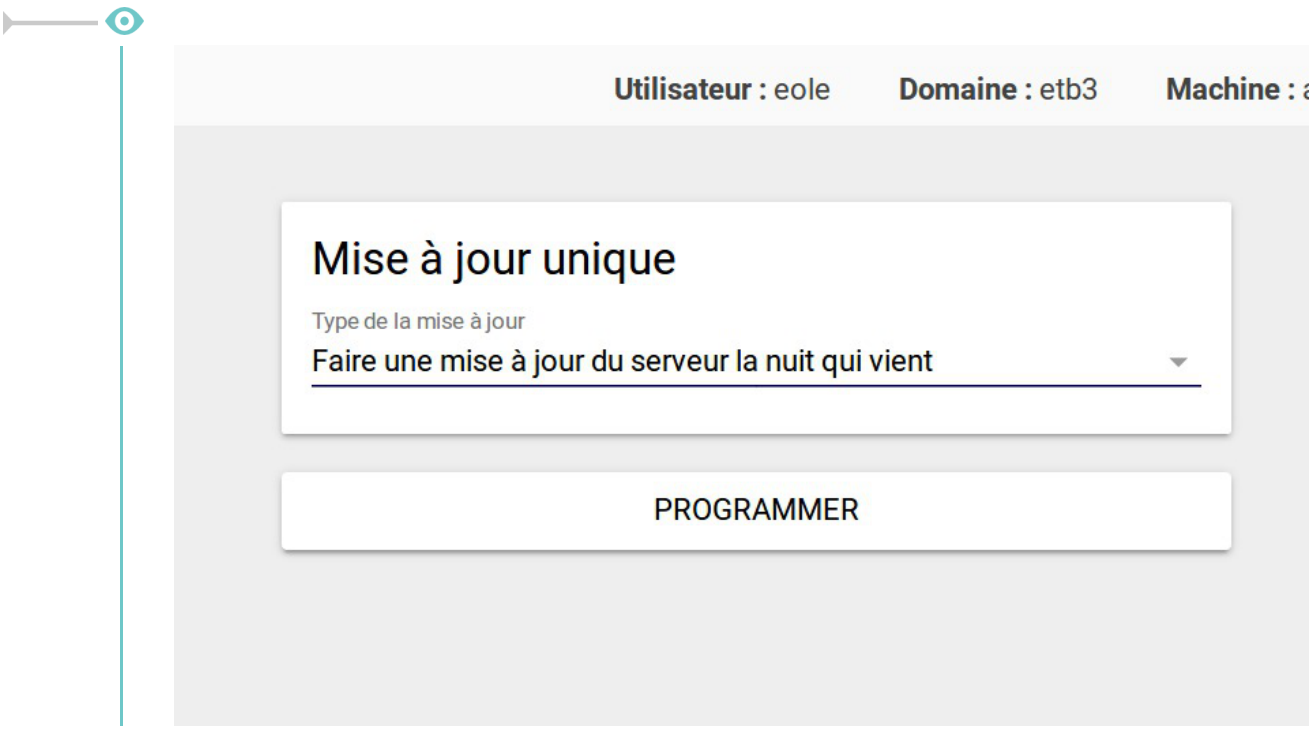
```
<variables>
    <family name='Mise à jour'>
    <variable description="Type de la mise à jour" type="string" name="typemaj">
    <value>Faire une mise à jour du serveur la nuit qui vient</value>
    </variable>
    <variable description="Choisir les options de mise à jour" type="string" name="majoption">
    <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

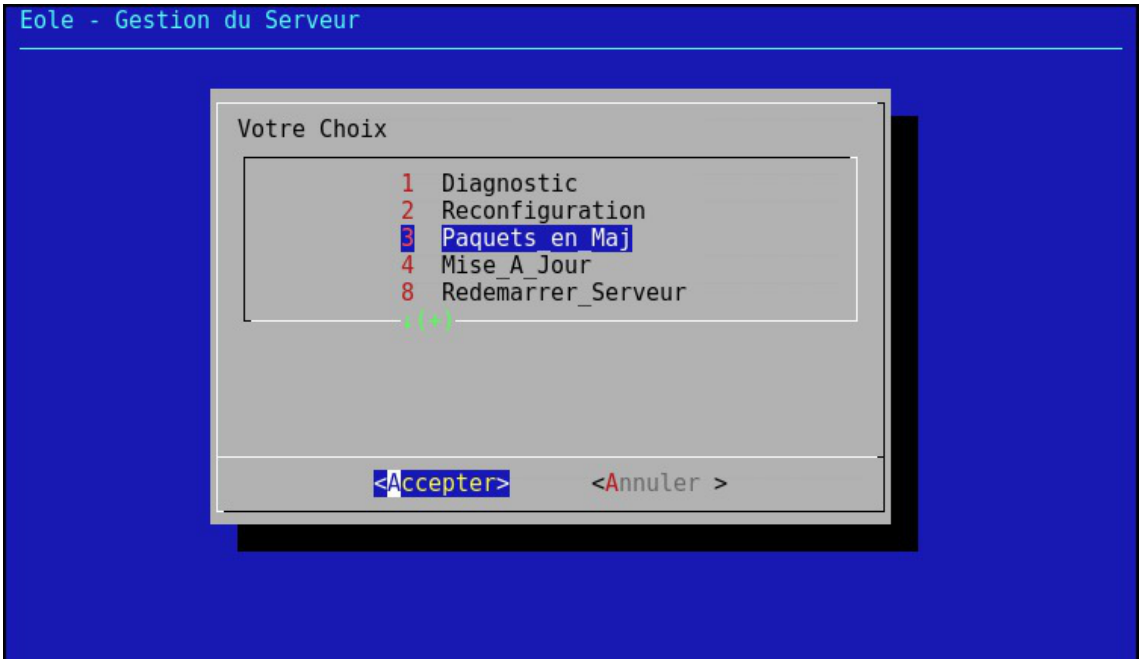
mars 01 11:31:48 scribe systemd[1]: Starting The Salt API...
mars 01 11:31:49 scribe systemd[1]: Started The Salt API.
root@scribe:~#
```

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.

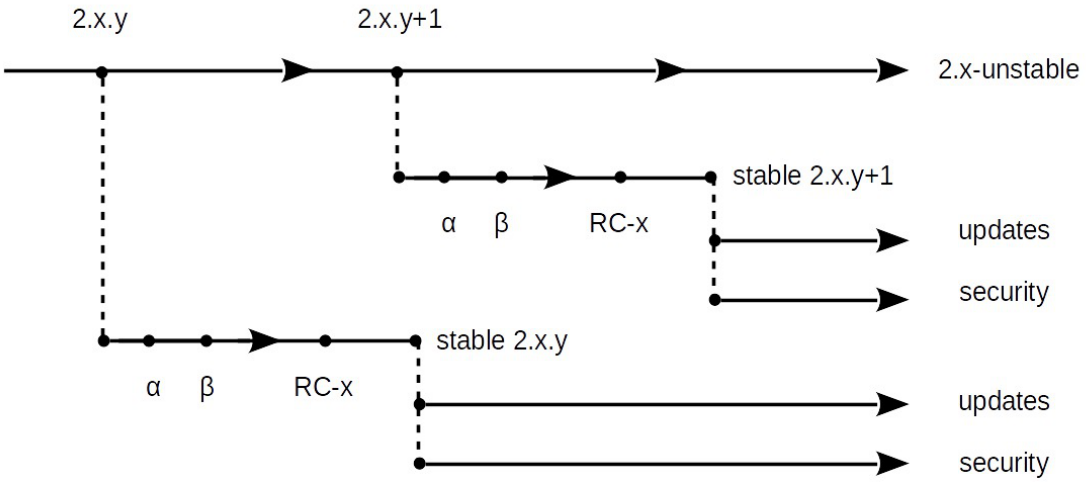
Par défaut une mise à jour hebdomadaire est configurée automatiquement à la fin de l'instanciation du module. Ce comportement est paramétrable et désactivable.

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.783] 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.690]

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.759] ;
- 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.

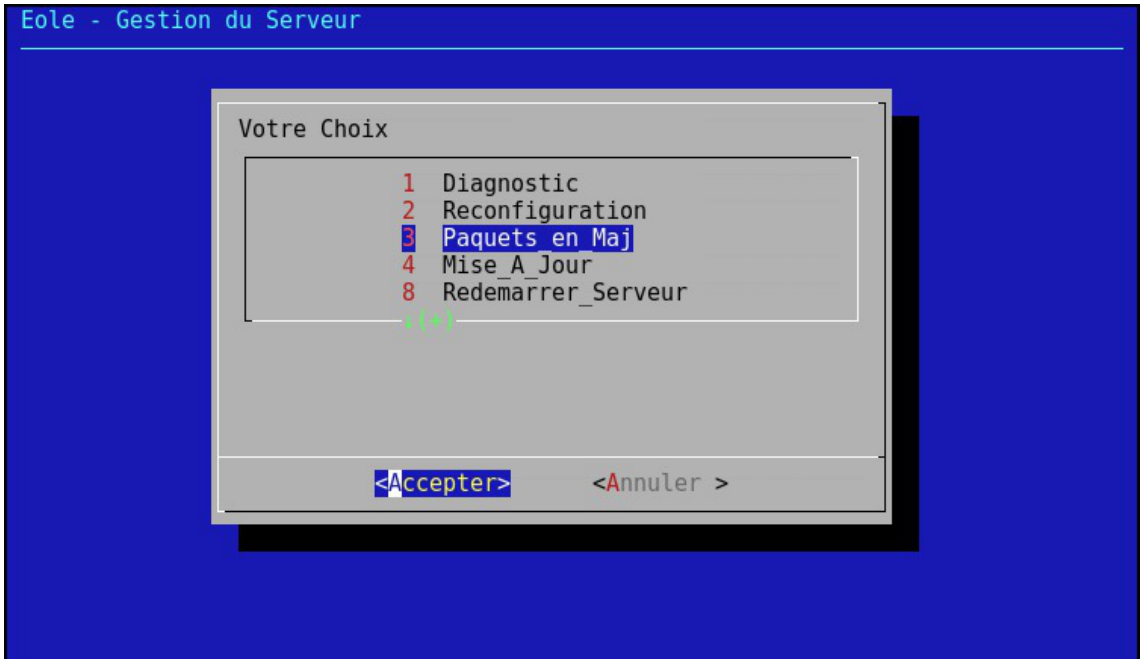
Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

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.667]

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.759].

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.690]

Reconfiguration [p.368]

Installation manuelle de paquets [p.439]

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.181]

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.384]

Gestion des tâches planifiées eole-schedule [p.667]

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.753] 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.753] 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.756] 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.435]

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.

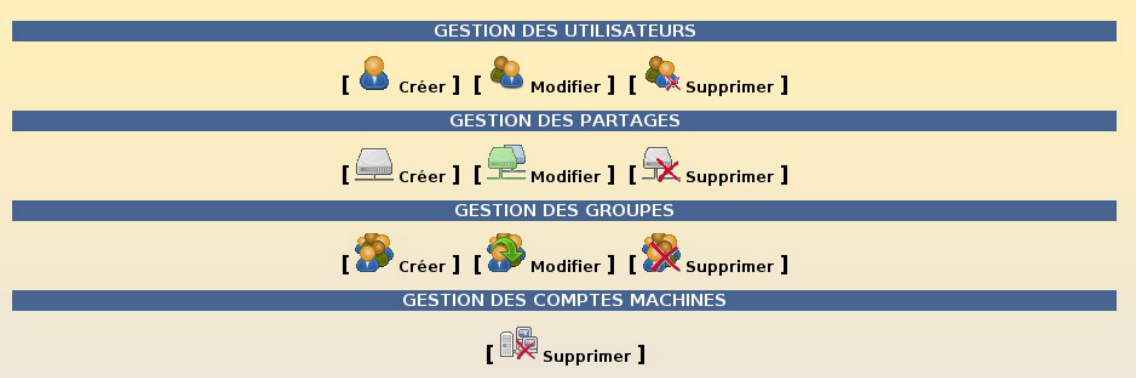
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. Fonctionnalités de l'EAD propres au module Horus

2.1. Gestion des comptes Horus

Le menu `Gestion` est dédié à la gestion des utilisateurs, des groupes, des clients et des partages du module Horus.

Index
Le sous-menu `Index` présente sur une seule page des raccourcis vers toutes les actions possibles du menu `Gestion`.



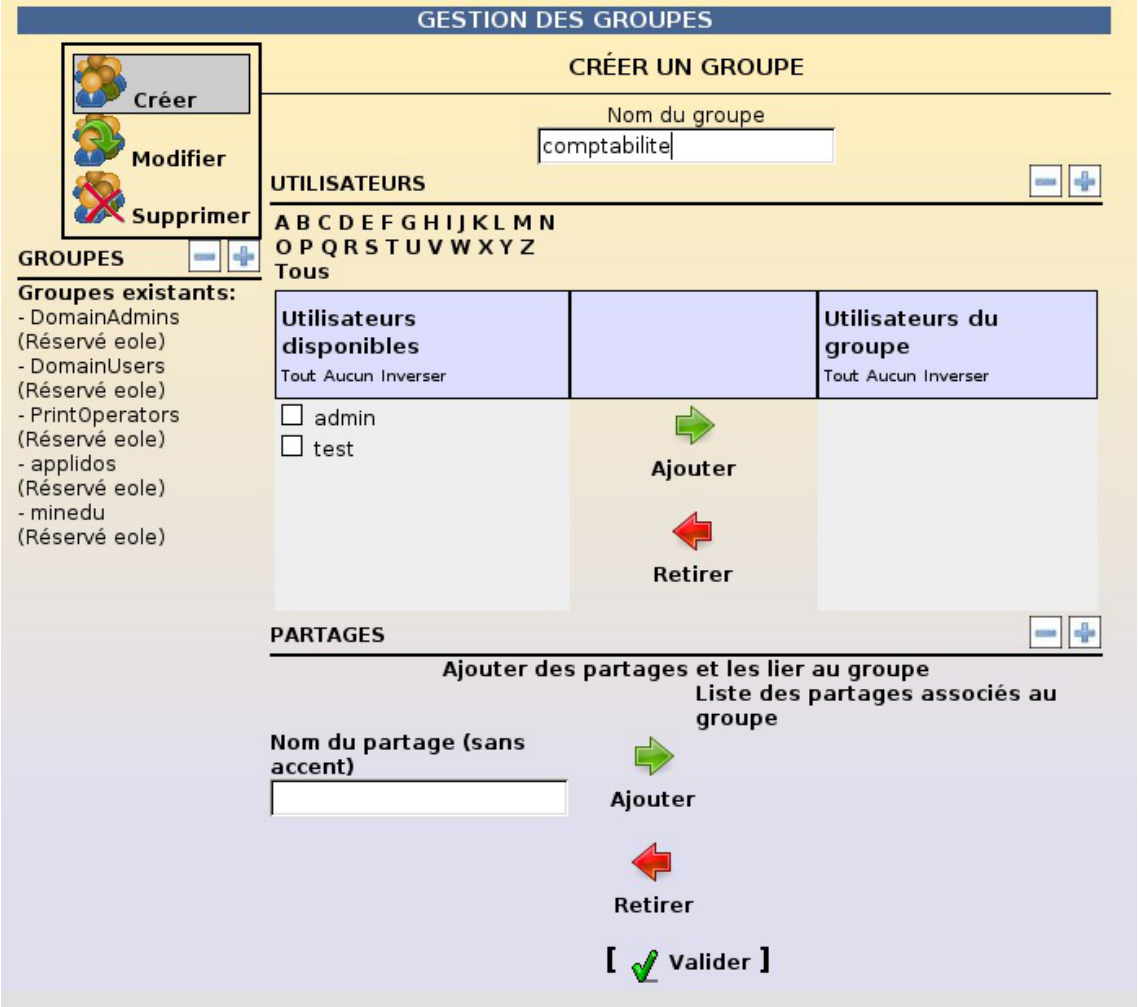
Index de Gestion

2.1.1. Gestion des groupes

Le sous-menu `Groupes` permet de créer, modifier et supprimer les groupes d'utilisateurs Horus.

Créer un groupe
Le formulaire de création d'un groupe Horus est découpé en 3 blocs distincts :

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



Création d'un groupe dans l'EAD

Pour créer un groupe, seul le *Nom du groupe* est requis (premier bloc).

Il est possible d'inscrire un ou plusieurs utilisateurs existants au groupe dès sa création (deuxième bloc).

Il est enfin possible d'affecter un ou plusieurs nouveaux partages au groupe dès sa création (troisième bloc).

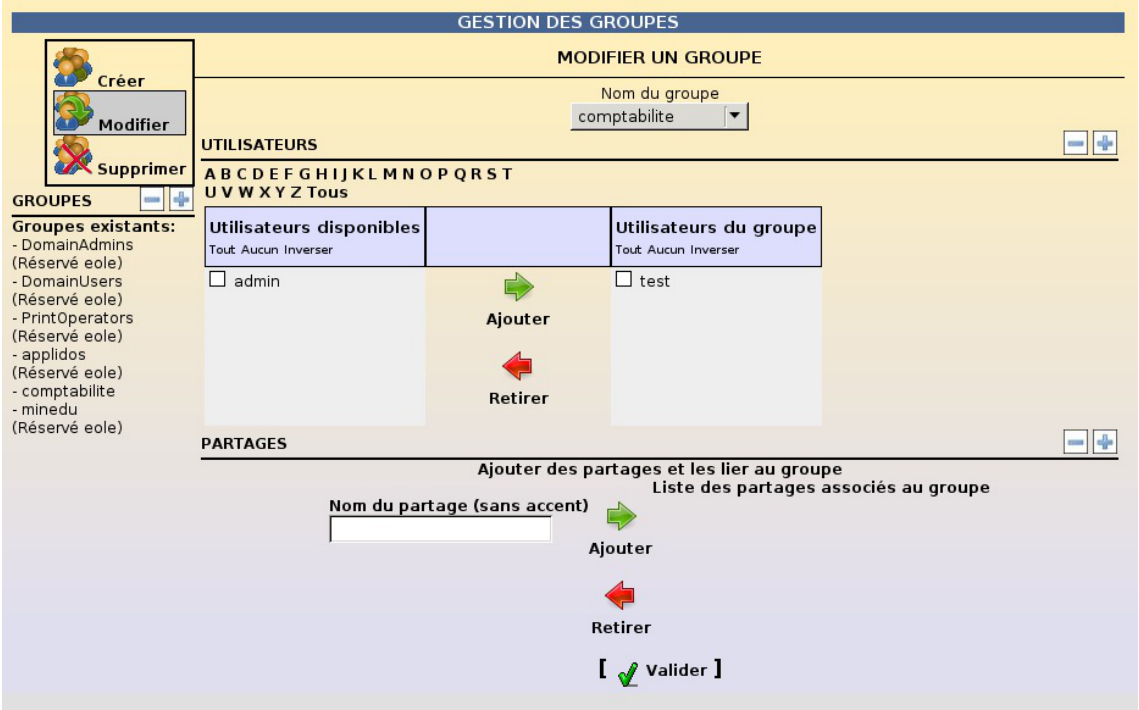
Modifier un groupe

Une liste déroulante permet de sélectionner le groupe à éditer.

Une fois le groupe choisi, deux blocs similaires à ceux du formulaire de création de groupe apparaissent.

Ils permettent respectivement d'inscrire/désinscrire des utilisateurs au groupe et d'ajouter/supprimer des partages au groupe.

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



Modification d'un groupe dans l'EAD

Les groupes suivis de la mention `(Réservé EOLE)` sont des groupes spéciaux qu'il faut manipuler avec précaution.

Le fait de supprimer la liaison entre un partage et un groupe (ou de supprimer le groupe lui-même) entraine la suppression du partage dans l'annuaire mais pas celle de ses données.

Il est donc possible de les récupérer en créant un nouveau partage du même nom (ou un partage utilisant le même chemin).

Pour ce genre de manipulation, il est préférable d'utiliser les actions du sous-menu `Partages` .

Supprimer un groupe

Une liste déroulante permet de sélectionner le groupe à supprimer.

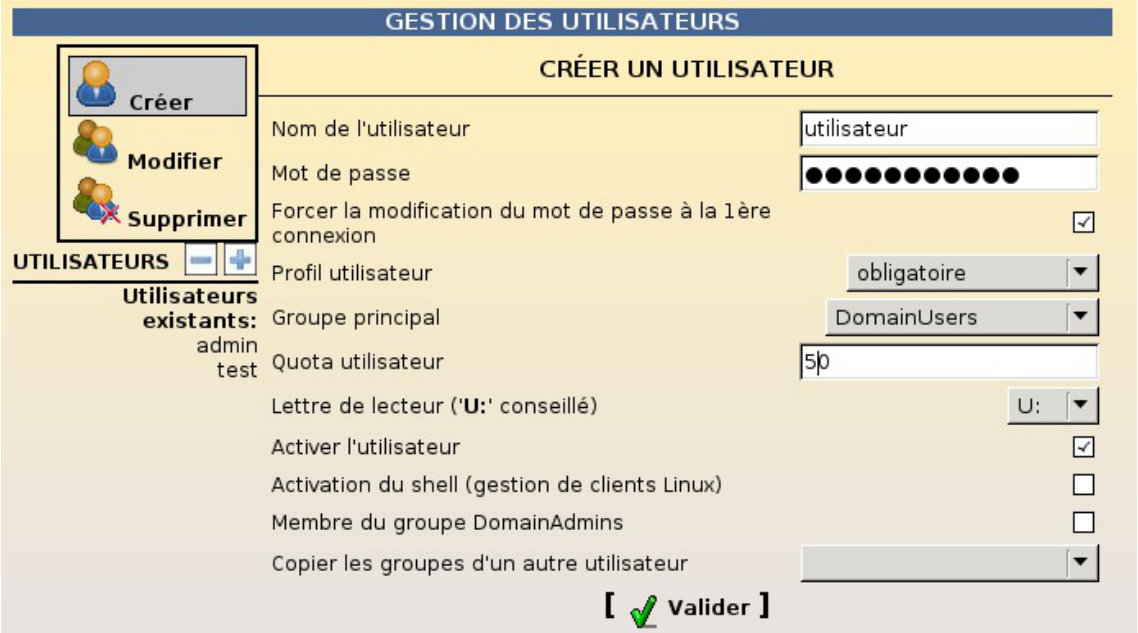
Les groupes spéciaux ne sont pas supprimables et n'apparaissent pas dans cette liste.

2.1.2. Gestion des utilisateurs

Le sous-menu `Utilisateurs` permet de créer, modifier et supprimer les utilisateurs Horus.

Le formulaire de création d'utilisateur Horus est assez simple.

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



Création d'un utilisateur dans l'EAD d'Horus

Pour créer un utilisateur, le *Nom de l'utilisateur* (login) et son *Mot de passe* sont requis.

Il est également possible de préciser :

- si l'utilisateur doit changer son mot de passe lors de sa première connexion Samba ;
- le profil Windows affecté à l'utilisateur ;
- le groupe principal de l'utilisateur ;
- un quota disque à affecter à l'utilisateur (en Mo) ;
- la lettre de lecteur utilisée pour monter son répertoire personnel ;
- si le compte utilisateur est activé ;
- si l'utilisateur dispose d'un shell Linux (nécessaire pour l'utilisation de clients GNU/Linux) ;
- si l'utilisateur est membre du groupe *DomainAdmins.*

La dernière option permet de récupérer la liste des groupes d'un autre utilisateur afin d'y inscrire le nouvel utilisateur (très pratique lors de la création de plusieurs utilisateurs à la chaîne).

DomainAdmins

Il est fortement **déconseillé** d'inscrire les utilisateurs au groupe *DomainAdmins*.

Cela leur donnera un accès en lecture et en écriture sur tous les partages y compris les répertoires personnels de tous les utilisateurs (*admin* inclus).

Modifier un utilisateur

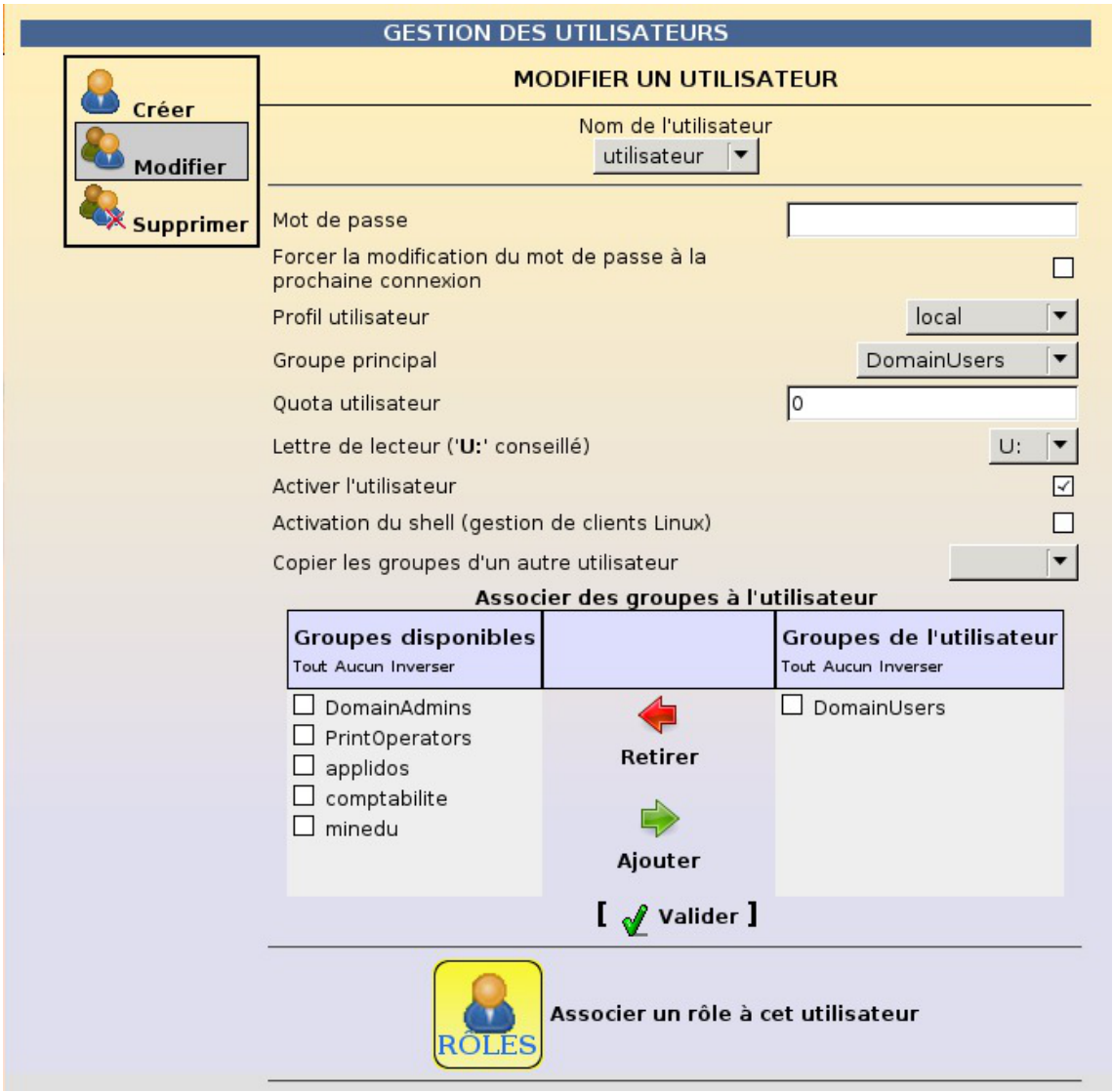
Une liste déroulante permet de sélectionner l'utilisateur à éditer.

Une fois l'utilisateur choisi, trois blocs apparaissent.

Ils permettent respectivement :

- de modifier les paramètres spécifiques à l'utilisateur ;
- d'inscrire/désinscrire l'utilisateur à des groupes ;
- d'associer un rôle EAD à l'utilisateur (également possible *via* le menu `Édition de rôles`).

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



Modification d'un utilisateur dans l'EAD d'Horus

Les paramètres utilisateurs modifiables sont :

- le mot de passe de l'utilisateur ;
- forcer l'utilisateur à changer son mot de passe lors de sa prochaine connexion Samba ;
- le profil Windows affecté à l'utilisateur ;
- le groupe principal de l'utilisateur (à utiliser avec précaution) ;
- le quota disque affecté à l'utilisateur (en Mo, mettre 0 pour ne pas avoir de limite) ;
- la lettre de lecteur utilisée pour monter son répertoire personnel ;
- l'activation/la désactivation du compte utilisateur ;
- l'activation/la désactivation du shell Linux pour l'utilisateur (nécessaire pour l'utilisation de clients Linux) ;
- l'inscription de l'utilisateur aux groupes d'un autre utilisateur.

Supprimer un utilisateur

Une liste déroulante permet de sélectionner l'utilisateur à supprimer.

Vous pouvez choisir de conserver ou de supprimer le répertoire personnel (fichiers et répertoires) de l'utilisateur.

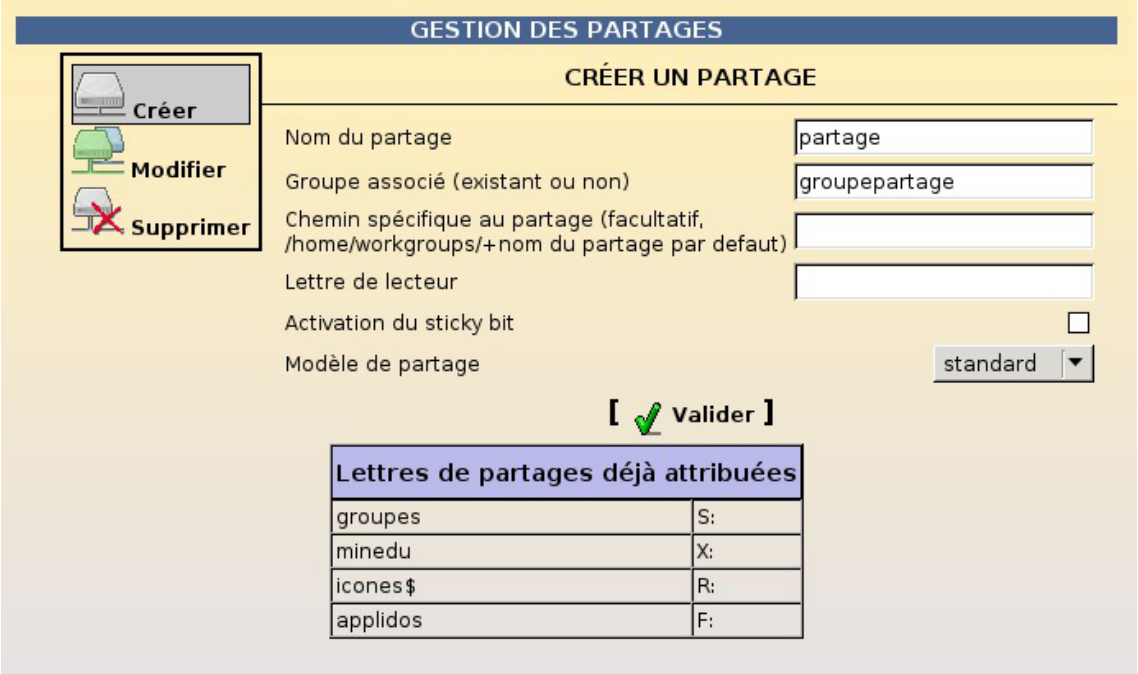
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.1.3. Gestion des partages

Le sous-menu `Partages` permet de créer, modifier et supprimer les partages Horus.

Créer un partage

Le formulaire de création de partage est composé du formulaire lui-même et d'un tableau récapitulant les lettres de lecteurs déjà réservées pour d'autres partages.



Création d'un partage dans l'EAD d'Horus

Pour créer un partage, seuls les *Nom du partage* et nom du *Groupe associé* sont requis.

Si le groupe associé au partage n'existe pas, il sera créé avec les paramètres par défaut.

Il est également possible de préciser :

- le chemin du partage sur le serveur Horus (par défaut : `/home/workgroups/<partage>`) ;
- une lettre de lecteur à associer à ce partage (exemple : `L :`) ;
- si le *sticky bit* doit être activé sur le partage (seul le propriétaire du fichier pourra effacer ces fichiers) ;
- le modèle de partage à utiliser pour générer la section associée au partage dans la configuration Samba.

activation du sticky bit

Le "sticky bit" était nécessaire au fonctionnement de certaines applications mais il ne devrait plus être utilisé.

Les modèles de partage

Le fichier de configuration Samba (`/etc/samba/smb.conf`) est généré à partir des informations

contenues dans l'annuaire.

Par défaut, les partages utilisent le template Python : `/usr/share/eole/fichier/models/standard.tmpl`

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

> Si vous souhaitez personnaliser certains partages (exemple : activer le *mode invité* sur un partage), il est possible de créer de nouveaux *templates* de partage dans ce même répertoire.
>
> Les modèles créés apparaissent alors dans l'EAD et il devient possible de les affecter à un ou plusieurs partages.

Modifier un partage

Une liste déroulante permet de sélectionner le partage à éditer.

Une fois le partage choisi, il est possible de modifier :

- la lettre de lecteur associée au partage ;
- le modèle de partage à utiliser.

Supprimer un partage

Une liste déroulante permet de sélectionner le partage à supprimer.

Les partages spéciaux ne sont pas supprimables et n'apparaissent pas dans cette liste.



Supprimer un partage dans l'EAD d'Horus

Vous pouvez choisir de conserver ou de supprimer les données (répertoire) du partage .

Voir aussi...

> Onglet Samba : Configuration du contrôleur de domaine [p.98]

2.1.4. Suppression des comptes de machine

Le sous-menu `Machines` permet de consulter la liste des stations Windows enregistrées dans l'annuaire et, si nécessaire, de supprimer l'un de ces comptes de machine.

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



Supprimer une machine dans l'EAD d'Horus

La ré-inscription d'une station dans le domaine (formatage et réinstallation d'une machine avec un nom identique) peut parfois renvoyer une erreur.

La suppression du compte de la station peut aider à résoudre le problème.

2.2. Gestion fine des groupes et des utilisateurs : ACL

Des ACLs[p.752] sont utilisées sur le système de fichiers pour permettre un réglage fin des droits d'accès aux partages et à leur contenu.

Modification des ACLs sous Windows

Avec un utilisateur ayant les privilèges nécessaires, depuis un poste client Windows, clic droit sur le `fichier/dossier => Propriétés => Sécurité` ;

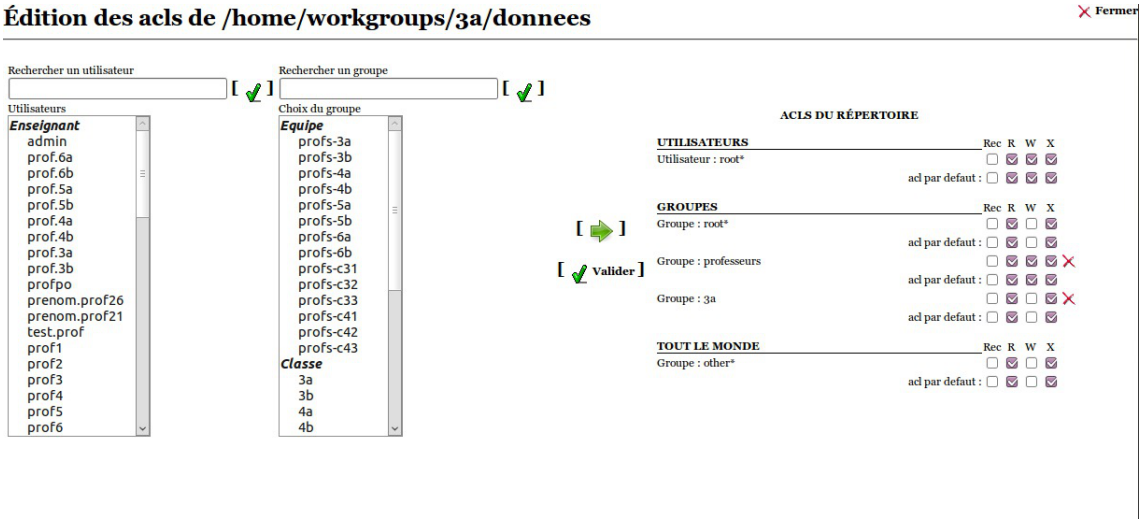
Modification des ACLs dans l'EAD

Le menu `Outils/Gestion des Acls` permet de modifier les ACLs[p.752] (droits étendus) sur les partages créés dans `/home/workgroups`.

Cette dernière méthode est la seule permettant de modifier les droits sur la racine d'un partage.

Il est possible de changer les droits sur des fichiers et des répertoires cachés.

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



Interface de gestion des ACLs

Dans la partie `ACLS DU RÉPERTOIRE` du formulaire :

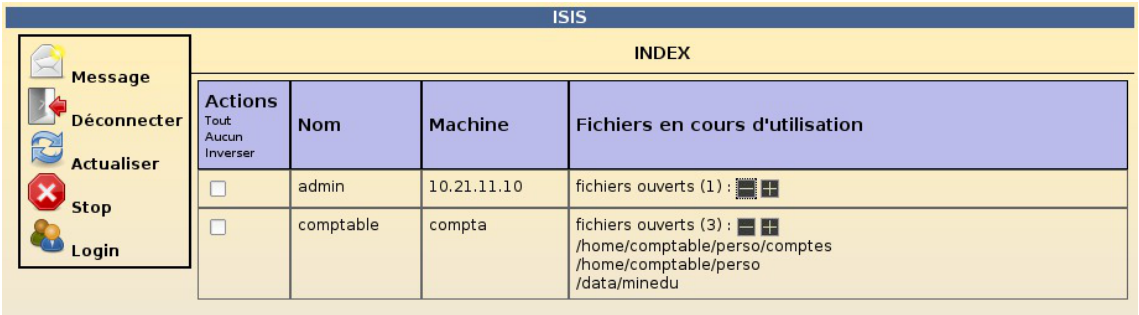
- l'étoile "*" indique que l'utilisateur ou le groupe en question est propriétaire du fichier ou du répertoire au niveau des droits Unix ;
- la case à cocher *Rec* permet d'appliquer la modification de façon récursive ;

  Cette case est toujours décochée au chargement et rechargement du formulaire : elle n'indique pas un état mais sert à utiliser l'option `-R` dans les commandes `setfacl` sur le serveur. Il faut donc la cocher à chaque fois qu'on désire appliquer un changement récursivement.
- la ligne *acl par défaut* seront les ACLs appliquées par défaut lors de la création d'un fichier ou d'un répertoire.

La levé d'une autorisation (suppression d'un droit : lecture, écriture, exécution) est toujours récursive.

2.3. Gestion des connexions

Le sous-menu `Connexion` permet de lister les utilisateurs connectés, les fichiers ou dossiers ouverts, d'écrire à ces utilisateurs, de les déconnecter et de gérer l'activation/la désactivation des comptes.

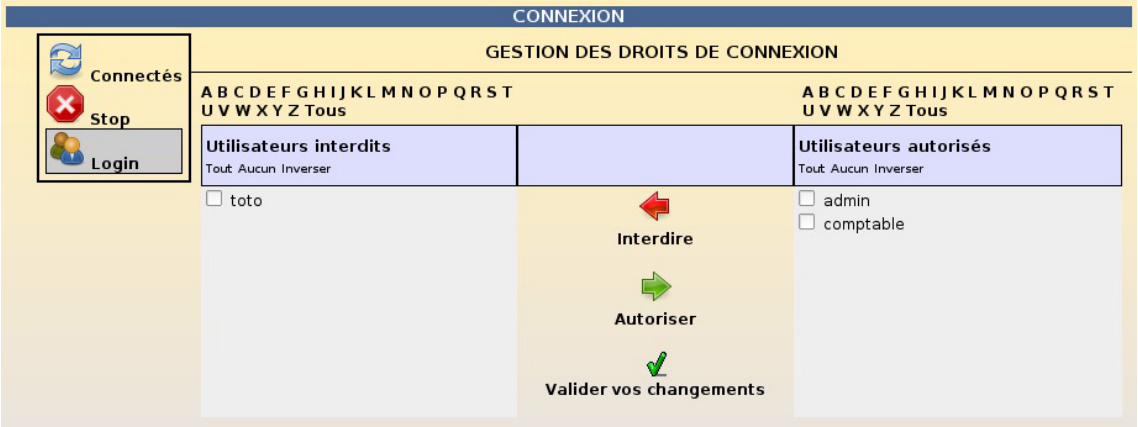


Affichage des utilisateurs connectés

- le bouton `Message` permet de rédiger un message de type *Winpopup* à envoyer aux utilisateurs sélectionnés ;

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

- le bouton `Déconnecter` permet de déconnecter et désactiver les comptes des utilisateurs sélectionnés ;
- le bouton `Actualiser` met à jour la liste des connectés et de leurs fichiers ;
- le bouton `Stop` permet de déconnecter et désactiver tous les comptes ;
- le bouton `Login` permet d'accéder au formulaire de gestion de l'activation des comptes. La fenêtre suivante s'ouvre :



Activation/Désactivation des comptes

Le formulaire de gestion de l'activation des comptes permet de gérer l'activation/la désactivation des comptes utilisateurs d'une manière globale.

Les boutons `Connectés` et `Stop` permettent d'accéder aux actions décrites précédemment.

2.4. Visualisation des quotas disque dans l'EAD

Fonctionnement des quotas disque

Il est possible, pour chaque utilisateur, de limiter la quantité de données qu'il peut stocker sur le serveur en lui imposant un quota disque maximum.

Les quotas sont composés d'une limite douce (soft) et d'une limite dure (hard).

Les règles suivantes s'appliquent à l'utilisateur :

- il ne peut pas dépasser la limite dure ;
- il peut dépasser la limite douce pendant 7 jours ;
- passé ce délai, seule la limite douce est prise en compte et il est obligé de supprimer des données afin de repasser en dessous de celle-ci ;
- à partir de là, le processus de la limite douce/dure reprend et l'utilisateur peut à nouveau dépasser la limite douce pour une durée maximale de 7 jours.

Dans l'EAD, c'est la limite douce qui est indiquée.

Sur les modules Scribe et Horus, la limite dure vaut le double de la limite douce.

Les quotas sur le module Horus

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

Le sous-menu `Quotas disque` permet de connaître l'espace disque utilisé par chaque utilisateur et de repérer les éventuels dépassements de quotas disque alloués.



Le tableau indique, pour chaque utilisateur du domaine, le rapport entre l'espace disque utilisé et l'espace disponible.

La colonne de droite précise le délai accordé aux utilisateurs dépassant le quota pour purger leurs fichiers.

Désynchronisation des quotas disque

Il peut arriver qu'il y ait une désynchronisation entre l'utilisation réelle du disque et le système de vérification des quotas.

Cela se traduit généralement par le fait que des utilisateurs sont considérés à tort comme dépassant leur quota disque.

La commande `quotacheck` permet de corriger le problème. Son utilisation demande quelques précautions.

Exemple d'utilisation de quotacheck sur le module Scribe où `/home` est la partition utilisée pour les données et les quotas utilisateurs.

1. arrêter les différents services susceptibles d'écrire sur la partition (samba, proftpd, exim4, ...) ;
2. démonter les éventuels montages liés à cette partition (images ISO, ...) ;
3. désactiver les quotas sur la partition : `quotaoff /home` ;
4. lancer la vérification des quotas : `quotacheck -vug /home` ;
5. réactiver les quotas sur la partition : `quotaon /home` ;
6. remonter les partitions : `mount -a` ;
7. démarrer les services précédemment arrêtés.

Cette procédure est également à appliquer dans le cas où la commande `repquota -a` ne rend plus la main.

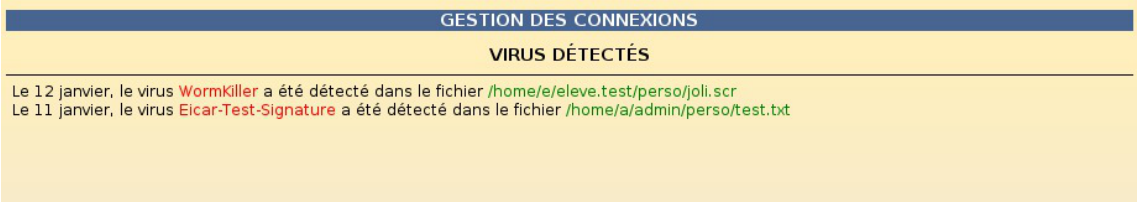
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.5. Observation des virus

Le menu Outils/Détection de virus de l'EAD permet de consulter les fichiers infectés détectés et mis en quarantaine par le serveur.

Il s'agit uniquement de fichiers qui ont été copiés dans l'un des répertoires partagés du serveur.

Chaque ligne indique la date, le nom du virus et le chemin du fichier infecté.



Affichage des virus détectés dans l'EAD

Lorsqu'un virus est détecté, il est renommé avec le préfixe `.virus:` et devient masqué pour l'utilisateur.

L'antivirus protège aussi le serveur de messagerie. Il ne protège par contre pas les stations.

Il est plus prudent, voire indispensable, suivant le système d'exploitation d'installer un anti-virus sur les stations clientes.

La détection des virus n'a lieu que si le module es configuré de la façon suivante :

- onglet Services : `Activer l'anti-virus ClamAV` à `oui`
- onglet Clamav : `Activer l'anti-virus temps réel sur SMB` à `oui`

2.6. Scripts administratifs

Le sous-menu Scripts administratifs permet de lancer l'exécution des scripts de pre/post installation pour les applications nationales.

Ces scripts sont fournis à l'équipe EOLE par le Pôle Ingénierie, Hébergement National et Expertise Technique de Paris, anciennement CAPTI (adresse à usage académique : http://pole.in.ac-paris.fr).



Exécution de scripts administratifs dans l'EAD

Le formulaire d'*Exécution de scripts administratifs* présente la dernière version de chaque script sous la forme d'une liste déroulante.

Une fois l'application nationale installée sur Horus, il suffit de choisir le script de post-installation associé et de cliquer sur le bouton Exécuter.

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

Il est possible d'ajouter un script en respectant les règles suivantes :

- le fichier doit être placé dans le répertoire : `/usr/share/minedu/scripts`
- il doit être exécutable et posséder l'extension *.sh*
- il doit contenir une ligne de commentaire spéciale débutant par `#MENU=`

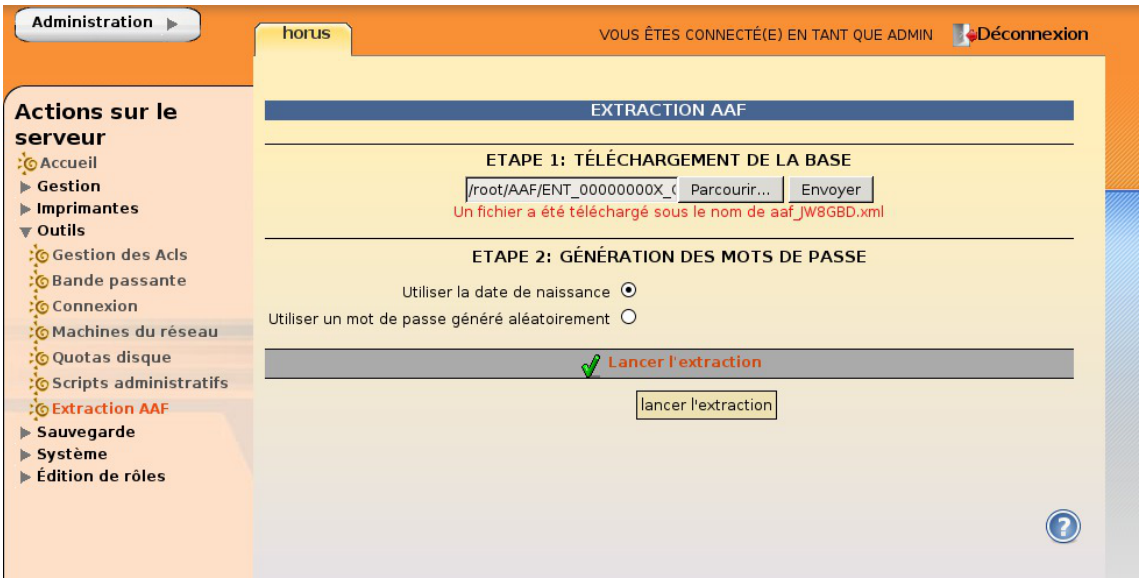
2.7. Extraction AAF

Le sous-menu `Extraction AAF` permet de créer des comptes pour les personnels administratifs de l'établissement à partir d'informations extraites de l'annuaire fédérateur (AAF).

Le fichier XML des personnels doit être fourni par l'Académie.

Le nom de ce fichier est traditionnellement de la forme :

`ENT_<rne_etablissement>_Complet_<date>_PersEducNat_0000.xml`



N'oubliez pas de cliquer sur le bouton `Envoyer` pour que votre fichier soit bien téléchargé.

Le bouton `Lancer l'extraction` permet de lancer les traitements.

Pour chaque personnel administratif défini dans le fichier extrait d'AAF, un compte de la forme "prenom.nom" sera créé.

Par défaut les utilisateurs seront inscrits à un groupe correspondant à leur fonction au sein de l'établissement (direction, assistant,...).

Dans la version actuelle du programme, les mots de passe attribués aux nouveaux utilisateurs sont stockés dans le fichier `/tmp/passwords.csv` .

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

2.8. Réservation d'adresse IP dans l'EAD

Si le service DHCP est activé sur le module EOLE, il est possible de fixer les adresses de certaines machines via l'EAD.

L'action dhcp apparaît dans le menu Outils/DHCP statique de l'EAD.



Réservation d'adresse dans l'EAD

Pour associer un nom et une adresse IP à une machine, il faut connaître son adresse MAC.

Pour faciliter les enregistrements, les informations sur les stations déjà connues du serveur DHCP sont directement réutilisables.

Pour cela, il suffit de sélectionner la machine souhaitée au niveau de la liste déroulante Baux en cours.

3. Gestion des utilisateurs sur le module Horus

L'outil Frontend Horus est composé d'un serveur installée sur le module Horus et d'une interface graphique GTK[p.764] permettant de gérer facilement les utilisateurs, les groupes et les partages sur le module.

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



L'outil Frontend Horus

Utilisateurs autorisés

Les utilisateurs autorisés à utiliser l'outil Frontend Horus sont :

- l'utilisateur `admin`
- les autres utilisateurs LDAP dans la mesure où une délégation de droit leur a été attribué.

Principales fonctionnalités

- création/modification/suppression d'utilisateur ;
- délégation de droits sur les membres d'un groupe ;
- importation d'utilisateurs en masse (Fichier/Import d'utilisateurs) ;
- création/modification/suppression de groupe et de partage.

Format du fichier d'importation d'utilisateurs

Le fichier d'importation doit être au format CSV[p.758] avec séparateur point-virgule et comporter les champs suivants :

- login
- groupes (séparés par des virgules)
- lettre de lecteur
- mot de passe

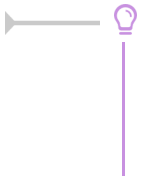
Exemple : `toto;minedu,applidos;U;pass`

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

Le serveur sur le module

La partie serveur est installée sur le module Horus mais doit être activé.

Son activation est possible via l'interface de configuration du module, dans l'onglet `Services`, passer `Activation du service horus_frontend` à `oui`.



Le client et le serveur utilisent le port 7080 pour communiquer.

L'état d'activation du serveur associé à l'outil Frontend Horus est disponible par la commande `diagnose`.

Le client Frontend Horus sur le serveur

Le client Frontend Horus est pré-installé sur le serveur Horus (paquet nommé `frontend-horus`).

Le client s'exécute à l'aide la commande : `frontend_horus`.

Le client Frontend Horus pour GNU/Linux

Le client Frontend Horus peut être installé sur une machine cliente GNU/Linux.

Ce client est téléchargeable sur le FTP du projet à l'adresse à l'adresse :

ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-ng.tar.gz

Il faut procéder au désarchivage :

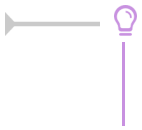
```
$ tar xvzf frontend-horus-ng.tar.gz
```

Pour exécuter le client :

```
$ cd frontend-horus
```

```
$ ./frontend.py
```


L'application requiert l'installation de `python`, `python-gtk2` et `python-glade2` sur la machine.



Des scripts python proposant des fonctionnalités équivalentes sont disponibles dans le répertoire `/usr/share/eole/backend`.

Le client Frontend Horus pour Windows

Le client Windows est téléchargeable sur le FTP du projet à l'adresse :

ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-setup.exe

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

4. Les sauvegardes

4.1. Généralités sur la sauvegarde

La sauvegarde[p.777] consiste à dupliquer des données stockées dans le Système Informatique (SI) de l'entité, dans le but de les mettre en sécurité.

Cette mise en sécurité a pour but de répondre à deux éventualités de restauration[p.776] :

- la restauration de tout ou d'une partie du SI, suite à une dégradation importante ou à une destruction ;
- la restauration de quelques fichiers, suite à une corruption ou une destruction limitée de données.

On distingue trois types de sauvegardes :

- la sauvegarde **totale** ;
- la sauvegarde **différentielle** ;
- la sauvegarde **incrémentale**.

La sauvegarde peut être :

- réalisée localement ;
- sur un média (serveur, disque, bande, CD-ROM) ;
- hébergé dans le SI (Système Informatique) à des fins de restauration rapide ;
- archivée ;
- externalisée.

4.1.1. Sauvegarde totale

Une **sauvegarde totale** ou **complète**, correspond à la copie **intégrale** d'un contenu à un instant T, sans prendre en compte l'historique.

Coûteuse en temps et en espace, cette sauvegarde reste malgré tout *la plus fiable*, puisqu'elle assure à elle seule l'*intégrité* de l'ensemble des données sauvegardées.

Il n'est pas judicieux de ne pratiquer que ce type de sauvegarde, car l'ensemble des données n'est jamais totalement modifié entre deux sauvegardes.

Il existe deux autres méthodes qui procèdent à la sauvegarde des seules données modifiées et/ou ajoutées entre deux sauvegardes totales :

- la sauvegarde incrémentale ;
- la sauvegarde différentielle.

4.1.2. Sauvegarde incrémentale

Une **sauvegarde incrémentale** réalise une copie des fichiers créés ou modifiés **depuis la dernière sauvegarde** quel que soit son type (complète, différentielle ou incrémentale).

Une sauvegarde totale est réalisée le jour T. Le jour T+1, la sauvegarde incrémentale est réalisée par

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

référence à la sauvegarde précédente, donc la sauvegarde T. Le jour T+2, la sauvegarde incrémentale est réalisée par référence à la sauvegarde précédente, à savoir T+1. Et ainsi de suite.

La restauration d'un système complet à un jour donné (par ex : au jour T+3) se fait en appliquant la dernière sauvegarde complète (jour T), ainsi que toutes les sauvegardes incrémentales jusqu'au jour cible, à savoir T+1, T+2 et T+3.

Lorsqu'il s'agit de la restauration d'un fichier ou d'un répertoire qui a été sauvegardé à la date T+3 (T étant le jour de la sauvegarde totale de référence), seule la sauvegarde incrémentale du jour T+3 est nécessaire.

4.1.3. Sauvegarde différentielle

Une **sauvegarde différentielle** réalise une copie des fichiers crées ou modifiés, en se basant sur les différences constatées avec la **dernière sauvegarde totale** (quelles que soient les sauvegardes intermédiaires).



La notion de sauvegarde différentielle peut varier suivant la solution de sauvegarde utilisée.

Cette présentation est fidèle à l'outil de sauvegarde choisi par EOLE.

4.1.4. Des outils de sauvegarde

Les systèmes GNU/Linux embarquent depuis toujours des outils unitaires d'archivage qui permettent de réaliser des embryons de stratégie de sauvegarde.

Ainsi des outils tels que la commande `tar` permettent de créer des archives sur des médias locaux (disques, ou lecteurs de bandes).

Via des scripts se basant sur les dates de modifications, il est possible d'implémenter les méthodes de sauvegarde détaillées dans les paragraphes précédents.

Des outils plus complexes, et souvent propriétaires, ont été développés depuis, pour faciliter la création de ces sauvegardes (gestion du contenu à sauvegarder), mais aussi pour faciliter la gestion du calendrier de sauvegarde (programmation des tâches et des successions de sauvegardes).

Enfin, la plupart de ces outils intègrent la gestion de la restauration, avec la possibilité de choisir la date cible à restaurer.

Les solutions logicielles les plus connus sont :

- **Tivoli Storage Manager** (TSM) - IBM
  - http://www-306.ibm.com/software/tivoli/products/storage-mgr/
- **Time Navigator** - Atempo
  - http://fr.atempo.com/products/timeNavigator/default.asp
- **Networker** - EMC/Legato
  - http://france.emc.com/products/detail/software/networker.htm
- **ARCserve Backup** - Computer Associate
  - http://www.ca.com/us/data-loss-prevention.aspx
- **Arkeia Network Backup** - Arkeia

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

- http://www.arkeia.com/products/arkeianetworkbackup/index.php
- **Bacula** - Bacula
  - http://bacula.org
- **Bareos** - Bareos
  - http://www.bareos.org

4.2. La sauvegarde EOLE

EOLE 2.5 utilise l'outil de sauvegarde libre **Bareos**.

Backup **A**rchiving **RE**covery **O**pen **S**ourced est un dérivé (fork) de l'outil de sauvegarde Bacula : http://www.bareos.org

Bareos permet de sauvegarder :

- des fichiers et des dossiers
- les droits POSIX[p.775]
- les ACLs[p.752]

Bareos permet de **sauvegarder** des données (indifféremment sur des disques locaux ou distants, des bandes magnétiques), de gérer un **nombre important** et **non limité de clients**, et évidemment de **restaurer** facilement les sauvegardes.

Bareos supporte, entre autres, la possibilité de faire des sauvegardes sur plusieurs unités de stockage si une première unité possède une capacité insuffisante.

4.2.1. Le vocabulaire Bareos

Bareos utilise un nombre important de ressources pour définir une sauvegarde.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-60001.3

Quelques définitions

Job

L'objet le plus élevé est la définition d'un **Job**, représentant une "sauvegarde" au sens Bareos du terme.

Un Job Bareos est une ressource de configuration qui définit le travail que Bareos doit effectuer pour sauvegarder ou restaurer un client particulier. Un Job consiste en l'association d'un type d'opération à effectuer (**Type** : backup, restore, verify, etc.), d'un niveau de sauvegarde (**Level** : Full, Incremental, ...), de la définition d'un ensemble de fichiers et répertoires à sauvegarder (**FileSet**), et d'un lieu de stockage où écrire les fichiers (**Storage**, **Pool**).

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-990008.2

Schedule

Un Job peut être immédiat, mais dans une stratégie de sauvegarde, il est généralement planifié via la ressource **Schedule**.

Le schedule détermine la date et l'instant où le job doit être lancé automatiquement, et le niveau (total, différentiel, incrémental...) du job en question.

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

Cette directive est optionnelle. Si elle est omise, le job ne pourra être exécuté que manuellement via la Console.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1010008.4

Volume

Un **Volume** est une unité d'archivage, usuellement une cartouche ou un fichier nommé sur disque où Bareos stocke les données pour un ou plusieurs **jobs** de sauvegarde. Tous les volumes Bareos ont un **label** unique (logiciel) écrit sur le volume par Bareos afin qu'il puisse être assuré de lire le bon volume. En principe, il ne devrait pas y avoir de confusion avec des fichiers disques, mais avec des cartouches, le risque d'erreur est plus important.

Les volumes ont certaines propriétés comme la durée de rétention des données et la possibilité d'être recyclés une fois cette durée de rétention expirée; ceci afin d'éviter de voir grossir indéfiniment l'espace disque occupé par les sauvegardes.

Pool

La ressource **Pool** définit l'ensemble des **Volumes** de stockage (cartouches ou fichiers) à la disposition de Bareos pour écrire les données. En configurant différents Pools, vous pouvez déterminer quel ensemble de volumes (ou média) reçoit les données sauvegardées.

Ceci permet, par exemple, de stocker les sauvegardes totales sur un ensemble de volumes, et les sauvegardes différentielles et incrémentales sur un autre. De même, vous pouvez assigner un ensemble de volumes à chaque machine sauvegardée.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1130008.8

FileSet

Un **FileSet** est une ressource qui définit **les fichiers à inclure dans une sauvegarde**. Il consiste en une liste de fichiers ou répertoires inclus, une liste de fichiers ou répertoires exclus et la façon dont les fichiers seront stockés (compression, chiffrement, signatures).

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1030008.5

Storage

Cette ressource définit les services de stockage que peut contacter le directeur. On y retrouve les répertoires de travail du processus, le nombre de Jobs concurrents qu'il est capable de traiter, et éventuellement, la définition des adresses IP des clients dont il accepte les connexions. Chaque **Job** est associé à une ressource **Storage**. Une ressource **Storage** peut être associée à plusieurs **Jobs**.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1120008.7

Device

Véritable destination physique de la sauvegarde, la ressource **Device** fait le lien entre le matériel de sauvegarde (lecteur de bandes, robots de sauvegarde, mais aussi disques locaux - internes comme externes) et la ressource **Storage**.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1250009.4

Catalog

La ressource Catalog précise quel catalogue utiliser pour le job courant. Actuellement, Bareos ne peut utiliser qu'un type de serveur de base de données défini lors de sa configuration : SQLite, MySQL,

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

PostgreSQL. En revanche, vous pouvez utiliser autant de catalogues que vous le souhaitez. Par exemple, vous pouvez avoir un catalogue par client, ou encore un catalogue pour les sauvegardes, un autre pour les jobs de type Verify et un troisième pour les restaurations.

Le catalogue (ressource **Catalog**) est une base de données utilisée pour stocker :

- des informations sur les fichiers: la liste, les permissions, l'emplacement sur les volumes de sauvegarde, etc.
- la définition de la configuration de Bareos.

Actuellement, trois formats de bases de données sont supportés : SQLite, MySQL et PostgreSQL.

SQLite est conseillé pour de petites installations, alors que MySQL est préférable pour les installations d'entreprise (à partir d'une dizaine de clients).

Attention, l'interface web ne fonctionne qu'avec les versions MySQL et PostgreSQL.

Le catalogue est une pièce majeure de Bareos, et doit également faire partie du plan de sauvegarde.

Ce catalogue peut rapidement devenir volumineux, il faut veiller au taux d'occupation et à la performance de la base de données.

Point important, la configuration de Bareos se fait à deux niveaux:

- les fichiers de configuration ;
- la base de données.

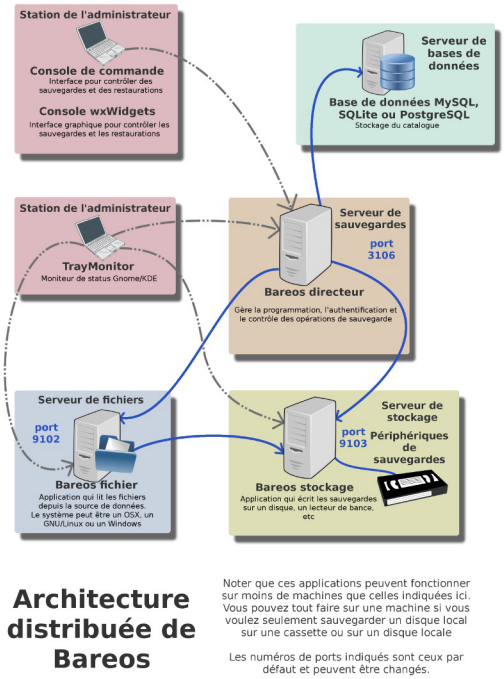
Bareos lit les fichiers de configuration au démarrage, et inscrit les valeurs dans la base de données du Catalogue. C'est le Catalogue qui définit la configuration utilisée par Bareos, donc il faut préférer le résultat des commandes console aux valeurs des fichiers.

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1150008.9

4.2.2. Architecture de Bareos

Bareos est construit suivant une **architecture distribuée** :

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



Architecture de Bareos inspiré du dessin original de Aristedes Maniatis (documentation officielle de Bacula)

- le serveur **directeur (backup server)** est l'élément central, qui supervise et archive les opérations de sauvegarde et de restauration, le nom du service sur un module EOLE est **bareos-dir** ;
- le serveur **base de données (database server)** gère le **catalogue** dans lequel le directeur archive les opérations et l'emplacement des fichiers dans les différents volumes de sauvegarde, au format SQLite ou MySQL. Il se trouve sur le même serveur que le directeur sur un module EOLE ;
- le serveur de **stockage** (**storage server)** est le serveur qui prend en charge l'écriture et la lecture des volumes de sauvegarde, le nom du service sur un module EOLE est **bareos-sd** ;
- le serveur de **lecture/écriture de fichiers (file server)** exécute les commandes de lecture/écriture des fichiers gérés par la sauvegarde sur chaque poste où il est installé, le nom du service sur un module EOLE est **bareos-fd** ;

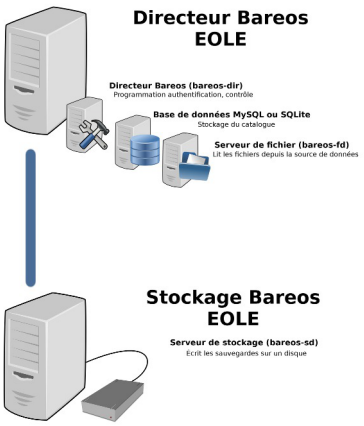
La communication entre chaque serveur est associée à un mot de passe. Ces différents serveurs peuvent être :

- installés **sur la même machine** sans problème ;
- présents **en plusieurs exemplaires** (on peut dupliquer les destinations de sauvegardes, avoir plusieurs

  directeur, etc.).

La configuration Bareos sur un module EOLE ne permet pas la séparation du serveur directeur, du serveur base de données et du serveur de fichiers.

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



Architecture de Bareos intégré à EOLE

Cette partie de la configuration est **appelée directeur** dans la suite de la documentation.

Par contre, il est possible de déporter le serveur de stockage sur un serveur disposant d'un disque de sauvegarde.

Pour résumer, 3 services liés aux sauvegardes se retrouvent sur un module EOLE :

- bareos-dir (lié à bareos-fd)
- bareos-fd (lié à bareos-dir)
- bareos-sd

Plusieurs directeurs peuvent envoyer les données sur un unique serveur de stockage en établissement.

Il est également possible de copier les sauvegardes au travers d'autres protocoles réseau : rsync, samba, SSH, *etc*.

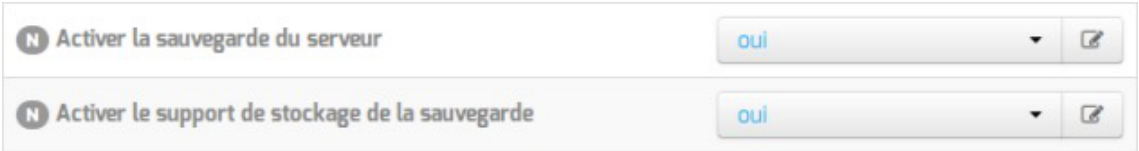
4.2.3. Configuration des sauvegardes

La configuration des sauvegardes consiste en une activation de la sauvegarde du serveur et/ou en l'activation du support de sauvegarde sur le module.

Si le support de sauvegarde est activé, un complément de configuration peut se faire soit par l'EAD soit en ligne de commande.

4.2.3.a. Activation et configuration de Bareos

La sauvegarde du serveur et le support de stockage de la sauvegarde sont activés par défaut sur certains modules, il peuvent être activés/désactivés dans l'onglet Services de l'interface de configuration du module.



Activation de la sauvegarde Bareos dans l'onglet Services de l'interface de configuration

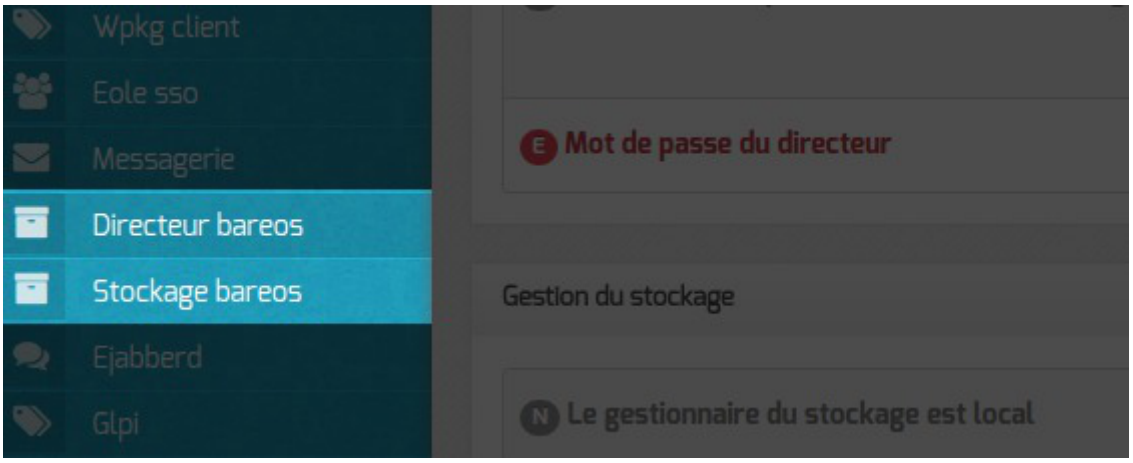
- L'activation du support de stockage de la sauvegarde permet d'accueillir des sauvegardes locales ou

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

distantes.

- L'activation de la sauvegarde permet d'activer la sauvegarde du serveur, celle-ci peut être locale si le support de stockage est activé ou déportée à condition d'avoir un serveur sur lequel est activé le support de stockage.

Cette fonctionnalité permet de mettre en place des sauvegardes croisées.

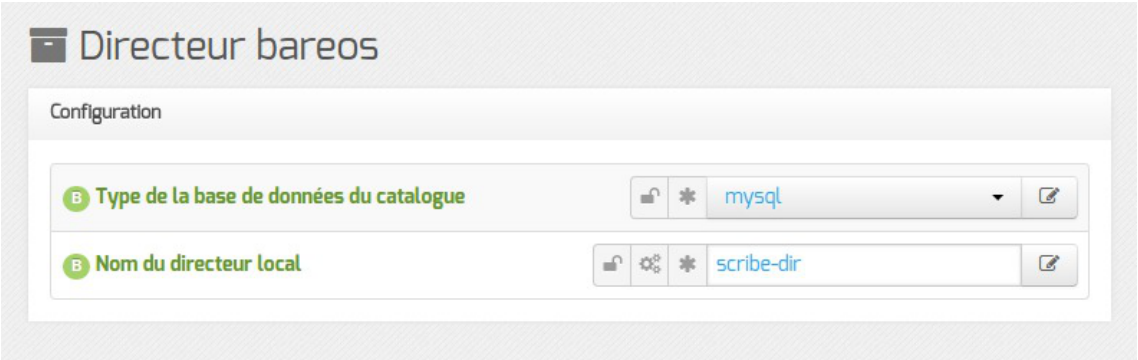


Si le support de stockage de la sauvegarde est activé (`Activer le support de stockage de la sauvegarde` à `oui`) un onglet `Stockage bareos` apparaît dans l'interface de configuration du module.

L'onglet permet de configurer le nom du serveur de stockage et d'autoriser des directeurs à se connecter au stockage.

Suite à l'activation de la sauvegarde du serveur (`Activer la sauvegarde du serveur` à `oui`) l'onglet `Directeur bareos` apparaît dans l'interface de configuration du module. Il permet de configurer le nom du directeur et les périodes de rétention et de définir si le serveur de stockage est distant ou local.

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.

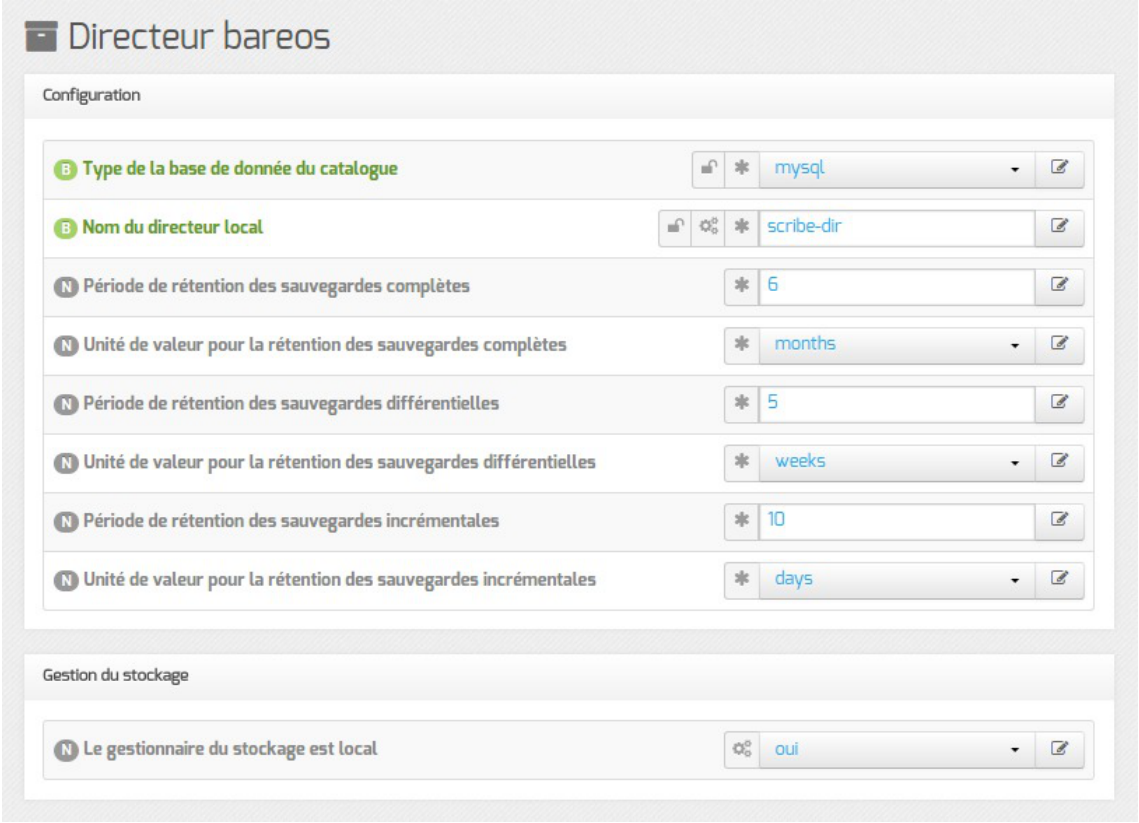
Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

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

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

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.759] 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.

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

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.

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

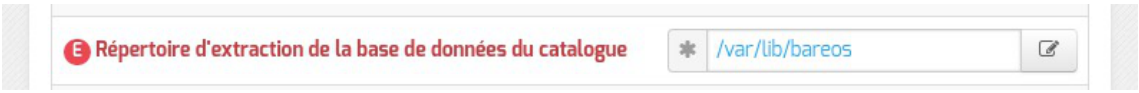
Dans le cas d'un serveur distant (`Activer le serveur de stockage localement` à `non`), il faut configurer l'adresse IP et le mot de passe du serveur de stockage distant.

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.

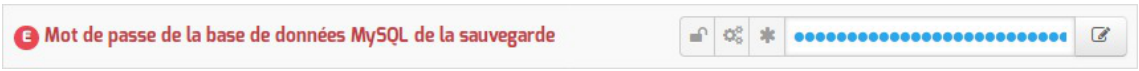
Le déport du service `bareos-sd` sur un autre serveur que `bareos-dir` ne permet pas de gérer correctement les verrous des tâches d'administration sur ce serveur : `bareos-dir` ne permet pas de signaler efficacement à `bareos-sd` qu'une sauvegarde est lancée et qu'il doit poser un verrou empêchant les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

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

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



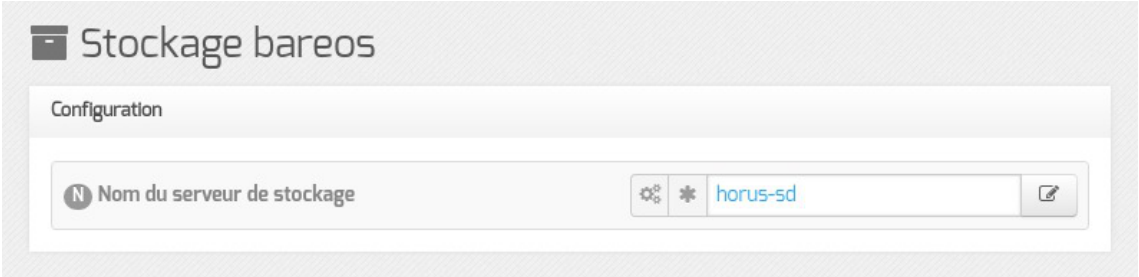
Type de compression et délai alloué

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 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.

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.



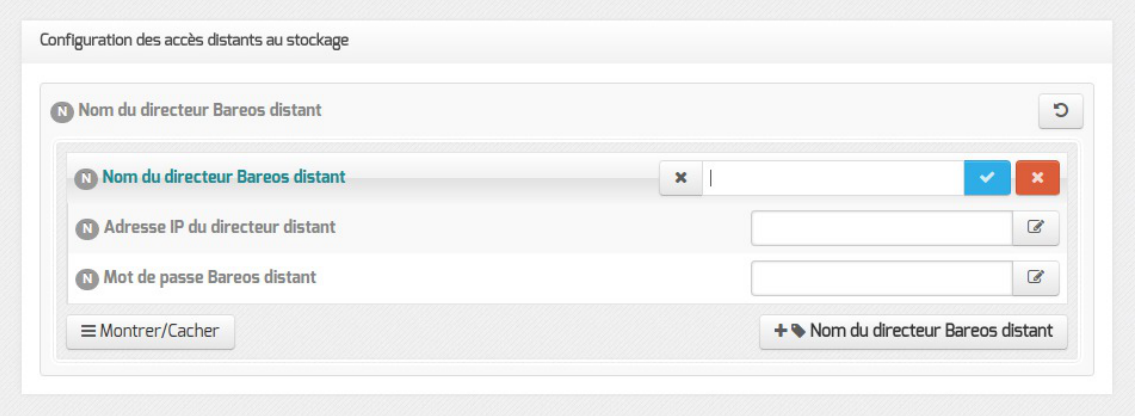
Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur `Nom du directeur Bareos distant`, le détail de l'autorisation s'affiche.

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

- son nom ;
- son adresse IP ;

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

- 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.

Pour que les modifications soient prises en compte, une reconfiguration du module est nécessaire avec la commande : `reconfigure`.

Voir aussi...

Les mots de passe

bareos-webui : outil d'administration pour Bareos [p.486]

4.2.3.b. Configuration depuis l'EAD

Une fois le stockage Bareos activé dans l'interface de configuration du module, il faut configurer le support de sauvegarde.

Le menu `Sauvegardes` de l'EAD propose une interface simplifiée pour la configuration du support de sauvegarde et le paramétrage facultatif de l'envoi des rapports.

Configuration du support

Trois types de support de sauvegarde sont proposés :

- SMB
- Disque USB local
- Configuration manuelle du support

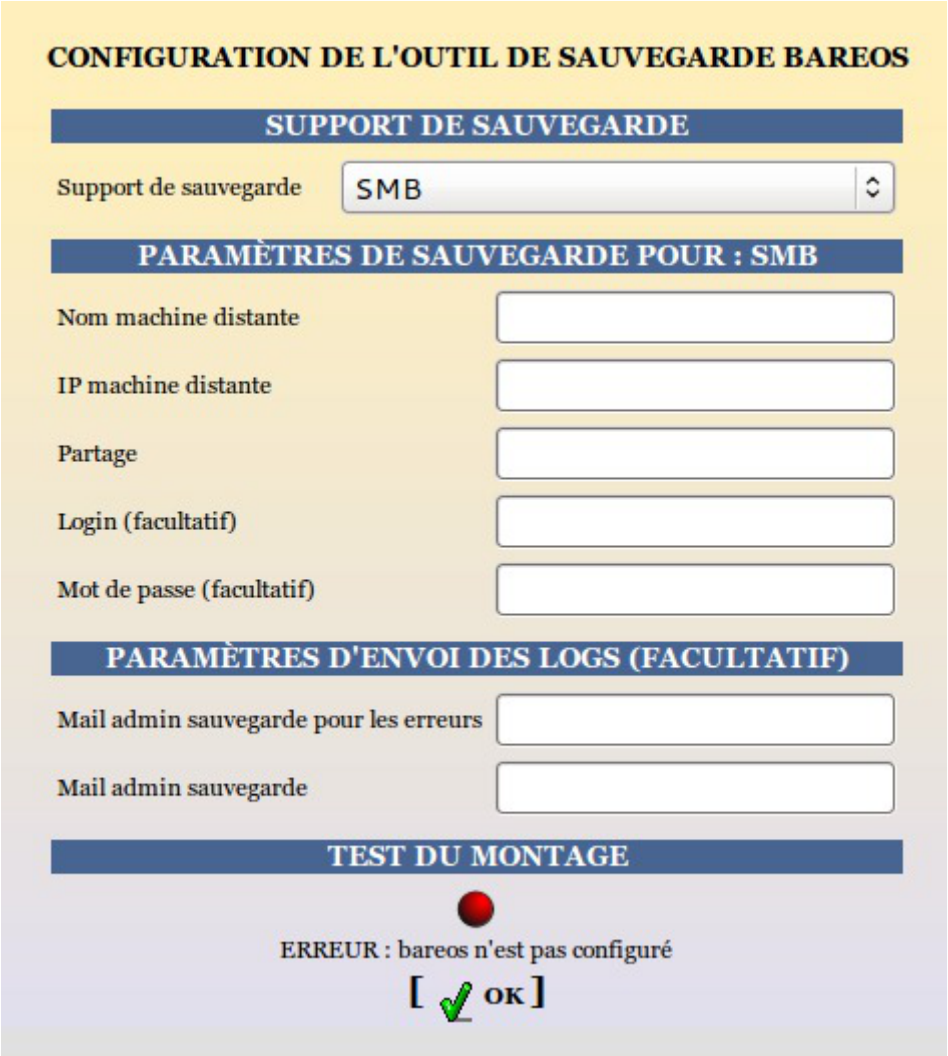
Le point de montage du support est, dans les trois cas de figure : `/mnt/sauvegardes`

- **SMB** : la sauvegarde se fait à travers un partage SMB[p.778].
  Il est préférable de déporter le serveur de stockage Bareos plutôt que d'utiliser le protocole SMB[p.778].
  Ce type de sauvegarde sera utilisé, par exemple, pour les NAS[p.770].

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

Les informations suivantes sont demandées :

- `Nom de machine de la machine distante` (n'accepte pas les majuscules) ;
- `IP de la machine distante` ;
- le nom du `Partage` ;
- optionnellement le `Login`, le `Mot de passe`.



Configuration d'un support de sauvegarde distant dans l'EAD

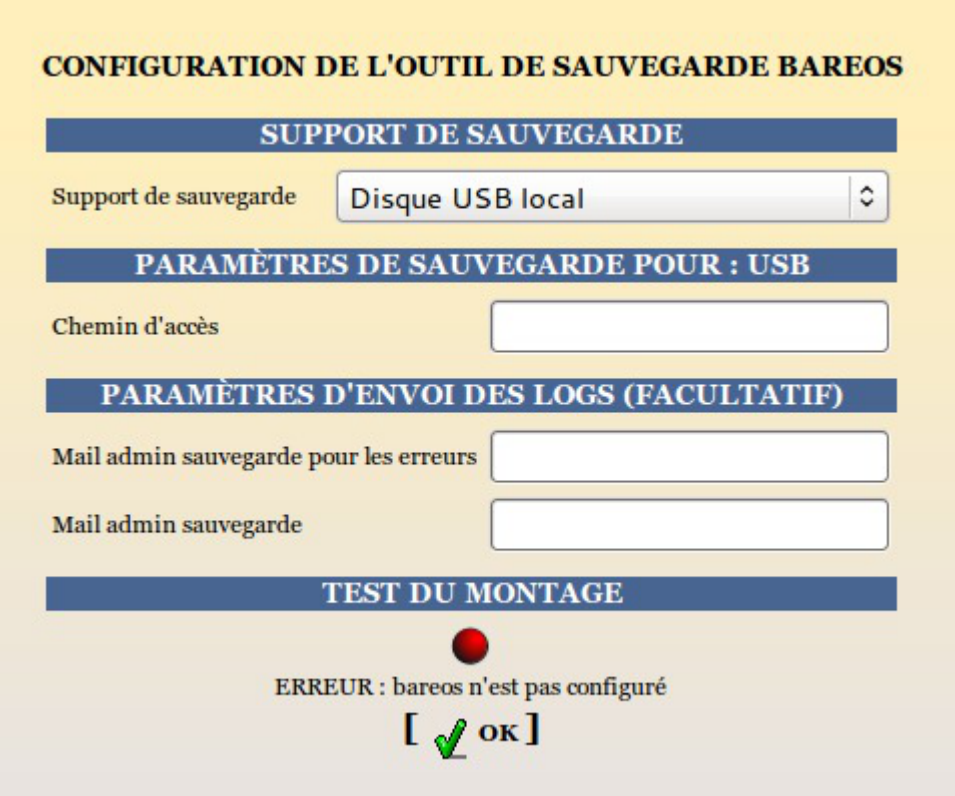
Les informations stockées dans les sauvegardes sont sensibles, il donc préférable de toujours authentifier l'accès aux partages contenant les données.

- **Disque USB local** : la sauvegarde se fait sur un support nécessitant un montage (disque USB, disque interne, etc.), contrôlé avant chaque sauvegarde.

  Le chemin d'accès à saisir correspond au nœud du périphérique (par exemple `/dev/hda1`, `/dev/disk/by-label/LABEL` si un label est disponible sur le disque).

  Si le périphérique utilise un label

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



Configuration d'un support de sauvegarde USB local dans l'EAD

Méthode purement locale à la machine, cette méthode est donc sensible aux corruptions éventuelles du serveur.

- **Configuration manuelle du support** : comme son nom l'indique elle permet à l'utilisateur de définir sa propre destination de sauvegarde via les outils Bareos. Ce choix correspond généralement à l'utilisation de lecteurs de bandes et s'intègre dans une stratégie de sauvegarde à plus grande échelle.

  Le point de montage par défaut est toujours `/mnt/sauvegardes`. Le montage n'est pas contrôlé.

Le pilote est dépendant du matériel, le lecteur de bande doit être configuré manuellement.

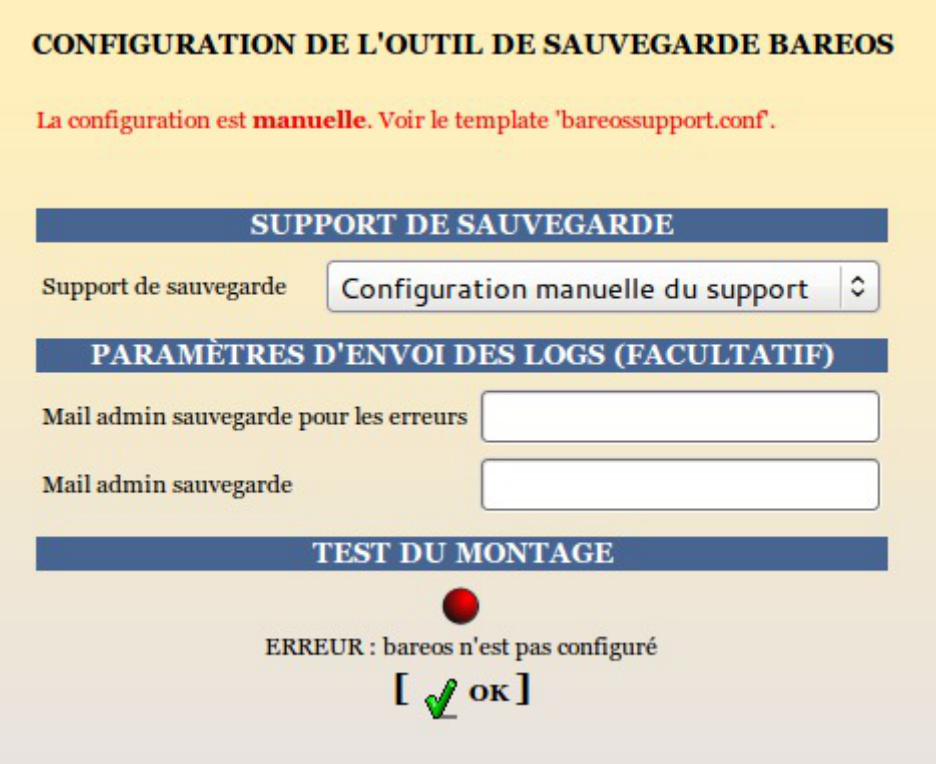
Pour information, le fichier template concerné `bareossupport.conf` est dans `/usr/share/eole/creole/distrib/`

Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE[p.774].

Voir la documentation officielle de Bareos pour le paramétrage :

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-480004

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



Configuration d'un support de sauvegarde manuelle dans l'EAD

Le support doit être monté sur `/mnt/sauvegardes` et l'utilisateur `bareos` doit avoir les droits en écriture :

```
# ls -l /mnt
# chown -R bareos:root /mnt/sauvegardes
```

Options de montage du support de sauvegarde

Le fichier `/etc/eole/bareos.conf` permet de personnaliser les options de montage du support de stockage de la sauvegarde. L'intérêt est que ce fichier ne sera pas écrasé lors de la prochaine mise à jour.

Le fichier `/etc/eole/bareos.conf` a une syntaxe du type fichier INI[p.765] : clé = valeur.

Il existe trois variables paramétrables `DISTANT_LOGIN_MOUNT`, `DISTANT_MOUNT` et `USB_MOUNT` :

- la ligne de commande permettant de monter un support distant avec authentification, la valeur par défaut de `DISTANT_LOGIN_MOUNT` est :

```
/bin/mount -t cifs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev,vers=
//{4}/{5} {6}
```

- la ligne de commande permettant de monter un support distant sans authentification, la valeur par défaut de `DISTANT_MOUNT` est :

```
/bin/mount -t cifs -o password={0},ip={1},uid={2},noexec,nosuid,nodev,vers=3.0
```


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

`//{3}/{4} {5}`

- la ligne de commande permettant de monter un support USB :

  Par défaut la valeur de la variable USB_MOUNT est :

  - `/bin/mount {0} {1} -o noexec,nosuid,nodev,uid={2},umask=0077` pour les systèmes VFAT et NTFS
  - `/bin/mount {0} {1} -o noexec,nosuid,nodev` pour le reste.

Sur les modules EOLE 2.6 utilisant un noyau Linux 4.4, le montage distant est paramétré avec l'ancienne option `sec=ntlm` qu'il est possible de remplacer par `vers=2.0` si le montage distant le requiert

Paramètres pour l'envoi de rapports

L'envoi de courriels est proposé si le directeur Bareos est activé sur le serveur.

EOLE offre la possibilité d'envoyer deux types de courriel :

- les rapports d'erreurs de Bareos ;
- les rapports de sauvegarde réussie.

Il est recommandé de définir les deux types d'envoi. Le premier type de rapport informe que la sauvegarde s'est mal déroulée, alors que le second informe qu'une sauvegarde s'est bien déroulée. Pensez à configurer correctement votre relai SMTP[p.778].

Il est possible de déclarer plusieurs destinataires en séparant les adresses par des virgules.

Exemple : `admin@ac-dijon.fr,technicien@ac-dijon.fr`

4.2.3.c. Configuration depuis la ligne de commande

Il n'est pas nécessaire de passer par l'EAD pour configurer le support de sauvegarde.

L'ensemble des paramétrages peut être réalisé avec le script `bareosconfig.py`.

Les informations définies dans l'EAD sont modifiables en ligne de commande et inversement.

Configuration du support

- Si le support est un partage SMB :

```
# bareosconfig.py -s smb --smb_machine=nom_machine --smb_ip=adresse_ip
--smb_partage=nom du partage --smb_login=login --smb_password=mot de passe
```

- Si le support est un disque USB local :

```
# bareosconfig.py -s usb --usb_path=/dev/device usb
```

- Si le support est un disque USB local avec un label :

```
# bareosconfig.py -s usb --usb_path=/dev/disk/by-label/LABEL
```

- Si le support est à configurer manuellement :

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

```
# bareosconfig.py -s manual
```

Vous devez ensuite configurer le support dans le fichier template /usr/share/eole/creole/distrib/bareossupport.conf

Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE[p.774].

`nom_machine` ne doit pas comporter de majuscule

Pour tester le support de sauvegarde (USB local ou SMB), il est possible d'utiliser le script bareosmount.py :

```
# bareosamount.py -t
Test de montage OK
```

En USB le numéro du périphérique dans /dev peut changer selon si un autre périphérique est connecté au serveur.

Une astuce consiste à utiliser un label pour identifier de façon plus certaine le périphérique utilisé.

Pour donner un label au périphérique :

```
# tune2fs -L Sauvegardes /dev/sdX
```

Pour configurer le support de sauvegarde sur le périphérique USB :

```
# bareosconfig.py -s usb --usb_path=/dev/disk/by-label/Sauvegardes
```

Options de montage du support de sauvegarde

Le fichier /etc/eole/bareos.conf permet de personnaliser les options de montage du support de stockage de la sauvegarde. L'intérêt est que ce fichier ne sera pas écrasé lors de la prochaine mise à jour.

Le fichier /etc/eole/bareos.conf a une syntaxe du type fichier INI[p.765] : clé = valeur.

Il existe trois variables paramétrables `DISTANT_LOGIN_MOUNT`, `DISTANT_MOUNT` et `USB_MOUNT` :

- la ligne de commande permettant de monter un support distant avec authentification, la valeur par défaut de `DISTANT_LOGIN_MOUNT` est :

```
/bin/mount -t cifs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev,vers=
//{4}/{5} {6}
```

- la ligne de commande permettant de monter un support distant sans authentification, la valeur par défaut de `DISTANT_MOUNT` est :

```
/bin/mount -t cifs -o
```


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

```
password={0},ip={1},uid={2},noexec,nosuid,nodev,vers=3.0
//{3}/{4} {5}
```

- la ligne de commande permettant de monter un support USB :

  Par défaut la valeur de la variable USB_MOUNT est :

  - `/bin/mount {0} {1} -o noexec,nosuid,nodev,uid={2},umask=0077` pour les systèmes VFAT et NTFS
  - `/bin/mount {0} {1} -o noexec,nosuid,nodev` pour le reste.

Sur les modules EOLE 2.6 utilisant un noyau Linux 4.4, le montage distant est paramétré avec l'ancienne option `sec=ntlm` qu'il est possible de remplacer par `vers=2.0` si le montage distant le requiert

Paramètres pour l'envoi de rapports

La configuration de l'adresse courriel se fait de la façon suivante :

```
# bareosconfig.py -m --mail_ok=adresse_courriel
--mail_error=adresse_courriel
```

Les paramètres --mail_ok et --mail_error ne sont pas obligatoires.

Afficher la configuration

Il est possible de lister l'ensemble des paramètres depuis la ligne de commande avec la commande `bareosconfig.py` :

```
1 # bareosconfig.py -d
2 Support : {'usb_path': '/dev/sdb1', 'support_type': 'usb'}
3 Mail : {'mail_error': [], 'mail_ok': []}
4 Programmation :
5   Aucun job programmé.
```

4.2.4. Programmation des sauvegardes

Une fois le support de sauvegarde défini, il est possible de programmer un type de sauvegarde par périodicité.

Cette programmation se fait soit par l'EAD soit depuis la ligne de commande.

EOLE propose trois périodicités et trois types de sauvegarde pour la programmation des sauvegardes :

Périodicité	Type de sauvegarde
sauvegardes mensuelles	totale
sauvegardes hebdomadaires	totale, différentielle, incrémentale
sauvegardes quotidiennes	totale, différentielle, incrémentale

En plus des périodicités proposées, il est possible de lancer une sauvegarde immédiate de type totale, différentielle ou incrémentale.

Seules les sauvegardes totales sont possibles dans le cas de la périodicité mensuelle.

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

Les sauvegardes mensuelles se font la première semaine du mois.

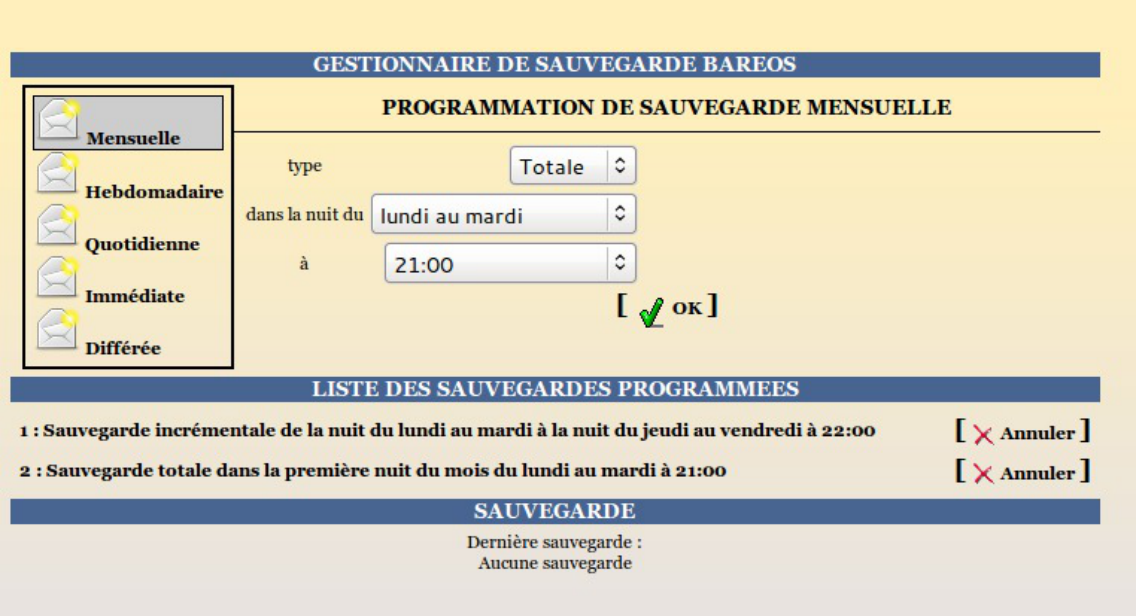
Si une autre sauvegarde est programmée la même nuit, celle-ci sera automatiquement reportée à la semaine d'après.

Les sauvegardes se programment pour une nuit de la semaine. Une nuit va de 12h à 11h59.

Pour les sauvegardes quotidiennes, il est possible de choisir une plage de jours.

Programmation depuis l'EAD

Le menu `Sauvegardes` de l'EAD propose une interface simplifiée pour programmer des sauvegardes périodiques ou pour lancer une sauvegarde immédiate.



L'interface de programmation des sauvegardes dans l'EAD

Programmation depuis la ligne de commande

Pour ajouter une nouvelle programmation, il faut connaître les paramètres suivants :

- choix de la périodicité : **quotidienne** → daily, **hebdomadaire** → weekly ou **mensuelle** → monthly ;
- le type : **totale** → Full, **différentielle** → Differential ou **incrémentale** → Incremental ;
- le jour de la semaine : de 1 (pour la nuit de dimanche à lundi) à 7 (pour la nuit du samedi à dimanche) ;
- en cas de sauvegarde quotidienne, éventuellement le jour de fin : de 1 à 7 ;
- l'heure de la sauvegarde : de 0 à 23, sachant que la nuit commence à 12h et fini à 11h le lendemain

Exemple pour ajouter une programmation de sauvegarde depuis la ligne de commande :

```
# bareosconfig.py -j daily --job_level=Incremental --job_day=2 --job_end_day=5 --job_hour=22
```

Les programmations ajoutées depuis la ligne de commande sont également visibles dans l'EAD.

Il est également possible de lancer une sauvegarde immédiate.

Il est nécessaire de choisir le type de sauvegarde totale (Full), différentielle (Differential) ou incrémentale (Incremental)).

Si aucune sauvegarde n'a été effectuée préalablement sur le serveur, la première sauvegarde sera automatiquement une sauvegarde totale.

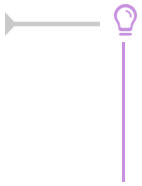
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour effectuer une sauvegarde immédiate, il faut exécuter la commande suivante :

```
# bareosconfig.py -n --level=Full
```

Il est possible de suivre l'évolution de la sauvegarde dans le fichier `/var/log/rsyslog/local/bareos-dir/bareos-dir.info.log`.

Les éventuelles erreurs sont enregistrées dans le fichier `/var/log/rsyslog/local/bareos-dir/bareos-dir.err.log`.



`bareosconfig.py --help` donne la liste des options de `bareosconfig.py`

Il existe également des pages de manuel :

`man bareos`, `man bareos-dir`, ...

Afficher la configuration

Il est possible de lister l'ensemble de la configuration depuis la ligne de commande avec la commande `bareosconfig.py` :

```
# bareosconfig.py -d
Support : {'usb_path': '/dev/sdb1', 'support': 'usb'}
Mail : {}
Programmation :
1 : Sauvegarde totale dans la première nuit du mois du mercredi au jeudi à 02:00
2 : Sauvegarde incrémentale de la nuit du lundi au mardi à la nuit au vendredi à 22:00
3 : Sauvegarde totale dans la première nuit du mois du lundi au mardi à 21:00
```

Supprimer un job

Il est possible de supprimer un job depuis la ligne de commande grâce à la commande `bareosconfig.py`. Elle s'utilise comme suit :

```
# bareosconfig.py -x <numéro job>
```

ou encore :

```
# bareosconfig.py --job_to_delete=<numéro job>
```

4.3. La restauration des sauvegardes EOLE

La restauration peut être :

- **complète**, elle va restaurer l'ensemble des bases de données, l'annuaire, les quotas, ... ainsi que l'ensemble des fichiers sauvegardés.
- **partielle,** elle peut restaurer l'ensemble ou une partie des fichiers sauvegardés.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.3.1. Restauration complète



La restauration d'un serveur s'effectue toujours sur un serveur instancié.

Préparation du serveur avant restauration

Mise à jour

Idéalement, le niveau de mise à jour du serveur avant restauration doit être identique au à celui du serveur sauvegardé.

Mettre à jour les paquets :

`Maj-Auto`

Choix du mode conteneur ou non

Si le serveur sauvegardé était en mode conteneur, il faut re-créer les conteneurs, avec la commande `gen_conteneurs`.

Configurer Bareos

- si le serveur est enregistré dans Zéphir, il faudra redescendre la configuration en ré-enregistrant le serveur avec la commande `enregistrement_zephir` ;
- si le serveur n'est pas enregistré dans Zéphir, il sera nécessaire de récupérer la sauvegarde de la configuration sur le support de sauvegarde.

  Configuration de Bareos pour un serveur non enregistré dans Zéphir

  ```
  # bareosconfig.py -s usb --usb path=/dev/device usb
  ```

  Configuration de Bareos pour un serveur non enregistré dans Zéphir avec le label du périphérique

  ```
  # bareosconfig.py -s usb --usb path=/dev/disk/by-label/LABEL
  ```

  Il est normal d'avoir le message suivant lors de l'utilisation de `bareosconfig.py` :

  ```
  Fichier template /var/lib/creole/bareossupport.conf inexistant
  ```

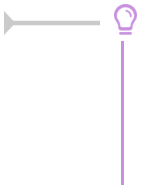
  Il peut être utile de configurer l'envoi des courriels en même temps que le support de sauvegarde.

  ```
  # bareosconfig.py -m --mail_ok=mailok@ac-dijon.fr
  --mail_error=mailerror@ac-dijon.fr
  ```

Paquets additionnels

Pour les paquets additionnels ajoutés sur l'ancien serveur (`eole-ejabberd` par exemple) il est impératif que le paquet soit installé sur le serveur au moment où on exécute la restauration.

- si le serveur était enregistré sur un serveur Zéphir, les paquets additionnels déclarés sont installés à la fin de l'enregistrement auprès du serveur Zéphir ;
- dans le cas d'une installation isolée, il est judicieux de réinstaller les paquets avant d'instancier le serveur.



Si l'ancien serveur est toujours accessible, il est possible de lister l'ensemble des paquetages installés grâce à la commande :

```
# dpkg --get-selections
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est possible de filtrer uniquement les paquets préfixé par `eole-` :

```
# dpkg --get-selections | grep eole-
```

La liste des paquets peut être exportée dans un fichier pour être transférée sur une autre machine :

```
# dpkg --get-selections > paquetages.txt
```

Récupération de la liste précédente :

```
# dpkg --set-selections < paquetages.txt
```

Installation des paquets de la liste :

```
# apt-get dselect-upgrade
```

Pour avoir plus d'informations (version, architecture et descriptif) sur les paquets installés il est possible d'utiliser l'option -l

```
# dpkg -l | grep eole
```

Montage du support

Une fois que le serveur est enregistré dans Zéphir ou que le support est configuré, il faut monter le support de sauvegarde :

```
# bareosmount.py --mount
```

```
Montage OK
```

Extraire le fichier config.eol de la sauvegarde

Pour extraire le fichier `config.eol` de la sauvegarde il est nécessaire de connaître le nom du directeur.

Le nom du directeur est, par défaut, de la forme : **nom_du_module-dir** (par exemple : *scribe-dir*).

Si vous ne vous souvenez plus du nom du directeur de votre serveur, il suffit de regarder le contenu du support de sauvegarde :

```
# ls /mnt/sauvegardes/*-catalog-0003
```

```
/mnt/sauvegardes/amonecole-dir-catalog-0003
```

Le directeur est dans ce cas **amonecole-dir**.

bareosrestore.py --configeol amonecole-dir

Le fichier `config.eol` extrait est enregistré dans `/root/zephir-restore.eol`.

Instance

Avant toute chose, il faut déplacer et renommer le fichier de configuration :

```
# mv /root/zephir-restore.eol /etc/eole/config.eol
```

Instancier maintenant votre serveur avec la commande : `instance`

Si vous avez enregistré votre serveur sur Zéphir, il est possible d'utiliser directement le fichier de configuration `zephir.eol`

À l'étape de Postconfiguration, sauf besoin exceptionnel il ne faut pas réinitialiser le catalogue :

```
Le catalogue Bareos a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non]
```

Ne pas tenir compte du message d'erreur suivant :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
ERREUR : /var/lib/eole/config/shedule.conf not exist
```

Récupération du catalogue

Pour récupérer le catalogue de sauvegarde il est nécessaire de connaître le nom du directeur.

Le nom du directeur est, par défaut, de la forme : **nom_du_module-dir** (par exemple : *scribe-dir*).

Si vous ne vous souvenez plus du nom du directeur de votre serveur, il suffit de regarder le contenu du support de sauvegarde :

```
# ls /mnt/sauvegardes/*-catalog-0003
/mnt/sauvegardes/amonecole-dir-catalog-0003
```

Le directeur est dans ce cas **amonecole-dir**.

Lancer la récupération du catalogue :

```
# bareosrestore.py --catalog
Restauration du catalog
Pas de fichier /var/lib/eole/config/bareosjobs.conf dans le volume nom du directeur-catalog-0003
Pas de fichier /etc/eole/bareos.conf dans le volume nom du directeur-catalog-0003
```

Les messages concernant l'absence de certains fichiers sont normaux.

Le répertoire `/var/lib/bareos/` doit contenir :

- nom_du_directeur-JobDefsCatalog.bsr
- nom_du_directeur-JobDefsSauvegarde.bsr
- bareos.sql

Démontage du support

Pour démonter le support de sauvegarde :

```
# bareosmount.py --umount
```

Restauration

Avant de lancer la restauration il est préférable de vérifier que le chemin du nœud du périphérique est toujours bon.

Il peut changer en fonction du nombre de périphériques connectés :

```
# bareosmount.py -t
```

Si le périphérique n'a plus le même nœud la commande `bareosmount.py` renvoie :

```
ERREUR : le périphérique /dev/sdb1 n'existe pas
```

Il faut alors changer la configuration du support :

```
# bareosconfig.py -s usb --usb path=/dev/device usb
```

ou si le disque a un label :

```
# bareosconfig.py -s usb --usb path=/dev/disk/by-label/LABEL
```

Le test de montage doit renvoyer OK :

```
# bareosmount.py -t
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Test de montage OK
```

Lister l'ensemble de la configuration :

```
# bareosconfig.py -d
```

La restauration complète du serveur va restaurer l'ensemble des bases de données, l'annuaire, les quotas, ... ainsi que l'ensemble des fichiers sauvegardés.

Pour ce faire il faut utiliser la commande `bareosrestore.py` :

```
# bareosrestore.py --all
```



Il est possible de suivre l'évolution des restaurations dans le fichier de log : `/var/log/bareos/restore.txt`

Les informations peuvent mettre un peu de temps avant d'apparaître car Bareos ne les "flush" pas tout de suite dans son fichier de log.

Si rien n'apparaît dans un délai raisonnable il faut vérifier le chemin du nœud du périphérique.

Lorsque la restauration complète est terminée, il faut re-configurer votre serveur à l'aide de la commande `reconfigure`.

4.3.2. Restauration partielle

Rechercher un fichier à restaurer

Pour rechercher un fichier ou un répertoire dans le support de sauvegarde (sur la dernière sauvegarde uniquement), on utilise l'option `--search` :

```
# bareosrestore.py --search nom_du_fichier
```

Il est possible d'utiliser les caractères `?` ou `*` pour remplacer respectivement un ou plusieurs caractères en l'échappant de la façon suivante :

```
# bareosrestore.py --search nom_du_\*
```

Il est également possible de lister le contenu d'un répertoire sauvegardé avec l'option `--ls_folder` :

```
# bareosrestore.py --ls_folder /etc/eole
liste du contenu de /etc/eole
config.eol
```

Restauration d'un fichier ou d'un répertoire

Pour restaurer un fichier de la dernière sauvegarde, on peut utiliser la commande :

```
# bareosrestore.py --file /chemin_absolu/nom_du_fichier
```

Exemple :

```
# bareosrestore.py --file /etc/eole/config.eol
```

Pour restaurer un répertoire et l'intégralité de son contenu, on peut utiliser la commande :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# bareosrestore.py --folder /chemin absolu/nom du répertoire
```

Exemple :

```
# bareosrestore.py --folder /usr/share/ead2/backend/config
```

Restauration de l'ensemble des fichiers sauvegardés

Pour restaurer l'ensemble des fichiers sauvegardés, il est possible d'utiliser la commande :

```
# bareosrestore.py --all_files
```

Restauration spécifique

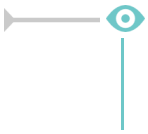
Les bases de données, les quotas, l'annuaire, ... ne sont pas sauvegardés sous forme de fichiers binaires.

Ils sont extraits avant la sauvegarde.

Pour restaurer, il existe une procédure particulière, différente suivant l'application.

Pour connaître les possibilités, faire :

```
# bareosrestore.py --help
```



Pour restaurer l'annuaire :

```
# bareosrestore.py --ldap
```

Restauration manuelle

Avant de lancer la restauration il est préférable de vérifier que le chemin du nœud du périphérique est toujours bon.

Il peut changer en fonction du nombre de périphériques connectés :

```
# bareosmount.py -t
```

Si le périphérique n'a plus le même nœud la commande `bareosmount.py` renvoie :

```
ERREUR : le périphérique /dev/sdb1 n'existe pas
```

Il faut alors changer la configuration du support :

```
# bareosconfig.py -s usb --usb_path=/dev/device_usb
```

ou si le disque a un label :

```
# bareosconfig.py -s usb --usb path=/dev/disk/by-label/LABEL
```

Le test de montage doit renvoyer OK :

```
# bareosmount.py -t
Test de montage OK
```

Lister l'ensemble de la configuration :

```
# bareosconfig.py -d
```

La restauration manuelle s'effectue au moyen d'un programme en ligne de commande, `bconsole` :

```
# bconsole
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est possible de spécifier le fichier de configuration :

```
# bconsole -c /etc/bareos/bconsole.conf
```

Une fois bconsole démarré, il est possible d'abandonner la procédure à tout moment en quittant la console avec la commande `quit`, `done` ou avec les touches `ctrl + c`.

Le prompt de bconsole est une étoile.



Dans cet exemple nous verrons comment restaurer le fichier `/home/a/admin/perso/icones.url`.

Dans bconsole, taper la commande restore qui indique à bconsole d'initialiser une restauration :

```
*restore
```

Il est possible de choisir directement le support de sauvegarde des fichiers, ce qui évite d'avoir à le choisir par la suite, pour cela utiliser la commande suivante (attention aux majuscules/minuscules et à la saisie sans accents) :

```
*restore fileset=FileSetSauvegarde
```

Vous avez alors plusieurs choix :

```
To select the JobIds, you have the following choices:
[...]
```

Les plus pertinents sont :

- Depuis que l'utilisateur a supprimé le fichier le système n'a effectué que des sauvegardes incrémentales alors le fichier est toujours présent dans la sauvegarde, choisissez la sauvegarde la plus récente pour un client :

  ```
  5: Select the most recent backup for a client (sélectionner la sauvegarde réussie la plus récente)
  ```

- Depuis que l'utilisateur a supprimé le fichier le système a effectué une sauvegarde complète (Full) alors le fichier n'est présent que dans les sauvegardes précédant la sauvegarde complète, sélectionner la dernière sauvegarde pour un client avant une certaine date et entrez une date antérieure à la dernière sauvegarde complète :

  ```
  6: Select backup for a client before a specified time (sélectionner la dernière sauvegarde réussie avant une date spécifiée)
  ```

La console propose trois options :

```
The defined FileSet ressources are :
1 : FileSetCatalog
2 : FileSetDefault
3 : FileSetSauvegarde
```

Il faut ensuite choisir le support de sauvegarde des fichiers (et non celui du catalogue) :

```
3 : FileSetSauvegarde
```

Un prompt apparaît et permet de naviguer dans l'arborescence des sauvegardes :

```
cwd is : /
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
$ ls
etc/
home/
root/
usr/
var/
$ cd /home/a/admin/perso
```

Il faut marquer les fichiers/dossiers à restaurer avec la commande `mark` (attention, la commande mark est récursive) :

```
$ mark icones.url
1 file marked.
```

Pour "dé-marquer" un fichier marqué par erreur :

```
$ unmark icones.url
1 file unmarked.
```

Lorsque les fichiers et les dossiers à restaurer sont sélectionnés, passer à l'étape suivante avec la commande :

```
$ done
```

bconsole propose plusieurs options, il faut choisir le job de restauration, ici l'option numéro 3 :

```
3: Restore file
```

On obtient alors le message suivant :

```
Bootstrap records written to /var/lib/bareos/xxxxxxxxx.restore.2.bsr
[...]
Ok to run ? (yes/mod/no) :
```

La restauration peut maintenant être lancée en répondant `yes` à la question.

Il ne sera plus possible d'abandonner après cette étape.

```
OK to run? (yes/mod/no): yes
```

La restauration est alors placée dans une file d'attente. Le numéro `JobId` est affiché à l'écran.

Il est possible de changer les paramètres de restauration en répondant `mod` à la question :

```
OK to run? (oui/mod/non): mod
Parameters to modify :
1 : Level
2 : Storage
[...]
```

Par exemple pour restaurer dans un autre répertoire, il faut choisir `Where` (9 dans le cas présent) et saisir le chemin de la restauration :

```
9 : Where
Please enter path prefix for restore (/ for none) :
```
/home/restauration

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `Ok to run ? (yes/mod/no) : yes`
>
> La restauration est alors placée dans une file d'attente. Le numéro `JobId` est affiché à l'écran.
>
> Pour quitter la console :
>
> `* quit`



> Il est possible de suivre l'évolution des restaurations dans le fichier de log : /var/log/bareos/restore.txt
>
> Les informations peuvent mettre un peu de temps avant d'apparaître car Bareos ne les "flush" pas tout de suite dans son fichier de log.
>
> Si rien n'apparaît dans un délai raisonnable il faut vérifier le chemin du nœud du périphérique.



> Pour conserver les droits étendus associés à un fichier (ACL), il faut restaurer un fichier issu d'une partition avec ACL (par exemple le répertoire /home sur le module Scribe) dans une partition supportant les ACL.

4.4. Ajouter des données à sauvegarder

Il est tout à fait possible d'ajouter des fichiers et/ou des répertoires à sauvegarder à ceux déjà configurés par défaut sur un module.

Pour cela il faut ajouter un fichier de configuration portant l'extension `.conf` dans le répertoire /etc/bareos/bareosfichiers.d/

Celui-ci ne doit comporter que les directives `Include` et `Exclude`, il ne faut pas, par exemple, spécifier le `Name` du FileSet car il est déjà défini dans le reste de la configuration.

Exemple d'un fichier de configuration pour la prise en charge de nouvelles données à sauvegarder :

```
Include {
   Options {
      # Sauvegarde des ACL
      aclsupport = yes
      # Tous les fichiers seront chiffrés en SHA1
      signature = SHA1
      # Compression des fichiers (niveau de com pression croissant de 0 à 9)
      compression = GZIP6
      # Permet de sauvegarder plusieurs systèmes de fichiers
      onefs = yes
   }
   File = /chemin/du/repertoire/ou/du/fichier/a/sauvegarder
   File = /chemin/du/repertoire/ou/du/fichier/a/sauvegarder
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
}
Exclude {
   File = /chemin/du/repertoire/ou/du/fichier/a/ignorer
   File = /chemin/du/repertoire/ou/du/fichier/a/ignorer
}
```

Pour sauvegarder les fichiers d'un conteneur il faut préciser le chemin complet du fichier, par exemple :

```
   File = /var/lib/lxc/reseau/rootfs/var/www/html/fichier
```

Les autres options pour la ressource FileSet sont consultables dans la documentation officielle du projet Bareos :

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1030008.5



Pour que l'ajout d'un fichier de configuration soit pris en compte par Bareos il faut procéder à la reconfiguration du module avec la commande `reconfigure`.

4.5. Réinitialisation de la sauvegarde

Pour réinitialiser la sauvegarde il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et surtout il faut ré-initialiser la base de données de Bareos.

Pour ce faire il faut utiliser la commande suivante :

```
# bareosregen.sh
La régénération du catalogue de la sauvegarde va écraser l'ancienne base, confirmez-vous ? [oui/non]
[non] : oui
```

4.6. bareos-webui : outil d'administration pour Bareos

bareos-webui est un logiciel libre écrit en PHP (basé sur Zend Framework), destiné à surveiller et à gérer les sauvegardes Bareos au travers d'une application web.

http://www.bareos.org/en/bareos-webui.html

L'interface web permet l'utilisation de plusieurs comptes pour gérer les sauvegardes et afficher les informations détaillées sur les jobs, les clients, groupes de fichiers, Pools, Volumes, stockages, Directeur, Scheduler et les journaux.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Mire d'authentification de bareos-webui

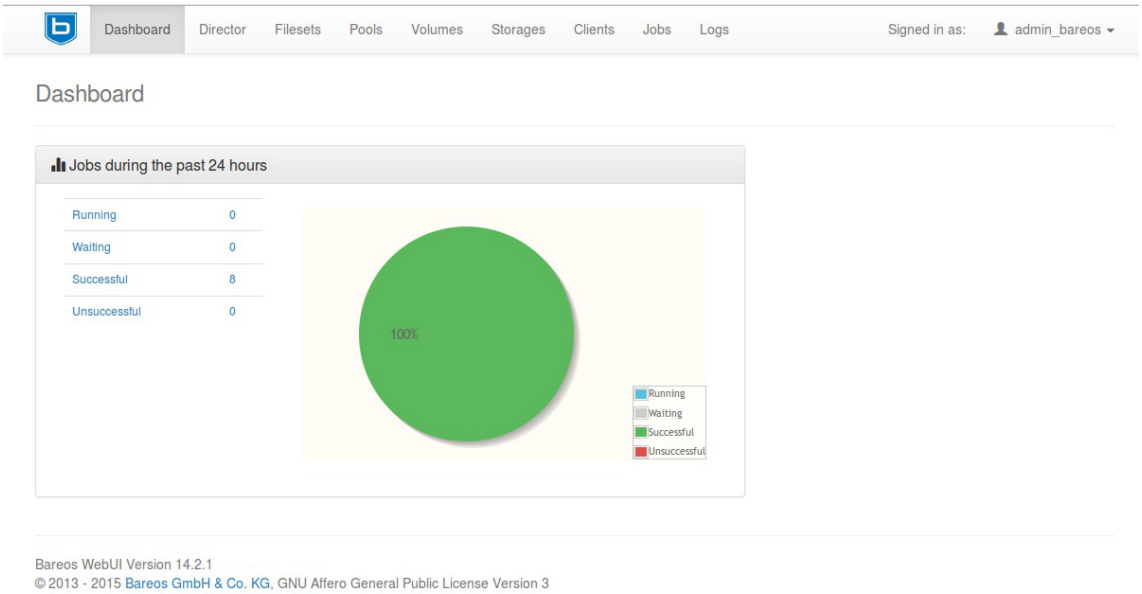
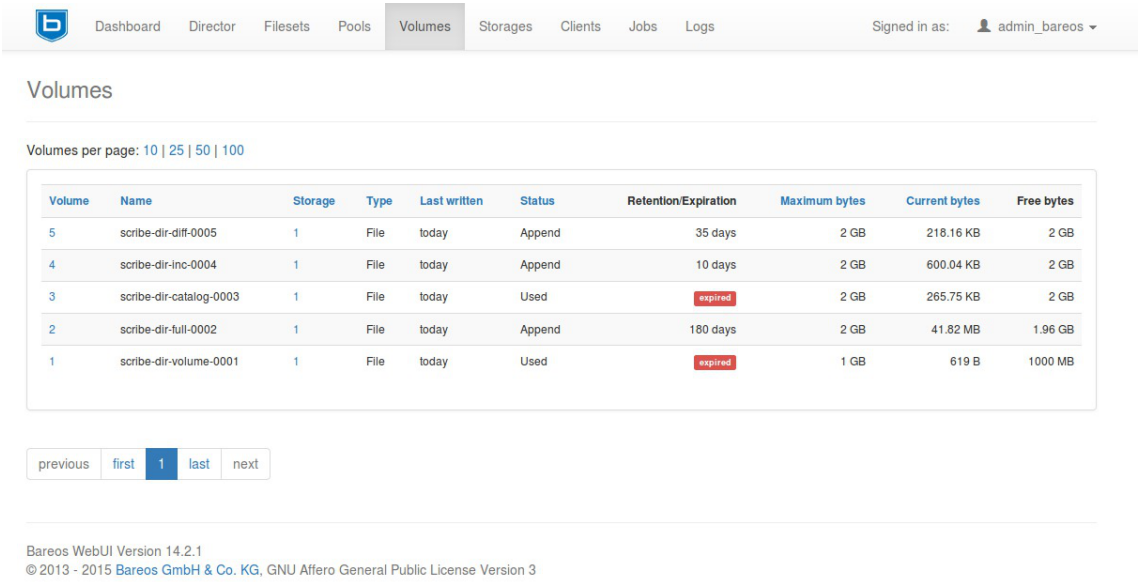
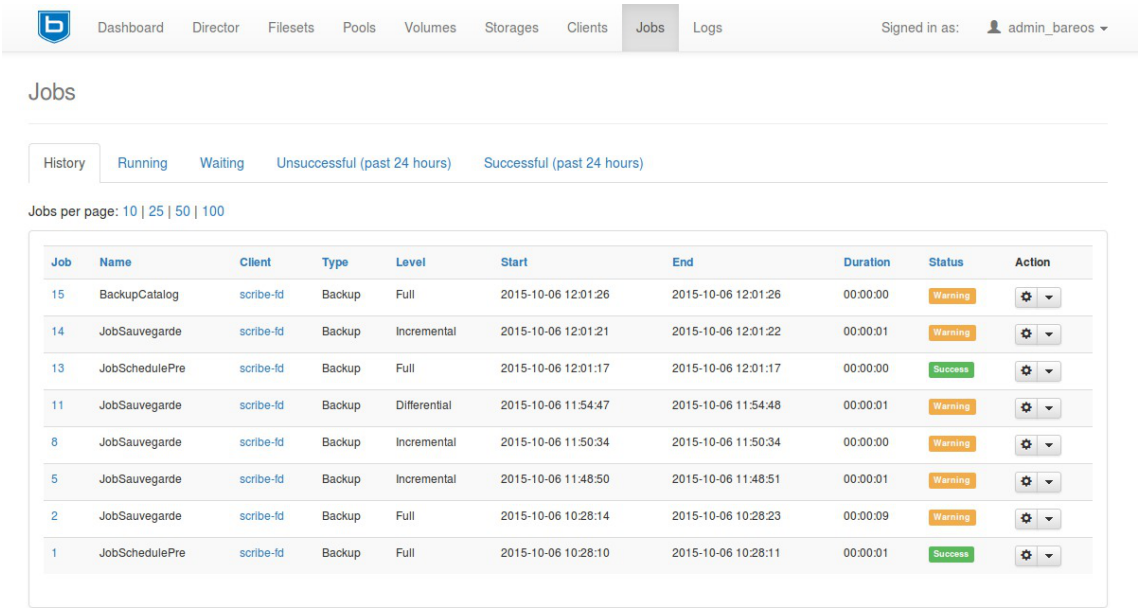


Tableau de bord de bareos-webui



Affichage des volumes dans bareos-webui

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Affichage des jobs dans bareos-webui

Installation

bareos-webui s'installe manuellement, saisir les commandes suivantes dans un terminal :

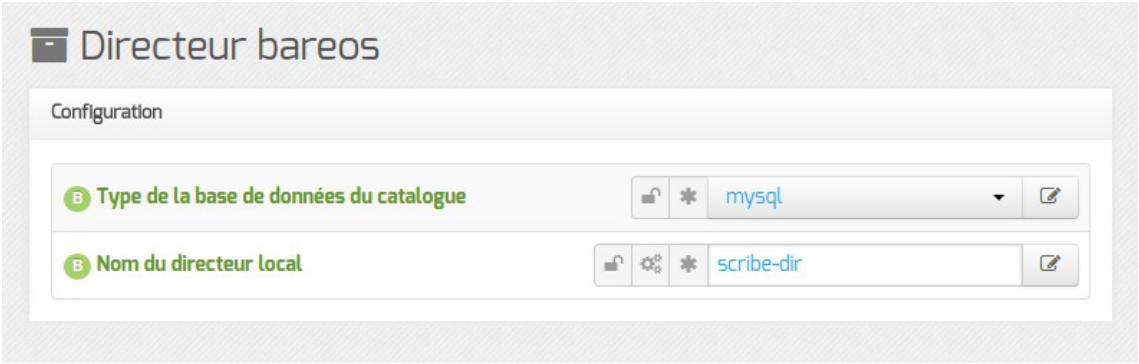
```
# Query-Auto
# apt-eole install eole-bareoswebui
```

Le paquet est pré-installé sur les modules Scribe, Horus et AmonEcole.

Configuration

Bareos doit être configuré pour utiliser une base de données MySQL.

Dans l'interface de configuration du module, dans l'onglet `Directeur Bareos`, le type de la base de données du catalogue doit être positionné sur `mysql`.



Le serveur web apache doit être activé sur le module. Dans l'interface de configuration du module, dans l'onglet `Services`, `Activer le serveur web Apache` doit être à `oui`.

Dans l'onglet `Applications web`, il faut passer `Activer Bareos WebUI (gestion de` `la`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`sauvegarde)` à `oui`.

Un nouvel onglet `Bareos webui` apparaît dans l'interface de configuration du module.



Il est possible de créer un ou plusieurs comptes autorisés à se connecter à l'interface bareos-webui en cliquant sur le bouton `+ Utilisateur autorisé à se connecter à l'interface web de gestion de la sauvegarde`.

Le mot de passe de la base de données MySQL peut éventuellement être personnalisé mais par défaut il est généré automatiquement. Une fois la configuration enregistrée, il ne sera plus possible de le modifier.

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/bareos-webui/`

L'authentification se fait **obligatoirement** avec les comptes déclarés dans l'interface de configuration du module.

Désactivation

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom de l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :

```
# service apache2 reload
```

Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# a2ensite nom de l'application
# service apache2 reload
```

Pour désactiver l'application pour une période plus longue voir définitivement, il faut désactiver l'application depuis l'interface de configuration du module, dans l'onglet Applications web.

L'opération nécessite une reconfiguration du module avec la commande reconfigure.

Voir aussi...

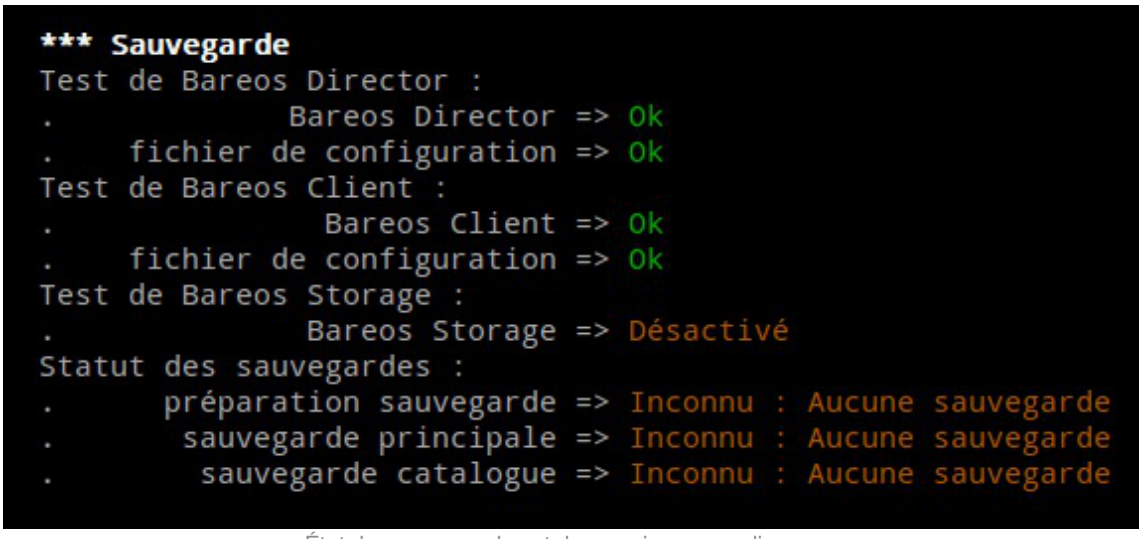
Activation et configuration de Bareos [p.325]

4.7. Diagnostic, rapport et résolution de problème

4.7.1. Outils de diagnostic et rapport

En plus de l'envoi de courrier électronique, il est possible de connaître l'état de la dernière sauvegarde en utilisant la commande diagnose.

Celle-ci liste également l'état des différents services de Bareos.



État des sauvegardes et des services avec diagnose

L'EAD permet également de connaître l'état de la dernière sauvegarde depuis sa page d'accueil.

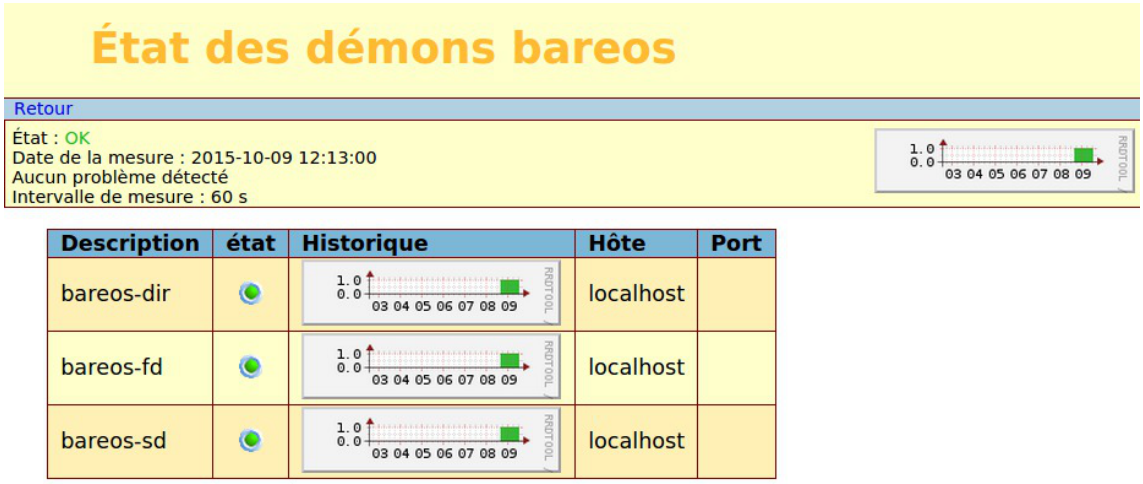
Le détail de la sauvegarde est disponible en cliquant sur Afficher le rapport.



État des sauvegardes dans l'EAD

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Par contre, pour voir l'état des différents services Bareos il faut se rendre à la rubrique `ETAT DES SERVICES` de la page d'accueil et cliquer sur `DETAILS`, puis sélectionner `État des démons bareos`.



États des services Bareos dans l'EAD

Si l'un des services est arrêté, il est possible de le relancer à l'aide de la commande `service` :

```
# service bareos-dir restart
* Restarting Bareos Director bareos-dir ... [ OK ]
```

Tester le support de sauvegarde

Pour tester le support de sauvegarde USB local ou SMB, il est possible d'utiliser le script `bareosmount.py`.

```
root@scribe:~# bareosmount.py -t
Test de montage OK
root@scribe:~#
```

```
root@scribe:~# bareosmount.py -t
Problème de montage (1 essais restants)
ERREUR : périphérique /dev/sda1 non reconnu
Problème de montage (0 essais restants)
ERREUR : périphérique /dev/sda1 non reconnu
Échec du test de montage :
point de montage : Erreur
permissions : Erreur
montage : Erreur
root@scribe:~#
```

```
root@scribe:~# bareosmount.py -t
Problème de montage (1 essais restants)
[Errno 32] mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

Problème de montage (0 essais restants)
[Errno 32] mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Échec du test de montage :
point de montage : Erreur
permissions : Erreur
montage : Erreur
root@scribe:~#
```

4.7.2. Base de donnée sqlite de Bareos irrécupérable

Lors d'un incident sur l'un des modules EOLE la base de donnée sqlite de Bareos peut être irrécupérable.

Il est possible de restaurer des données sans la base de données avec les commandes `bls` et `bextract`.

Inspiré de l'article suivant : https://pipposan.wordpress.com/2010/06/09/bacula-tape-restore-without-database/



Il est également possible de réaliser la récupération avec la commande `bconsole`.

Montage du support de sauvegarde et affichage des volumes par date

La commande `ls -lrt` permet de trier l'affichage des volumes par date :

```
root@srv-scribe:~# ls -lrt /mnt/sauvegardes/
```

On voit une sauvegarde FULL le 06/06/2015 (de nombreux volumes de 2Go ont la même date) :

```
-rw-r----- 1 bareos root 1999997379 2015-06-06 02:02 ScribeVolume0044
-rw-r----- 1 bareos root 1999936662 2015-06-06 02:05 ScribeVolume0068
-rw-r----- 1 bareos root 1999936707 2015-06-06 02:09 ScribeVolume0045
[...]
-rw-r----- 1 bareos root 1999936658 2015-06-06 04:34 ScribeVolume-0241
-rw-r----- 1 root root 1999936613 2015-06-06 04:38 ScribeVolume-0302
```

Utilisation de la commande bsl

```
root@srv-scribe:~# bls -j -V ScribeVolume0044 /mnt/sauvegardes
bls: butil.c:282 Using device: "/mnt/sauvegardes" for reading.
15-jun 16:38 bls JobId 0: Prêt à lire les données du volume « ScribeVolume0044 » depuis le device "FileStorage" (/mnt/sauvegardes).
Volume Record: File:blk=0:208 SessId=103 SessTime=1427205136 JobId=1 DataLen=173
End Job Session Record: File:blk=0:603258940 SessId=103 SessTime=1427205136 JobId=3381
Date=03-jun-2015 02:08:39 Level=I Type=B Files=13,342 Bytes=752,617,191 Errors=0 Status=T
Begin Job Session Record: File:blk=0:603259372 SessId=104
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
SessTime=1427205136 JobId=3382
Job=BackupCatalog.2015-06-03_02.00.00_48 Date=03-jun-2015 02:12:24 Level=I Type=B
End Job Session Record: File:blk=0:60359372 SessId=104 SessTime=1427205136 JobId=3382
Date=03-jun-2015 02:12:24 Level=I Type=B Files=0 Bytes=0 Errors=0 Status=T
[...]
Begin Job Session Record: File:blk=0:1308041742 SessId=109 SessTime=1427205136 JobId=3387
Job=Complet.2015-06-06_02.00.00_53 Date=06-jun-2015 02:00:12 Level=F Type=B
15-jun 15:54 bls JobId 0: Fin de Volume au fichier 0 sur le Device "FileStorage" (/mnt/sauvegardes), Volume « ScribeVolume0044 »
15-jun 15:54 bls JobId 0: Fin de tous les Volumes.
```

Le Job du 06/06/2015 a SessId=109 et SessTime=1427205136. Ainsi que le Job du dernier volume en date du 06/06/2015

```
root@srv-scribe:~# bls -j -V ScribeVolume-0302 /mnt/sauvegardes
bls: butil.c:282 Using device: "/mnt/sauvegardes" for reading.
15-jun 15:59 bls JobId 0: Prêt à lire les données du volume « ScribeVolume-0302 » depuis le device "FileStorage" (/mnt/sauvegardes).
Volume Record: File:blk=0:209 SessId=109 SessTime=1427205136 JobId=33 DataLen=174
15-jun 16:00 bls JobId 0: Fin de Volume au fichier 0 sur le Device "FileStorage" (/mnt/sauvegardes), Volume « ScribeVolume-0302 »
15-jun 16:00 bls JobId 0: Fin de tous les Volumes.
```

Génération d'un fichier bootstrap avec la liste des volumes à utiliser (tous ceux du 06/06/2015)

```
root@srv-scribe:~# cat boostrap.bsr
Volume="ScribeVolume0044"
VolSessionId=109
VolSessionTime=1427205136
Volume="ScribeVolume0068"
VolSessionId=109
VolSessionTime=1427205136
Volume="ScribeVolume0045"
VolSessionId=109
VolSessionTime=1427205136
[...]
Volume="ScribeVolume-0302"
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
VolSessionId=109
VolSessionTime=1427205136
```

Restauration

```
root@srv-scribe:~# root 15133 15119 25 16:26 pts/5 00:07:31 bextract -b boostrap.bsr /mnt/sauvegardes /home/restore/
```

Restauration LDAP

```
root@srv-scribe:~# service slapd stop
root@srv-scribe:~# md /home/sav/ldap
root@srv-scribe:~# mv /var/lib/ldap/*.* /home/sav/ldap/
root@srv-scribe:~# slapadd -l /home/sauv_ldap.ldif
```

Restauration MySQL

```
root@srv-scribe:~# mysql_pwd.py eole21 nomodif
root@srv-scribe:~# mysql -uroot -peole21 < /home/sauv_mysql.sql
```

Restauration Quotas

```
root@srv-scribe:~# bareosrestore.py --quota
```

Restauration SID

```
root@srv-scribe:~# cat /etc/eole/${MODULE}_SID | xargs net setlocalsid
```

Reconfiguration du serveur

Il faut procéder à la reconfiguration du serveur à l'aide de la commande `reconfigure`.

4.8. Annexes

Voici un complément d'information (outils d'administration, liens, ...) pour aller plus loin avec Bareos.

4.8.1. Autres outils d'administration pour Bareos

L'administration de Bareos se fait au travers d'une **console** (texte ou graphique), qui pourra être installée sur le même serveur que le directeur (**Director**), mais aussi sur d'autres postes pour permettre de commander Bareos à distance.

Différentes versions existent :

- **bconsole** est la console en mode texte ;
- **Bareos Administration Tool** (BAT) est l'interface graphique standard qui permet d'exploiter bconsole, installable (25Mo) sur les modules EOLE avec la commande :

  `# apt-eole install bareos-bat`

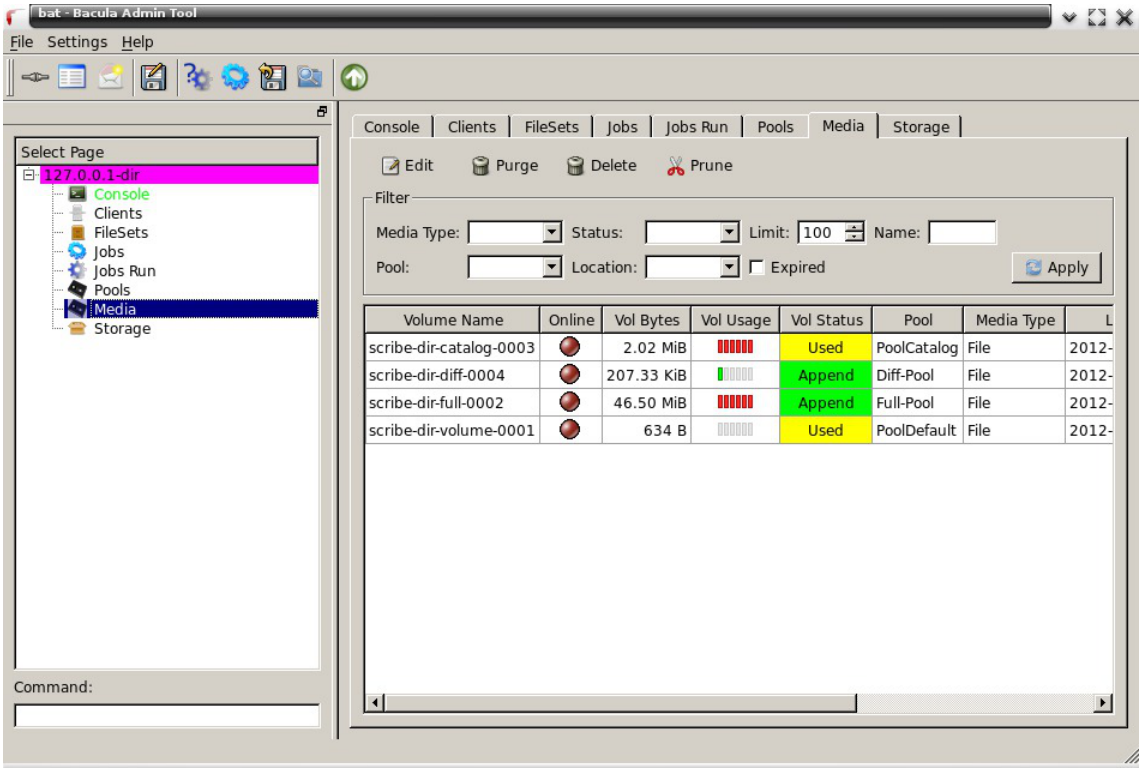
  BAT se lance avec la commande suivante :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# bat -c /etc/bareos/bat.conf
```

Il est possible de lancer l'interface BAT à travers SSH avec l'option -X pour activer le déport de l'affichage et l'option -C pour éventuellement compresser les données (pratique pour les lignes à faible débit) :

```
# ssh -C -X <adresse_serveur>
```



BAT (Bacula Administration Tool)

- **bgnome-console** est une console graphique (notamment pour les opérations de restauration), mais nécessite l'installation des librairies GNOME 2.x ;
- **bwx-console** est une version graphique utilisant wxWidgets

  L'installation de bwx-console est décrite pour Mandriva et pour Ubuntu à l'adresse suivante : http://m-k.cc/spip.php?rubrique3
- **bacula-win** (http://sourceforge.net/projects/bacula/files/) permet notamment d'installer :
  - un client Windows (File Daemon) ;
  - des consoles : BAT, bconsole et TrayMonitor.

Il existe aussi des versions Web comme :

- **bacula-web** écrit en PHP :

  http://www.bacula-web.org/
- ou **bweb** écrit en perl :

  http://bacula.svn.sourceforge.net/viewvc/bacula/trunk/gui-old/bweb/

Pour avoir plus d'informations sur les outils mentionnés : http://wiki.bacula.org/doku.php?id=3rd_party_addons

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.8.2. Quelques références

Voici quelques références autour de Bareos et des sauvegardes.

- Définition de la sauvegarde : http://fr.wikipedia.org/wiki/Sauvegarde
- Le site officiel de Bareos : http://www.bareos.org
  - L'accès à la documentation en HTML mais aussi en PDF : http://www.bareos.org/en/documentation.html
  - Tutoriel : http://www.bareos.org/en/HOWTO.html
  - Manuel utilisateur : http://www.bareos.org/en/manual/articles/manual.html

Définition des éléments de sauvegarde Bareos :

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-60001.3

4.8.3. Un répertoire partagé Windows 7 comme support de sauvegarde

Les modules EOLE permettent d'utiliser plusieurs supports pour effectuer les sauvegardes, dont un répertoire partagé.

Pour la sauvegarde, les accès au partage doivent impérativement se faire en utilisant un compte local du poste sur lequel se trouve le dossier partagé.

Donner des droits d'accès au partage à un compte du domaine pose un problème pour le bon déroulement des sauvegardes. En effet pour avoir accès au partage, la station va vérifier la validité de l'utilisateur et de son mot de passe auprès du contrôleur de domaine mais le service Samba est arrêté par Bareos pour éviter qu'un fichier/dossier ne soit modifié pendant la sauvegarde. L'accès au partage n'est donc pas validé par le contrôleur de domaine et la sauvegarde ne peut pas se faire.

Voici comment créer un partage avec les droits d'accès adéquats sur un poste équipé de Windows Seven.

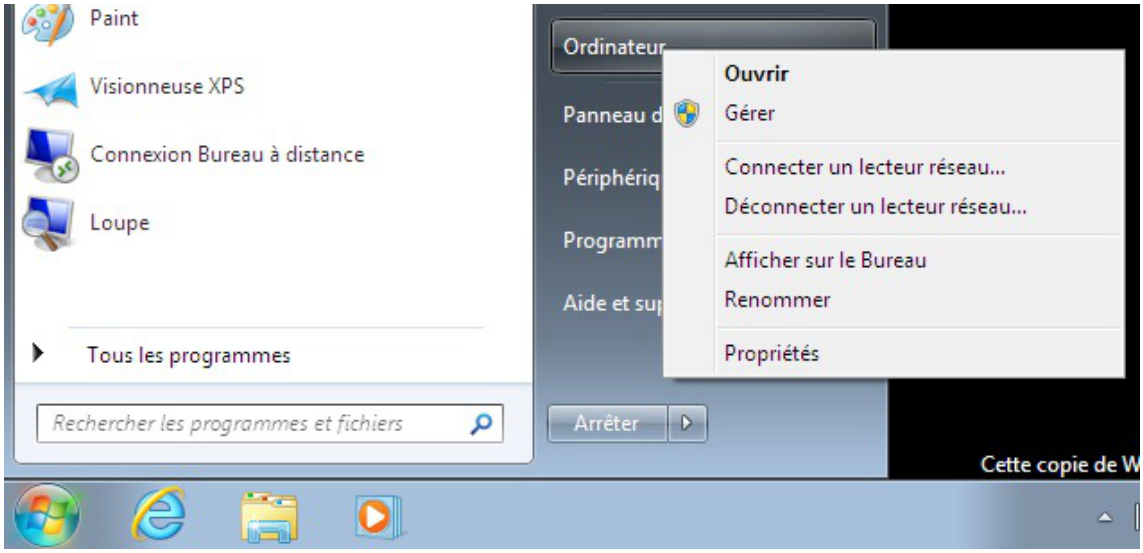
Le dossier partagé peut se trouver sur le disque dur de la station Windows mais il peut aussi se trouver sur un disque dur externe connecté à la station.

Création d'un compte dédié sur le poste Windows 7

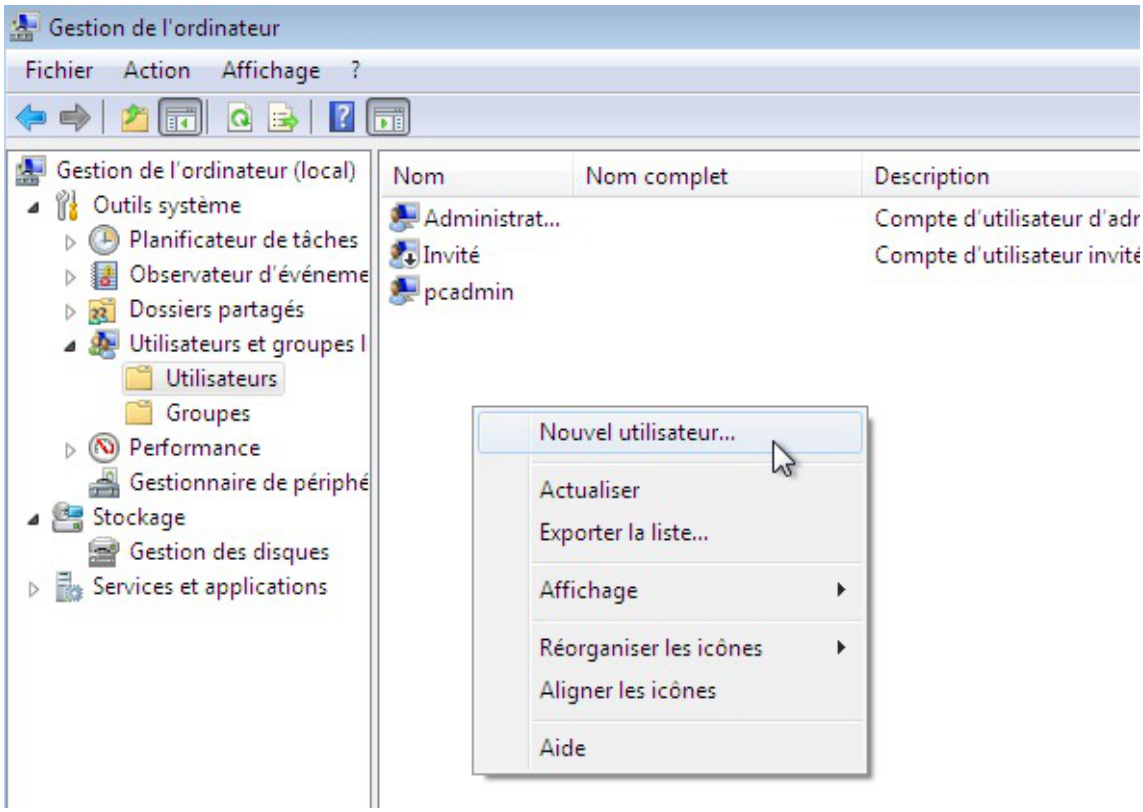
Ouvrir une session en administrateur local de la station sur laquelle vous voulez créer le partage.

Puis ouvrir la console de **Gestion de l'ordinateur** : Menu démarrer → Ordinateur → clic droit Gérer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

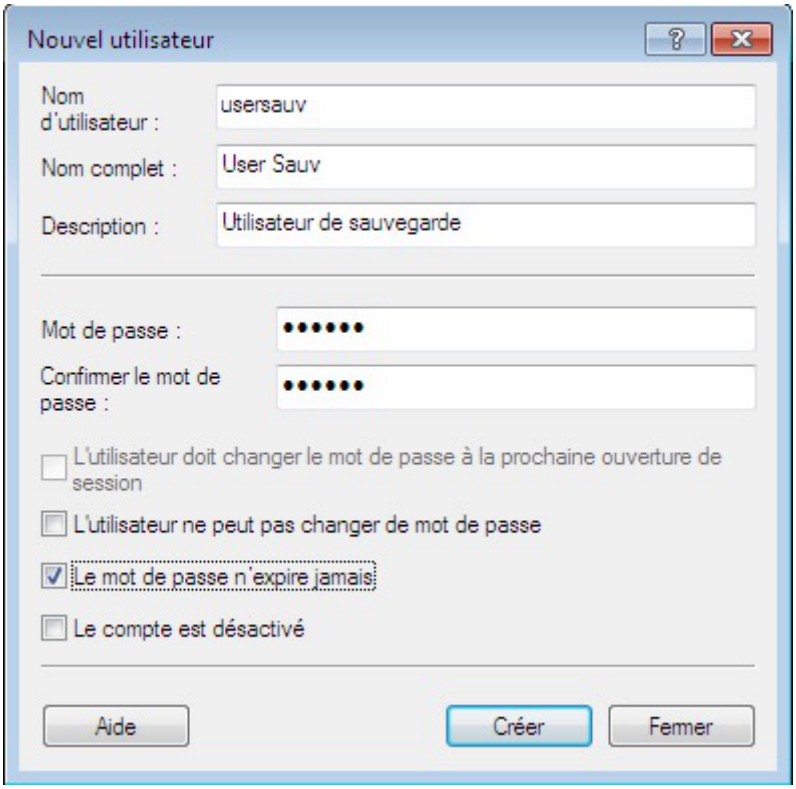


Aller dans le menu : Outils système → Utilisateurs et groupes locaux → Utilisateurs, puis effectuer un clic droit dans l'espace vide.



Configurer l'utilisateur comme ceci :

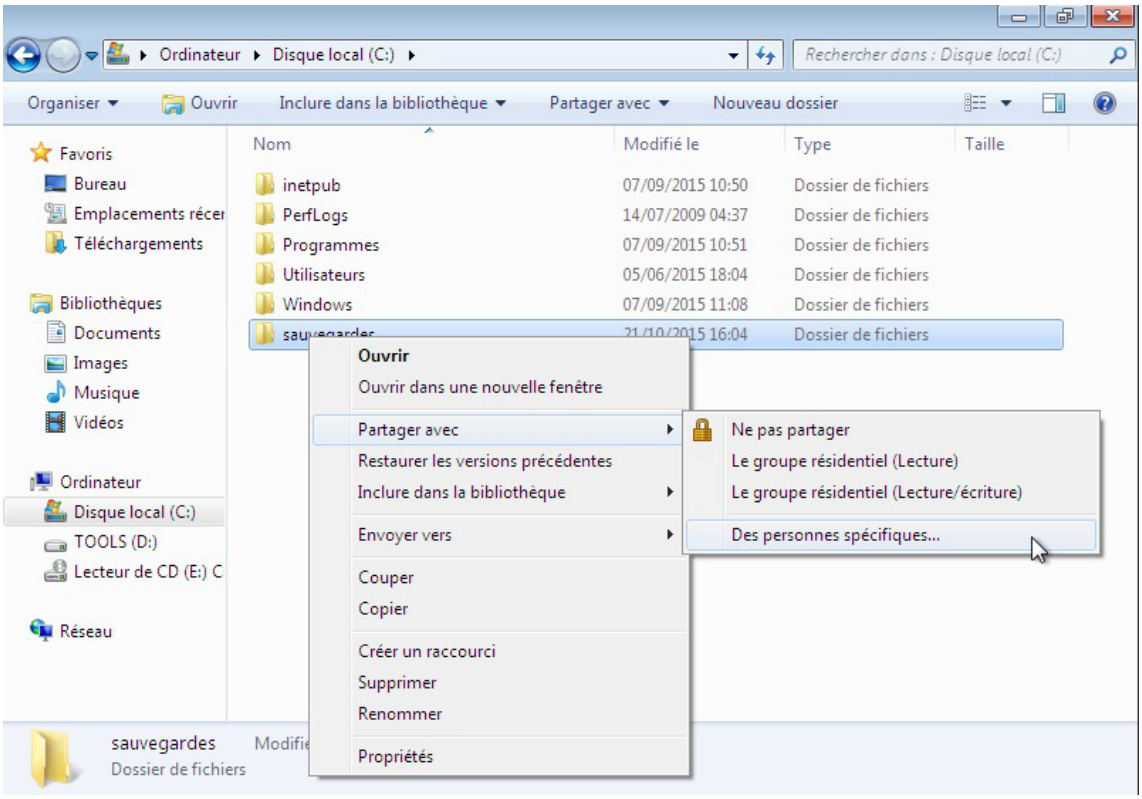
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Finaliser l'opération en cliquant sur le bouton `Créer`.

Partage du dossier et réglage des droits d'accès

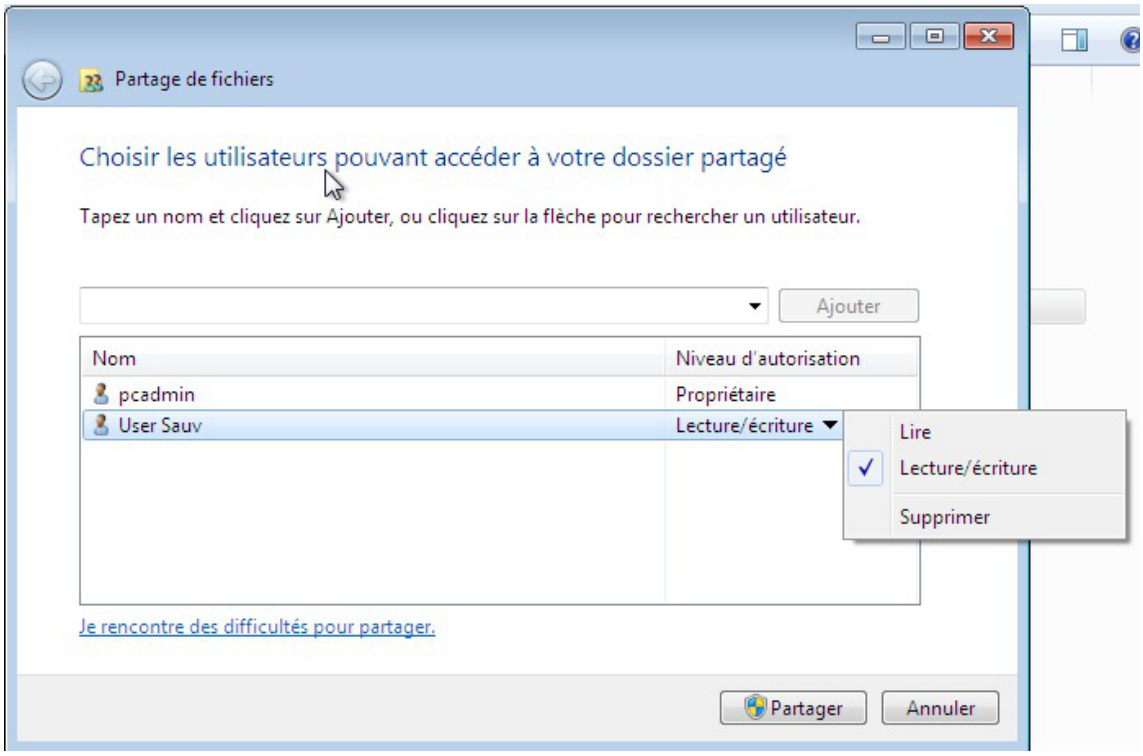
Après avoir créé un dossier `sauvegardes` à l'emplacement de votre choix, effectuer un clic droit sur le dossier et sélectionner `Partager avec` puis `Des personnes spécifiques...`



Entrer le nom de l'utilisateur créé précédemment et cliquer sur le bouton `Ajouter`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Lui donner les droits en Lecture/écriture.



Finaliser l'opération en cliquant sur le bouton Partager.

L'interface propose une liste déroulante pour la sélection des utilisateurs spécifiques. Elle affiche le **nom complet** alors qu'il faut fournir le **nom d'utilisateur**.

En cas d'erreur du type *Windows n'a pas pu trouver <utilisateur>*, vérifier que le nom saisi correspond bien au **nom d'utilisateur**.

4.8.4. Un répertoire partagé Windows XP comme support de sauvegarde

Les modules EOLE permettent d'utiliser plusieurs supports pour effectuer les sauvegardes, dont un répertoire partagé.

Pour la sauvegarde, les accès au partage doivent impérativement se faire en utilisant un compte local du poste sur lequel se trouve le dossier partagé.

Donner des droits d'accès au partage à un compte du domaine pose un problème pour le bon déroulement des sauvegardes. En effet pour avoir accès au partage, la station va vérifier la validité de l'utilisateur et de son mot de passe auprès du contrôleur de domaine mais le service Samba est arrêté par Bareos pour éviter qu'un fichier/dossier ne soit modifié pendant la sauvegarde. L'accès au partage n'est donc pas validé par le contrôleur de domaine et la sauvegarde ne peut pas se faire.

Voici comment créer un partage avec les droits d'accès adéquats sur un poste équipé de Windows XP.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

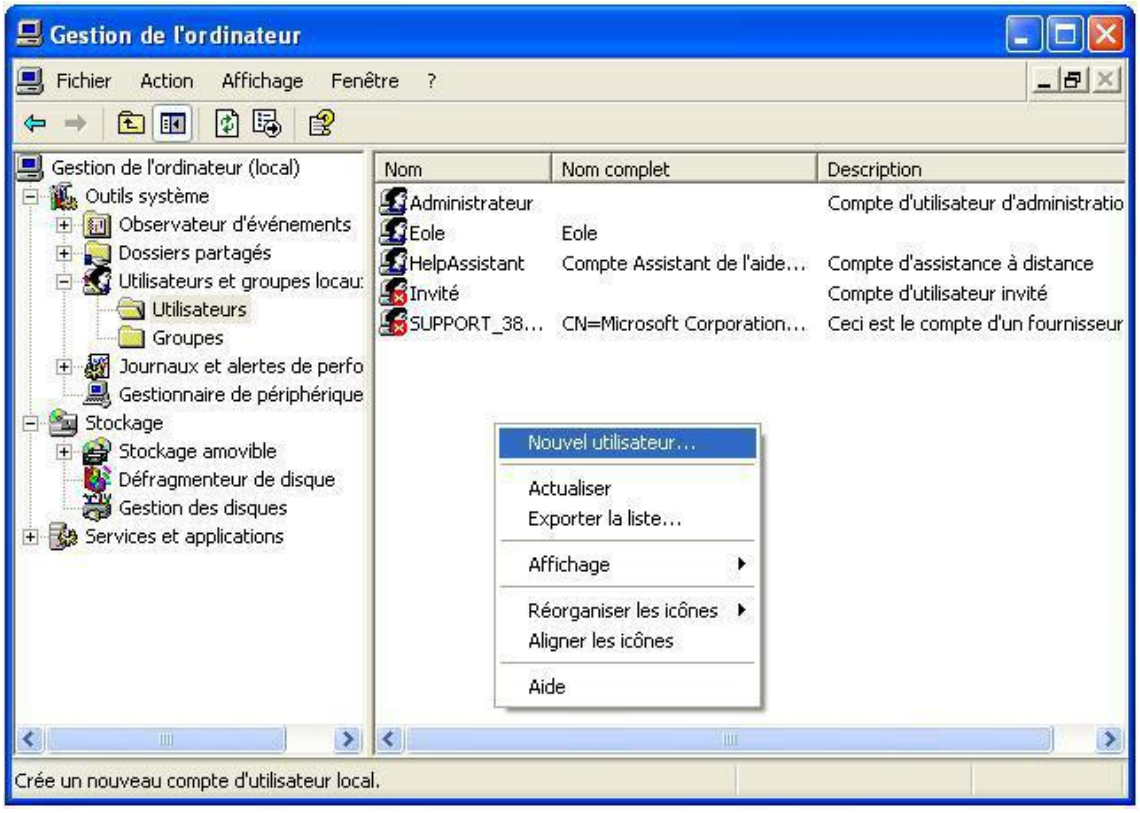
Le dossier partagé peut se trouver sur le disque dur de la station Windows mais il peut aussi se trouver sur un disque dur externe connecté à la station.

Création d'un compte sur le poste Windows XP

Ouvrez une session en administrateur local de la station sur laquelle vous voulez créer le partage. Puis ouvrez la console de **Gestion de l'ordinateur**.

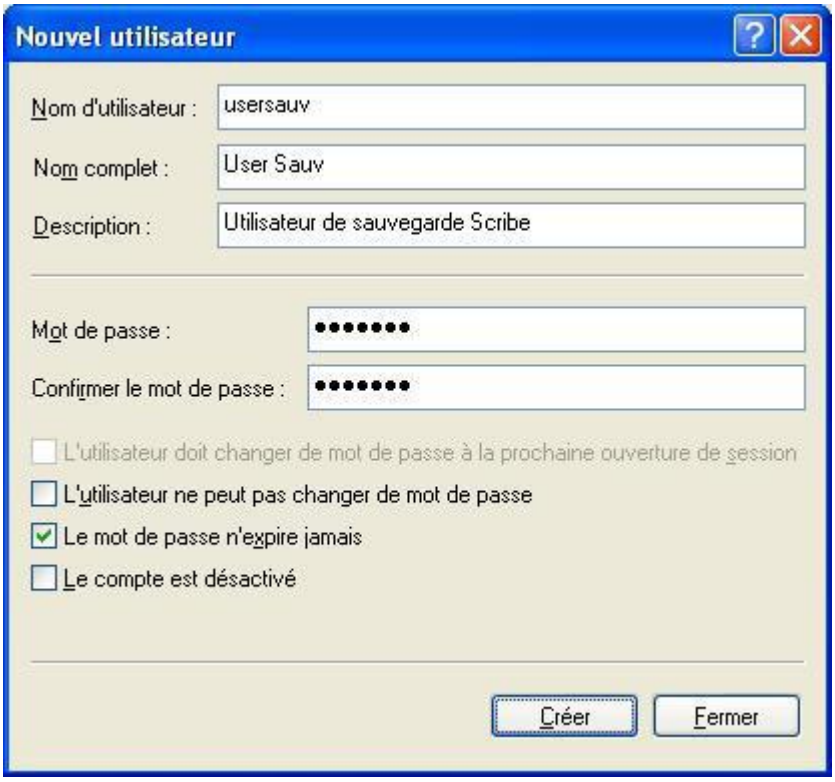


Ensuite, créez un nouvel utilisateur : Menu "**Action**" ou clic droit dans l'espace vide de la colonne de droite.



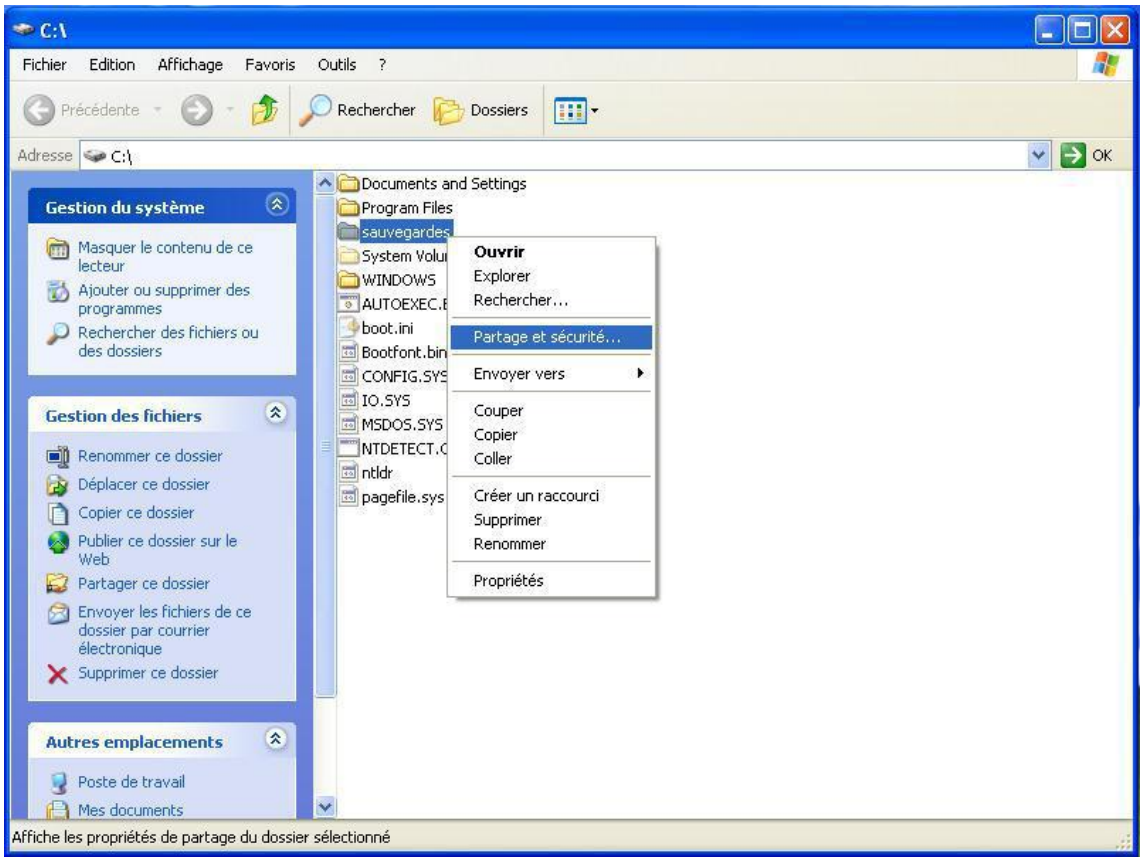
... avec les options configurées.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



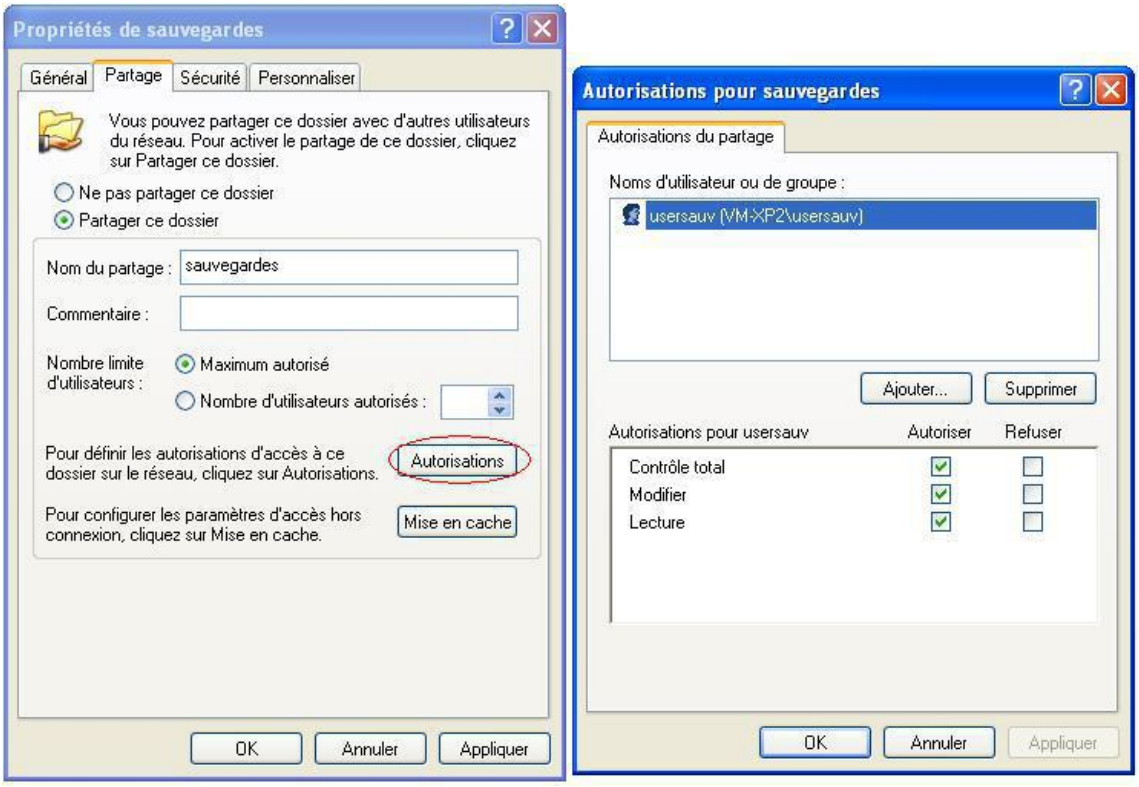
Partage du dossier et réglage des droits d'accès

Après avoir créé un dossier "*sauvegardes*" à l'emplacement de votre choix, partagez-le à l'aide d'un clic droit sur le dossier.

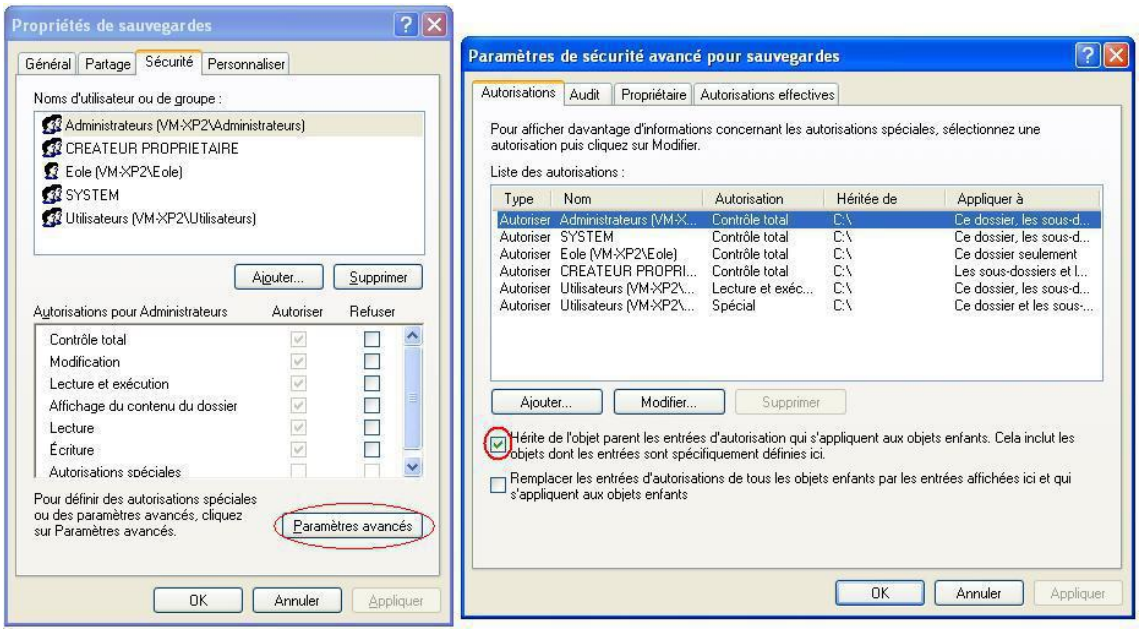


Puis cliquez sur **Autorisations**. Supprimez les autorisations par défaut ("*Tout le monde*") puis ajoutez "*usersauv*" avec "**Contrôle total**".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

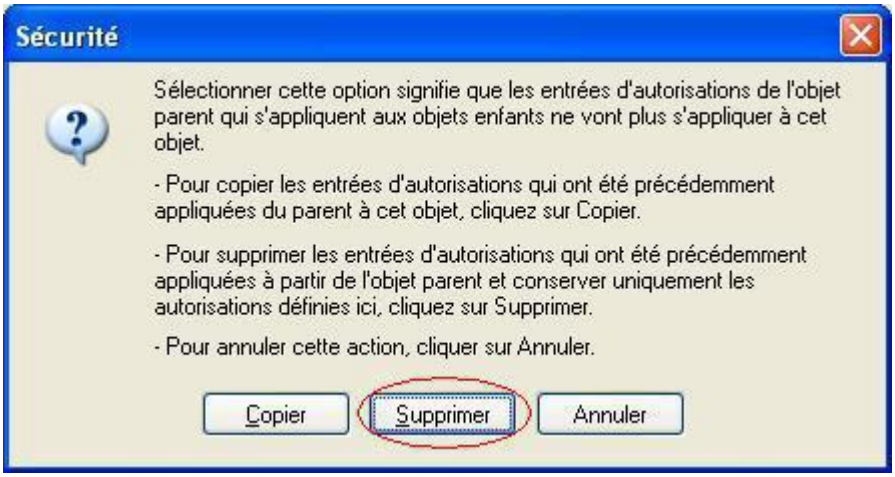


Fermez la fenêtre des autorisations puis allez dans l'onglet "**Sécurité**" et cliquez sur "**Paramètres avancés**".



Décochez "**Hérite de l'objet parent...**", une fenêtre s'ouvre alors, sélectionnez "**Supprimer**".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

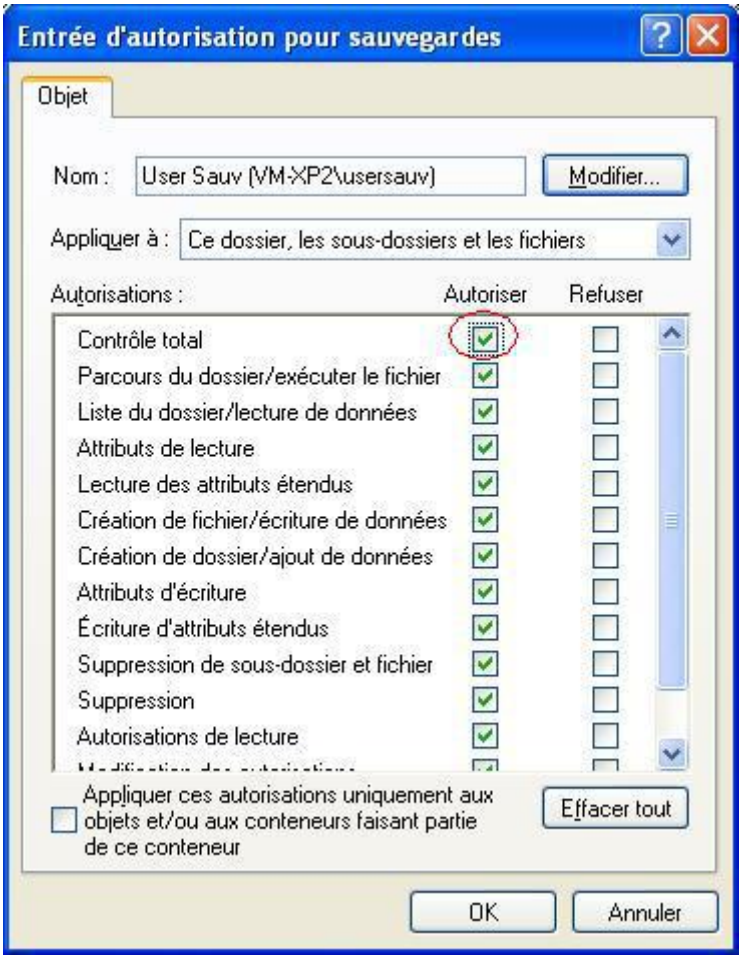


Ajoutez ensuite l'utilisateur "*usersauv*" toujours avec le "**Contrôle total**".



Enfin, affectez le "**Contrôle total**".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



5. Les imprimantes

Il y a plusieurs façon de gérer les imprimantes dans un établissement.

Il est possible :

- de partager les imprimantes sur les postes utilisateurs ;
- de passer par des serveurs d'impression ;
- ou d'utiliser le module EOLE comme serveur d'impression.

Nous ne traiterons ici que de cas où le module EOLE sert de serveur d'impression avec CUPS[p.758].

Deux interfaces sont disponibles pour gérer les imprimantes :

- l'interface simplifiée intégrée à l'EAD (gestion) ;
- l'interface de gestion CUPS (gestion et installation/configuration).

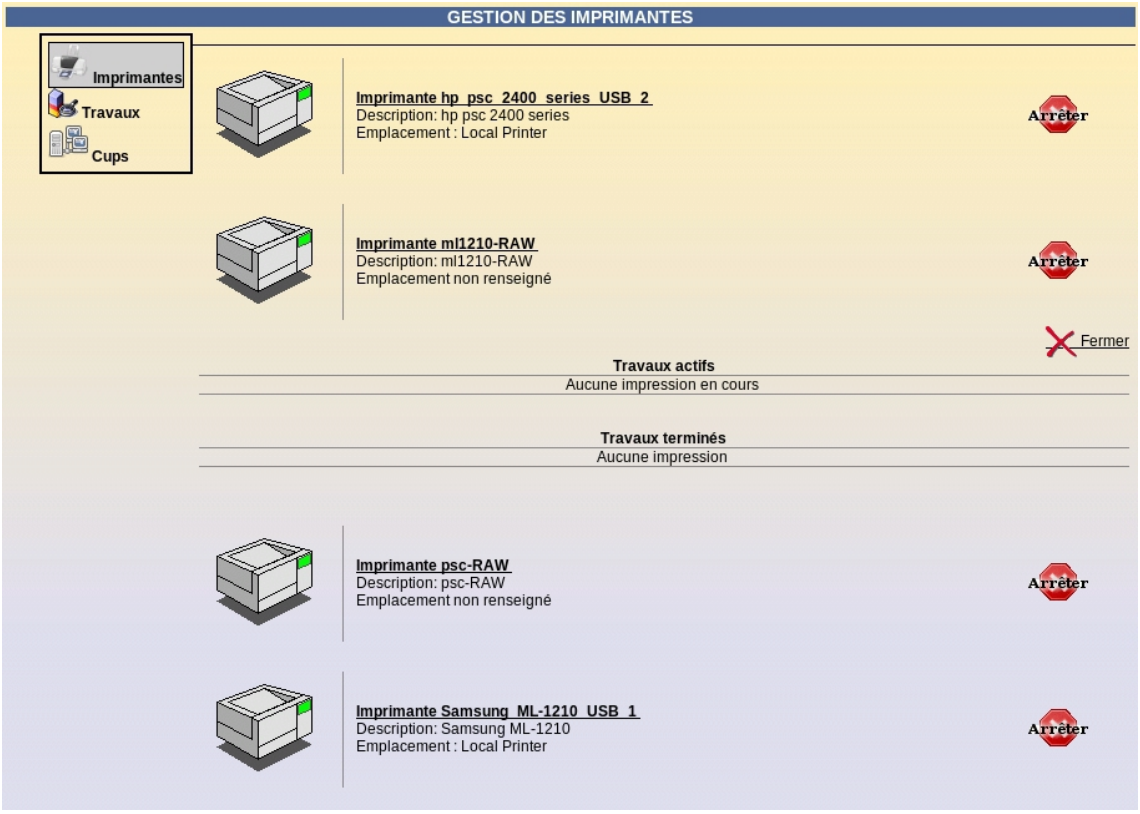
5.1. L'interface simplifiée

L'interface de gestion des imprimantes intégrée à l'EAD permet de gérer les imprimantes déjà installées.

L'administrateur et les enseignants peuvent :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- consulter l'état des imprimantes ;
- consulter/interrompre/relancer les travaux d'impression ;
- arrêter/démarrer des imprimantes.



5.2. L'interface de gestion CUPS

CUPS (Common UNIX Printing System) est le serveur d'impression libre intégré à la solution EOLE.

https://www.cups.org/

CUPS fournit une interface web pour faciliter l'installation et la gestion des imprimantes sur le serveur.

Cette interface est totalement accessible aux utilisateurs *root*, *admin* et aux utilisateurs du goupe *PrintOperators*. Sur le module Scribe, elle est en accès restreint pour les professeurs, identique à celle proposées dans l'interface simplifiée de l'EAD.

https://<adresse_serveur>:631 [https://<adresse_serveur>:631/]

5.2.1. Création de l'imprimante

5.2.1.a. Ajouter une nouvelle imprimante

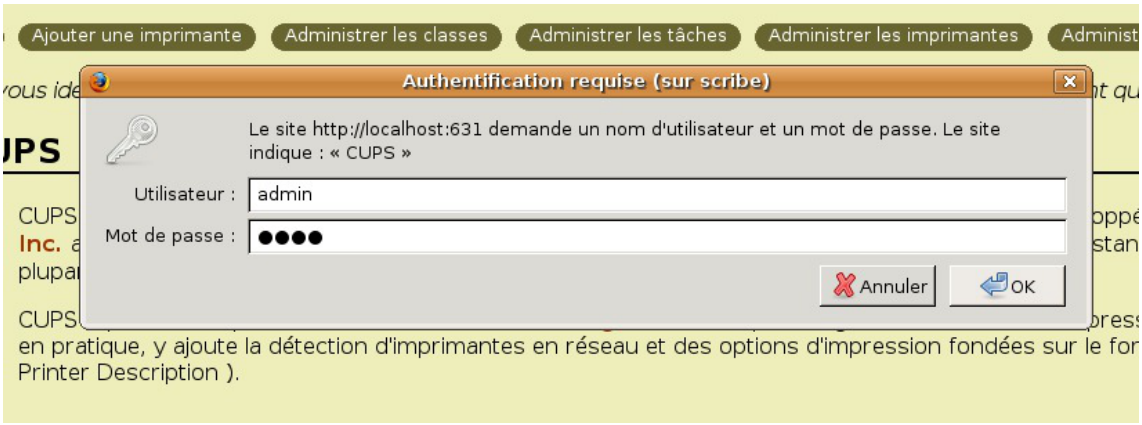
Dans l'EAD, le menu `Imprimantes/Imprimantes/CUPS` ouvre l'interface de configuration CUPS dans une nouvelle fenêtre.

Cliquer dans la fenêtre le bouton `ajouter une imprimante`.

Il est nécessaire de s'identifier avec un utilisateur *root*, *<nom du module>*, *admin* ou appartenant au

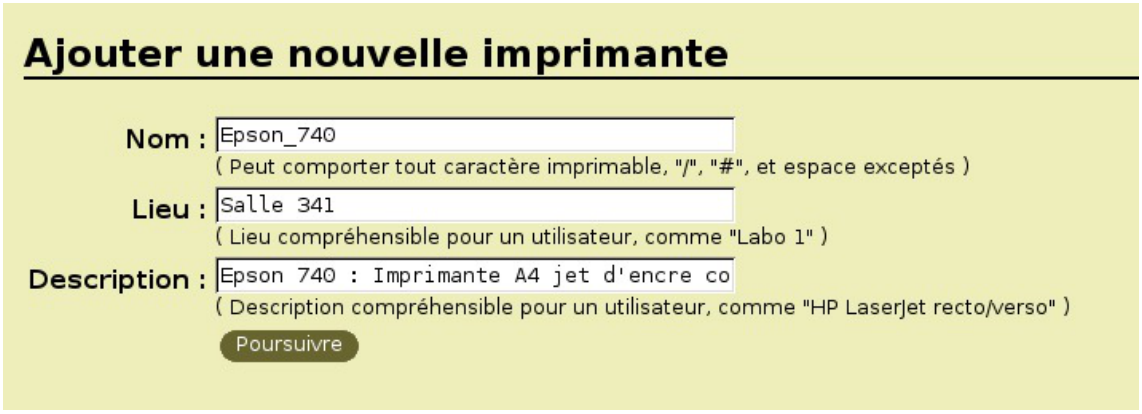
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

groupe *PrintOperators*.



Ajouter une imprimante CUPS

Il suffit alors d'indiquer un nom (généralement le nom de l'imprimante), un lieu (généralement le nom de la salle) et une description (généralement les caractéristiques de l'imprimante : A4, recto-verso, noir et blanc/couleur...). Puis cliquer sur poursuivre.



Description de la nouvelle imprimante CUPS

5.2.1.b. Choix du matériel

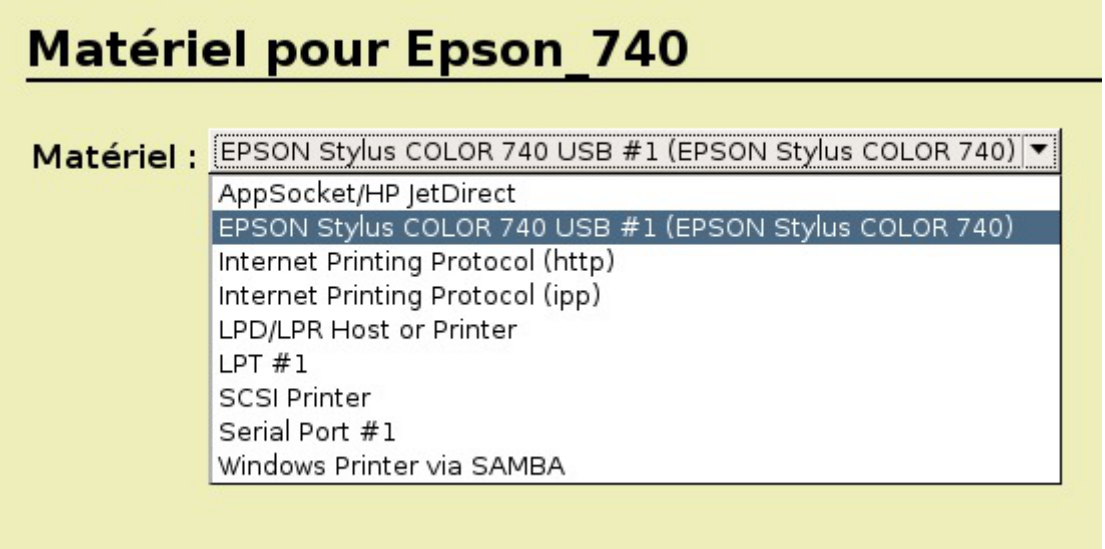
Il y a trois grands types d'imprimantes :

- les imprimantes locales (avec un port USB, parallèle, ...) ;
- les imprimantes réseaux ;
- les imprimantes partagées sur un poste client Windows.

> Les imprimantes locales

Seules les imprimantes USB sont reconnues directement par le système. Pour les imprimantes sur le port parallèle, le port série, le port SCSI, il suffit de choisir le "matériel" correspondant et de le configurer. Consulter la documentation CUPS en cas de doute.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Matériel pour une imprimante locale CUPS

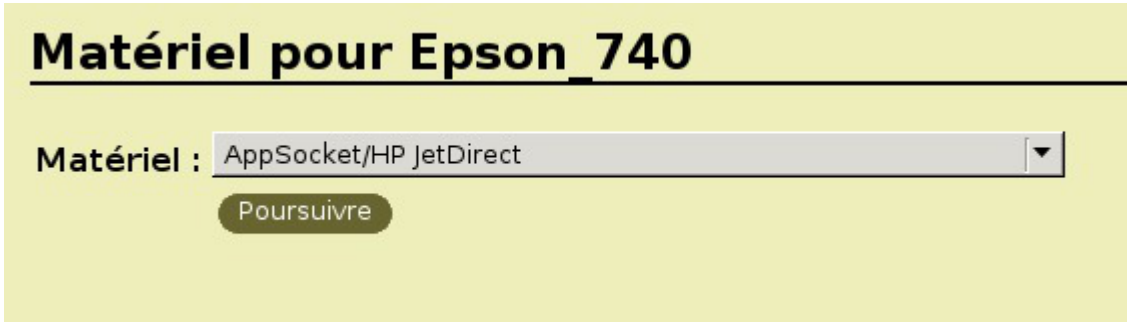
> Les imprimantes réseaux

Il existe un grand nombres de protocoles réseaux pour les imprimantes : AppSocket/HP JetDirect, Internet Printing Protocol (HTTP ou IPP). Généralement, les imprimantes réseaux sont capable de faire du JetDirect. En cas de doute, se reporter à la documentation de l'imprimante.

Imprimante compatible JetDirect

Choisir le matériel "*AppSocket/HP JetDirect*" et poursuivre. Indiquer ensuite une *URI du matériel* du type :

`socket://192.168.230.123:9100`



Matériel pour une imprimante réseau CUPS

> Les imprimantes partagées sur un poste client Windows

Création d'un partage d'imprimante sous Windows XP

Nous partons du principe que l'imprimante est fonctionnelle sur le système d'exploitation propriétaire Windows.

Il est possible d'accéder directement à l'imprimante du poste sans passer par le serveur. Cette documentation ne traite pas de ce cas.

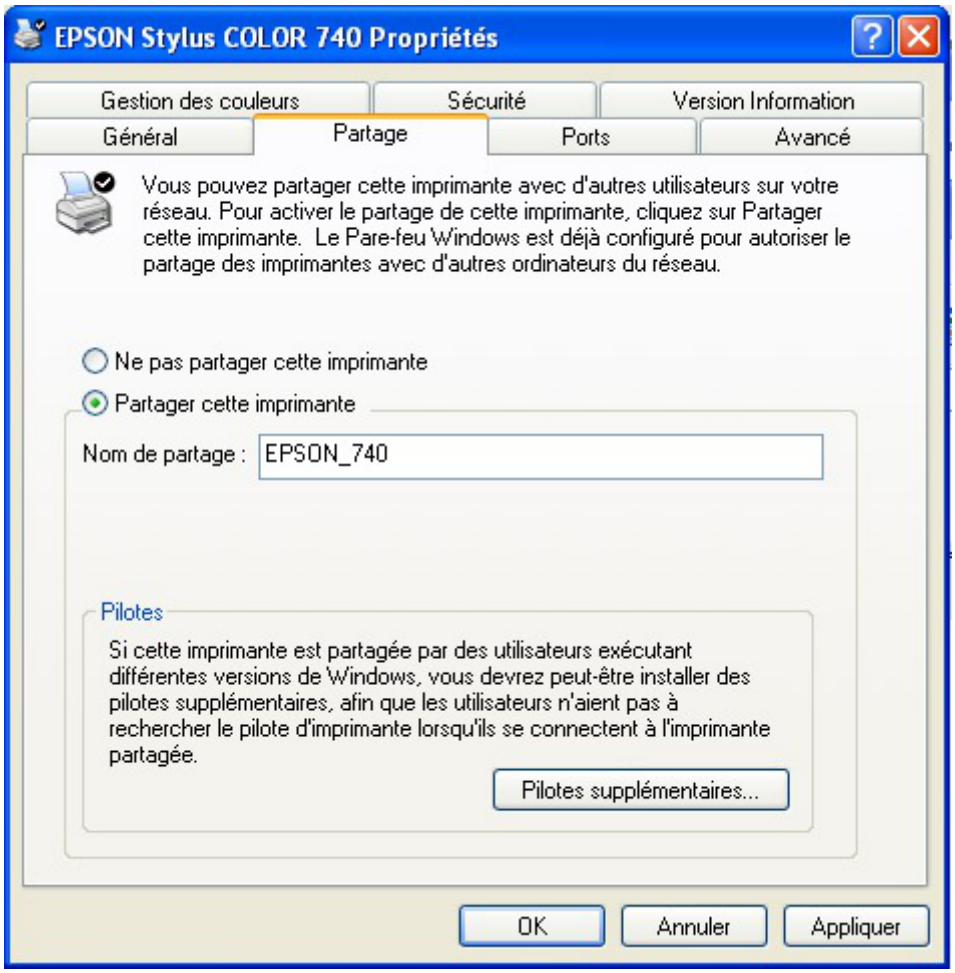
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Dans le menu Windows `Démarrer/Imprimantes et télécopieurs` cliquer droit sur votre imprimante et choisir `Partager...`.



Partager une imprimante sous Windows

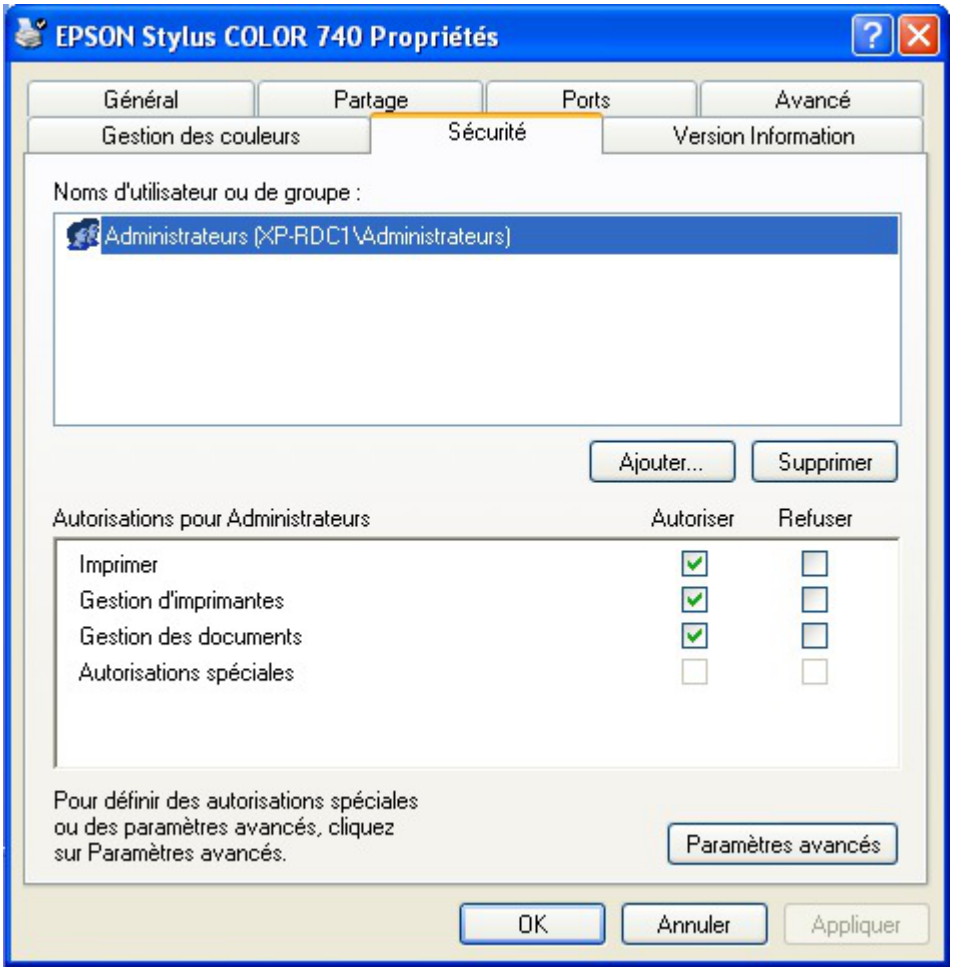
Il suffit alors de cocher `◉ partager cette imprimante` et de donner un *Nom de partage*.



Partager cette imprimante Windows

Enfin, dans l'onglet `Sécurité`, supprimer toutes les autorisations aux autres groupes et utilisateurs que *Administrateurs*. Ce groupe devant avoir toutes les autorisations.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Choix des droits du partage de l'imprimante Windows

Configuration de CUPS

Il suffit de sélectionner le matériel "*Windows Printer via Samba*" et `poursuivre`.

L'URI du matériel est du type :

`smb://admin:motdepasse@xp-rdc1/Epson_740`



Matériel pour une imprimante CUPS partagé sous Windows

Lors de la modification de l'imprimante, l'URI n'affichera plus le nom de l'utilisateur ni le mot de passe. Il sera nécessaire de le re-indiquer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

5.2.2. Choix du pilote

Il existe deux catégories de choix pour les pilotes d'impression.

- utilisation du pilote client Windows ;
- utilisation du pilote CUPS.

5.2.2.a. Avantages et inconvénients des solutions

Le pilote client est plus compliqué à mettre en place et diffère suivant les constructeurs. Par contre, le pilote est parfois plus complet que la version serveur. Cette solution ne concerne que Windows.

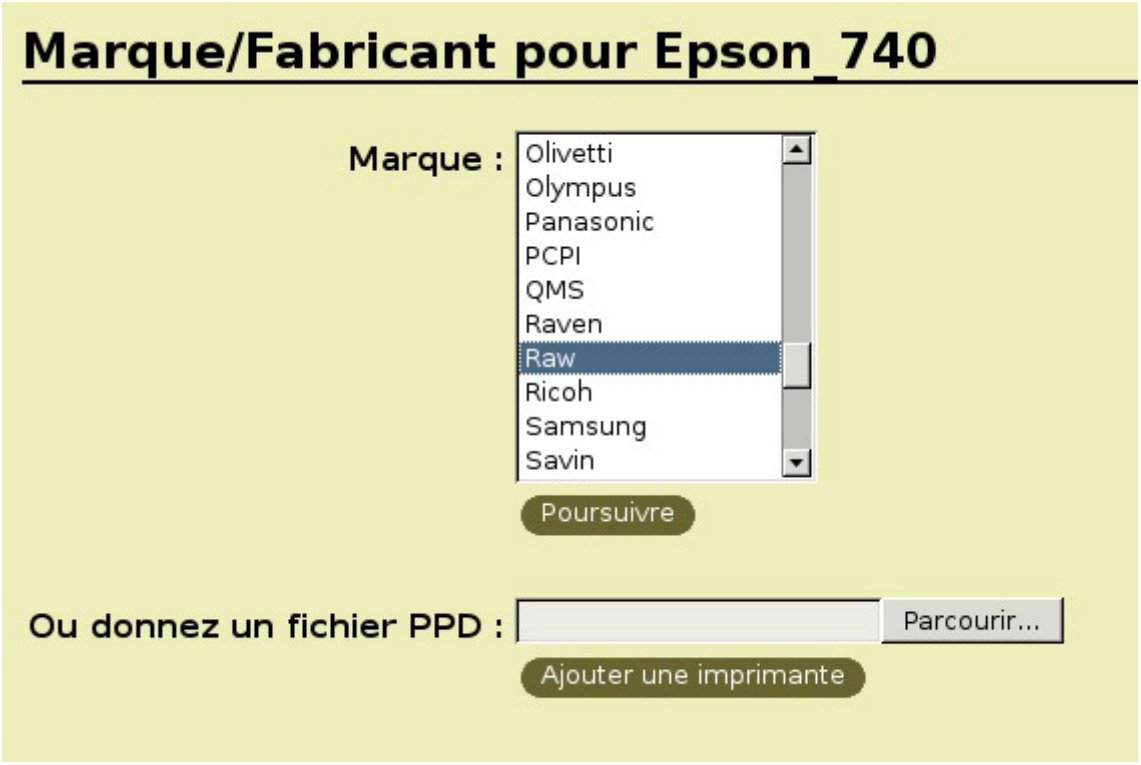
Le pilote CUPS est plus simple à mettre en place. Il est particulièrement adapté aux réseaux hétérogènes. Par contre, les pilotes ne sont souvent pas écrits directement par les constructeurs.

5.2.2.b. Utilisation des pilotes clients Windows

Configuration de CUPS

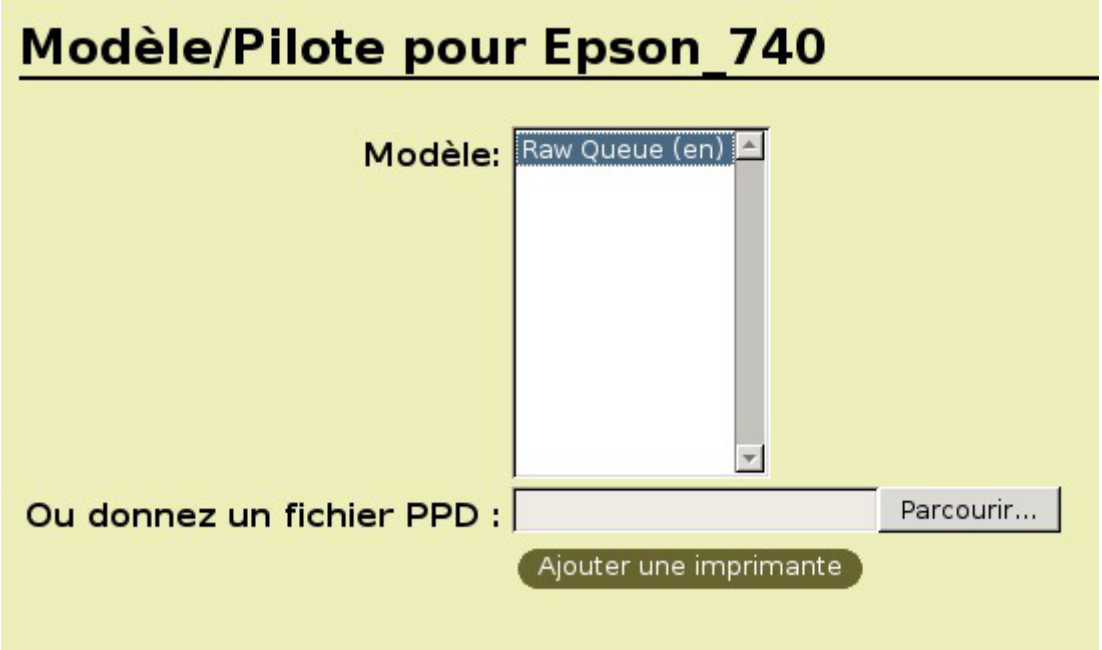
Dans la liste des marques, choisir "*Raw*" quelque soit le modèle de l'imprimante et "*Raw Queue*" comme modèle.

Dans ce cas, CUPS envoie directement les données à l'imprimante sans les traiter.



Driver Raw pour l'imprimante CUPS

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Driver Raw pour l'imprimante CUPS

Installation du pilote Windows

Cette étape est importante. Elle permettra aux différents postes utilisateur de récupérer les pilotes d'impression pour pouvoir imprimer les documents.

L'installation se fera depuis un poste client Windows intégré au domaine. Il faut se munir du pilote fourni par le constructeur de l'imprimante.

Il faut commencer par se connecter à un poste Windows en "*admin*" ou un utilisateur appartenant au groupe *PrintOperators*.

Ensuite, dans un navigateur de fichiers il faut se rendre sur le partage du serveur : `\\<nom du serveur>` puis choisir "*imprimantes et télécopieurs sur ...*".

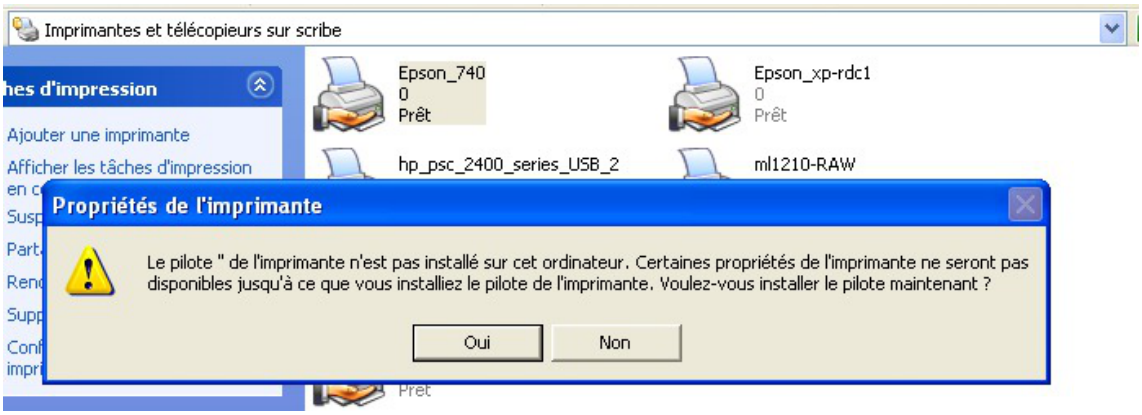
Cliquer droit et choisir `propriétés`.



Propriété de l'imprimante sous Windows

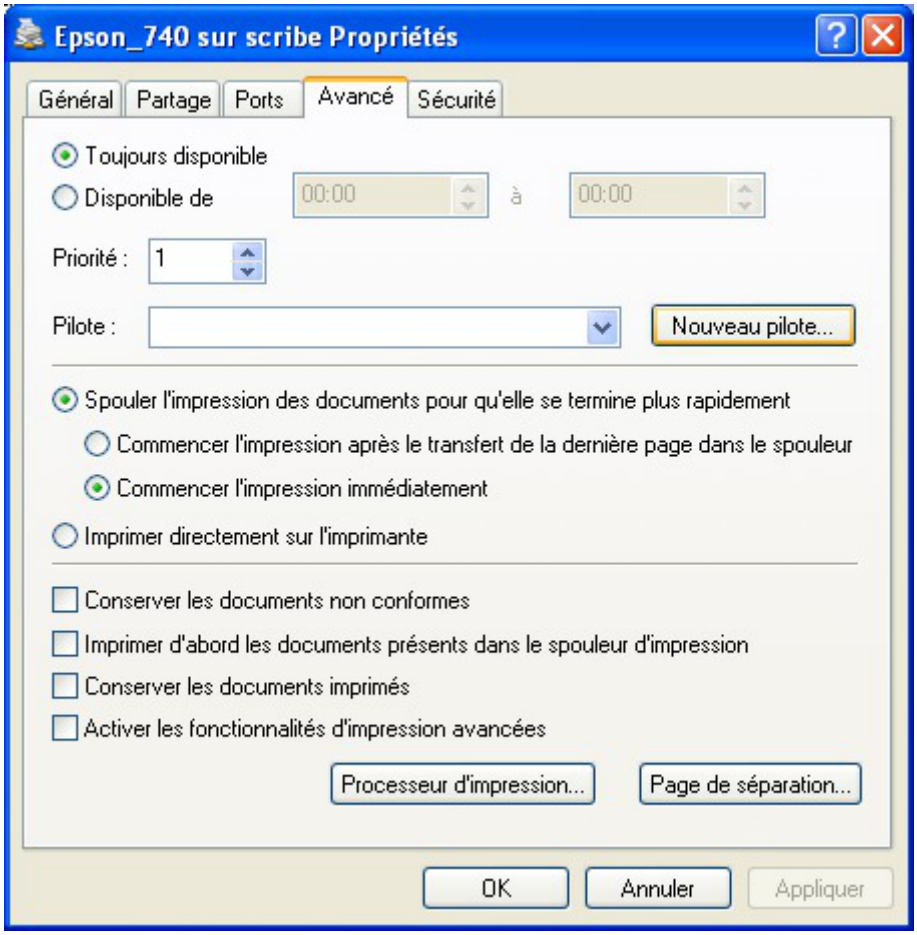
Répondre `non` à la question "*Voulez-vous installer le pilote maintenant*".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Annulation de l'installation des pilotes

Il est alors possible de choisir un pilote déjà présent sur le serveur ou d'installer un nouveau pilote dans l'onglet "*avancé*" dans la section "*pilote*".



Nouveau pilote d'impression Windows

Il se peut que Windows change le nom de l'imprimante à cette étape. Vérifier que le nom correspondent à ce que vous souhaitez.

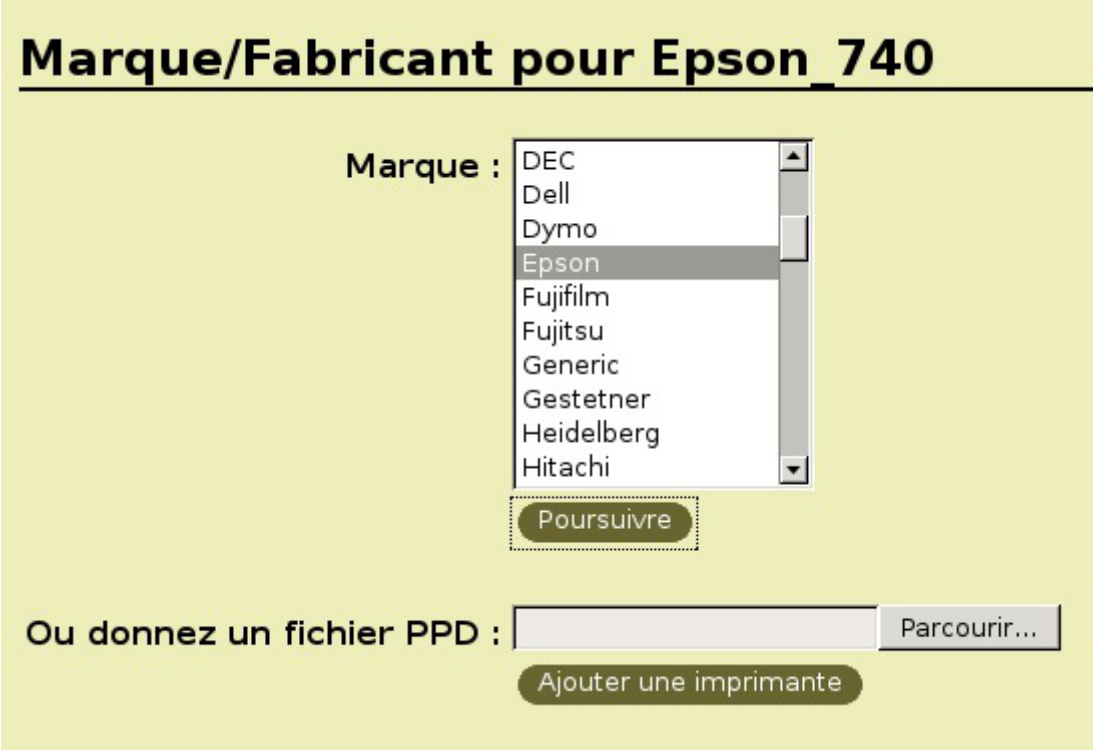
Dans l'onglet "Partage" il est possible d'installer des "Pilotes supplémentaires..." pour les autres versions de Windows.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

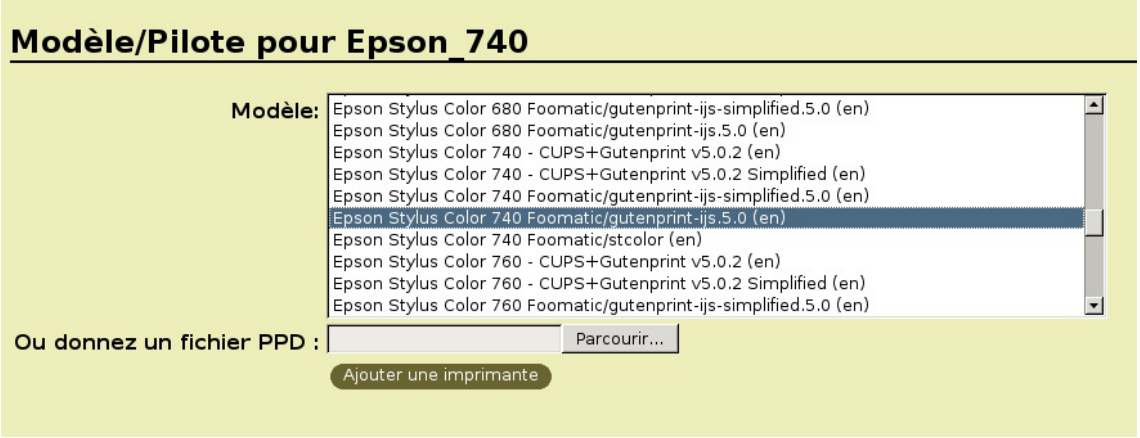
5.2.2.c. Utilisation des pilotes CUPS

Configuration de CUPS

Dans la liste des marques, choisir la marque de votre imprimante, puis cliquer sur poursuivre. Enfin, choisir le modèle de votre imprimante.



Marque/Fabriquant de la nouvelle imprimante CUPS



Modèle/Pilote de l'imprimante CUPS

Si vous ne trouvez pas votre matériel dans la liste par défaut, il est possible de rechercher son imprimante sur le site de CUPS : http://cups.org/ppd.php.

Installation du pilote Windows

Lorsque les pilotes sont installés sur CUPS, il est nécessaire de configurer le poste client avec des pilotes PostScript.

Il existe plusieurs pilotes PostScript. Dans cette documentation nous utiliseront les pilotes PostScript

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Microsoft. Cela ne s'appliquera que pour les versions de Windows supérieurs ou égales à Windows 2000.

Si vous utilisez encore des versions de Windows inférieurs, il vous faudra, par exemple, les pilotes PostScript proposés par l'éditeur Adobe.

Il faut commencé par récupérer les pilotes PostScript Microsoft.

Les pilotes d'impression PostScript Microsoft se trouve dans le répertoire suivant de Windows XP : `%WINDIR%\SYSTEM32\SPOOL\DRIVERS\W32X86`.

Il vaut faudra les fichiers suivant :

- `ps5ui.dll`
- `pscript5.dll`
- `pscript.hlp`
- `pscript.ntf`

Ces fichiers sont à copier sur le serveur, en tant qu'utilisateur root, dans le répertoire suivant :

`/usr/share/cups/drivers/`

Enfin, il faut associer les pilotes CUPS aux imprimantes.

Pour associer les pilotes CUPS à une imprimante, il faut taper la commande suivante :

```
# cupsaddsmb -v -H localhost -U admin <Epson_740>
```

<Epson_740> étant le nom de l'imprimante définit dans l'interface CUPS.

5.2.3. Quotas d'impression

Aucune gestion de quotas d'impression n'est, à ce jour, intégrée sur les modules EOLE.

Le document suivant explique étape par étape comment mettre en place le logiciel de gestion de quotas d'impression Pykota sur un module Scribe ou Horus en version 2.2 :

http://eoleng.ac-dijon.fr/documentations/2.2/contributions/pykota.pdf

5.3. Gestion des imprimantes sous Windows



Ceci ne concerne pas les postes Windows Millennium et inférieur et nécessite l'utilisation du logiciel ESU[p.761].

Dans la partie règle utilisateurs, que l'on obtient en cliquant sur un groupe d'utilisateurs dans la colonne de gauche, sélectionner `Panneau de Configuration` section *"Imprimantes*".

A cet endroit vous pouvez spécifier le chemin UNC (\\<scribe>\<imprimante>) d'accès aux imprimantes disponibles pour ce groupe de machine et ce groupe d'utilisateur.

Ainsi élèves et professeurs peuvent avoir des imprimantes différentes sur un même poste et un utilisateur peut avoir des imprimantes différentes en fonction du poste et du groupe de machines auquel il

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

appartient.

6. Compatibilité entre GFC et le module Horus

La qualification de GFC (Gestion Financière et Comptable) sur le module Horus est réalisée par l'équipe de diffusion de Montpellier.

L'actualité des applications nationales est consultable sur le site intranet de diffusion : http://diff.in.ac-montpellier.fr/

Les tests de compatibilités réalisés entre les différentes versions de GFC et du module Horus sont disponibles dans la rubrique `Téléchargements des versions` : http://diff.in.ac-montpellier.fr/index.php/gfc/telechargements-des-versions



Il existe également un espace dédié au module Horus sur le site de diffusion du Pôle de Compétence de Paris :

https://pole.in.ac-paris.fr/vosapplication/HORUS

7. Mise en place des sondes EQOS

EQoS permet à tout responsable, personnel de direction en établissement ou autorité académique, de mesurer la qualité de service de ses applications selon des critères objectifs.

Ces outils sont développés par pôle de Compétences Inter-Académique de Nancy-Metz (adresse à usage académique https://pole.in.ac-nancy-metz.fr).

Leur mise en place sur un module EOLE est simplifiée par la réalisation d'un paquet nommé `eole-eqos`, pour l'installer :

```
# Query-Auto
# apt-eole install eole-eqos
# reconfigure
```



Une documentation est disponible sur le site du pôle Compétences (adresse à usage académique) : https://pole.in.ac-nancy-metz.fr/wiki/EqosDispoInstallSonde [https://pole.in.ac-nancy-metz.fr/wiki/EqosDispoInstallSonde]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

8. Les clients Windows

8.1. Installation et configuration des clients Windows

8.1.1. Principe

Le module Horus agissant comme un contrôleur de domaine, les stations Windows doivent dans un premier temps être intégrées dans le domaine.

Mises à jour et sécurité

Les mises à jour n'apportent pas seulement de nouvelles fonctionnalités, elles corrigent aussi des failles de sécurité.

Il est donc important que **les clients soient aussi à jour**.

Cela concerne aussi bien le **système d'exploitation** (Windows Update) que **les programmes installés** (Firefox, Java, QuickTime, etc .).

Des vulnérabilités peuvent, en effet, toucher n'importe quel programme.

Ne pas appliquer les mises à jour rendrait votre système vulnérable aux attaques.

Rappelons à ce sujet que, statistiquement, la majorité des attaques proviennent de l'intérieur et non de l'extérieur.

8.1.2. Configuration réseau

Avant l'intégration au domaine, il est indispensable de s'assurer que les paramètres réseau de la station soient corrects (adresse IP, passerelle, DNS, WINS).

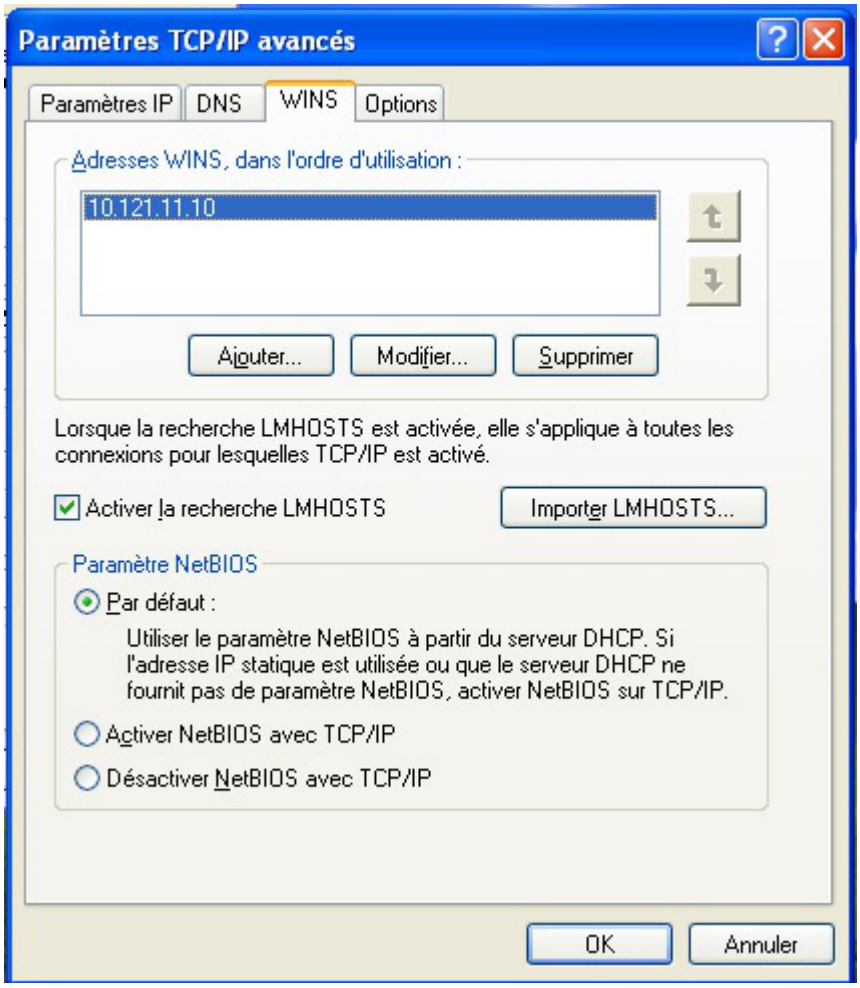
Plusieurs cas sont possibles :

- la station obtient son adresse IP du serveur DHCP du serveur EOLE, dans ce cas il n'y a rien à faire ;
- la station obtient son adresse IP d'un serveur DHCP autre que le serveur EOLE, il faudra veiller à paramétrer l'adresse du serveur WINS[p.783] ;
- la station est adressée manuellement, il faudra veiller à paramétrer l'adresse du serveur WINS.

Configuration du serveur WINS sous Windows XP

Pour accéder à la configuration du serveur WINS il faut aller dans `Panneau de configuration`, `Connexions réseau`, faire un clic droit sur l'icône `réseau local` et sélectionner `propriétés`, puis double-cliquer sur `Protocole Internet (TCP/IP)`, cliquer sur `Avancé...` et enfin sélectionner l'onglet `WINS`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Configuration du serveur WINS dans Windows XP

8.1.3. Intégration et installation du client Horus automatique

Windows 10

Depuis la version 1709 de Windows 10, l'intégration au domaine d'une station nécessite au préalable d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.

Depuis la version 1903 de Windows 10, le fonctionnement des profils obligatoires n'est plus garanti.

Accéder au répertoire personnel de l'administrateur du domaine

Depuis la version 1709 de Windows 10, il est impossible d'accéder au lecteur réseau en mode invité.
Pour accéder au répertoire de l'administrateur avant la jonction au domaine il faut :

- soit appliquer une clé de registre pour supprimer cette interdiction ;
- soit monter un lecteur réseau en spécifiant les identifiants de connexion.

https://support.microsoft.com/de-ch/help/4046019/guest-access-smb2-disabled-by-default-in-windows-1(

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Réactiver l'accès aux partages guest via une clé de registre

La clé de registre suivante permet de réactiver la possibilité de se connecter à un partage non sécurisé.

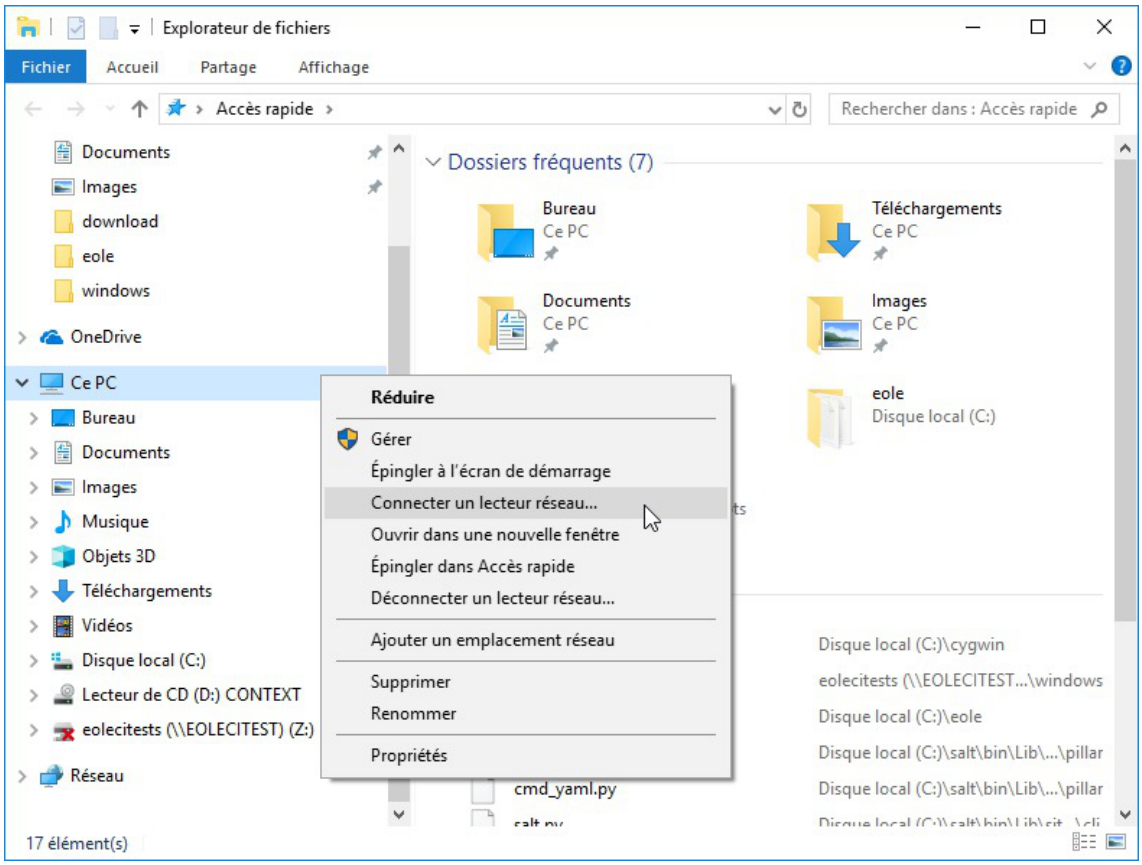
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

Monter un répertoire en spécifiant les identifiants de connexion

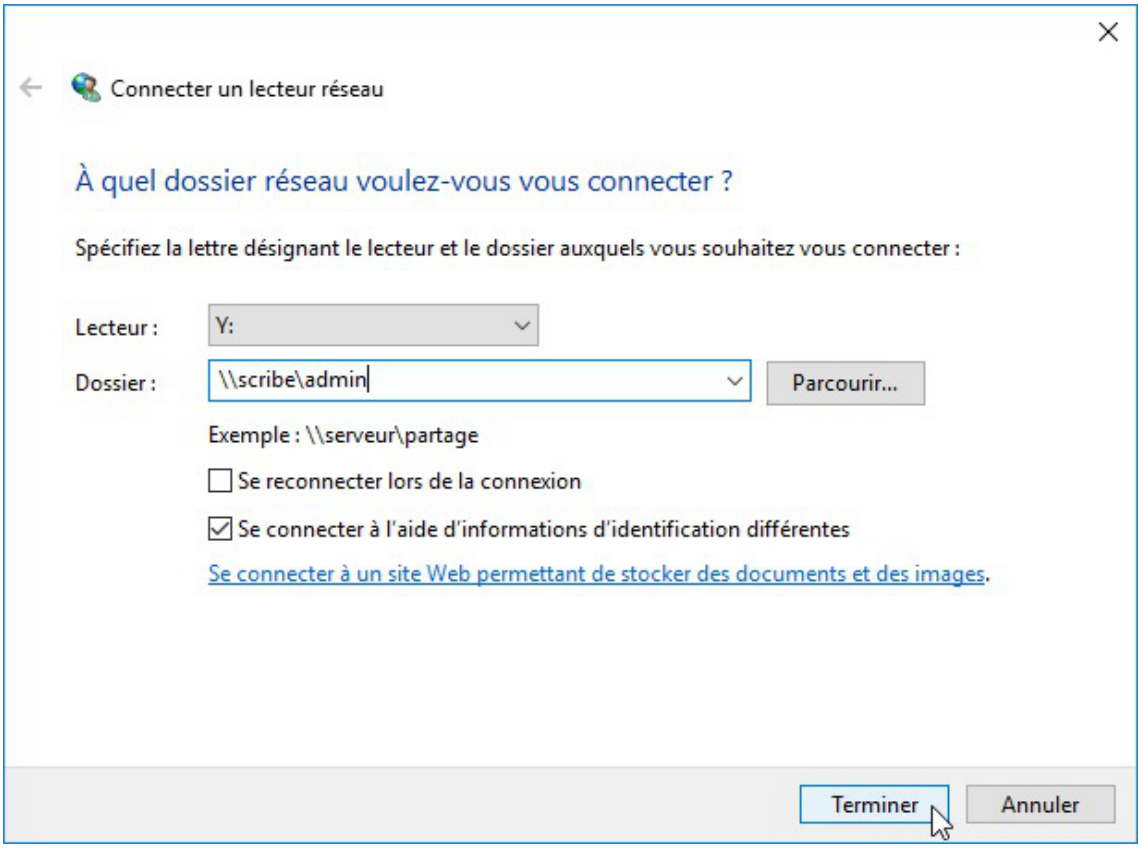
Pour accéder au répertoire personnel de l'administrateur :

- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;

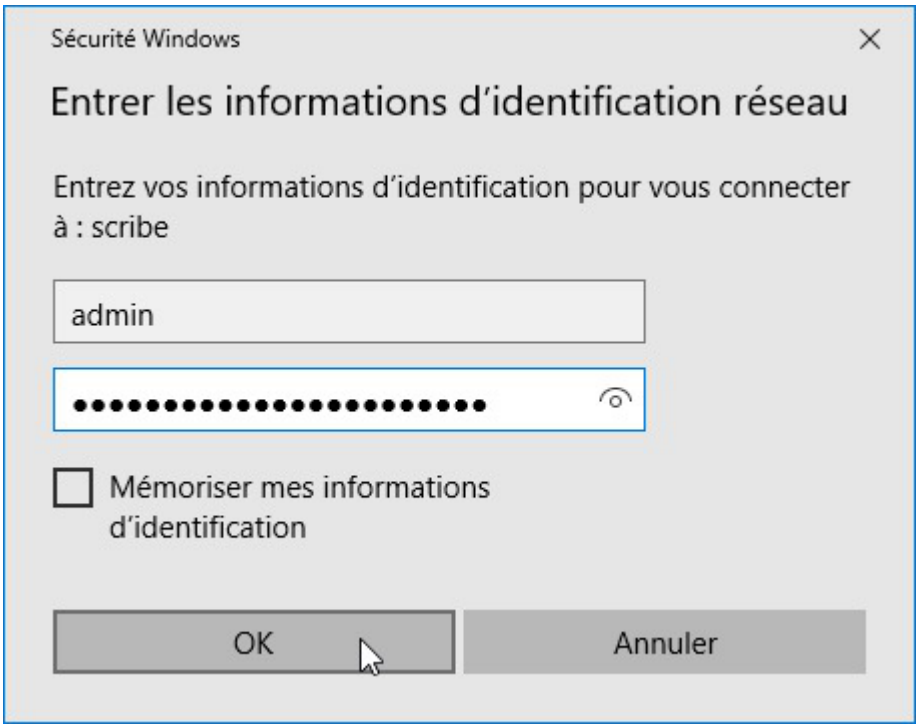


- Faire un clique droit sur `Ce PC` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

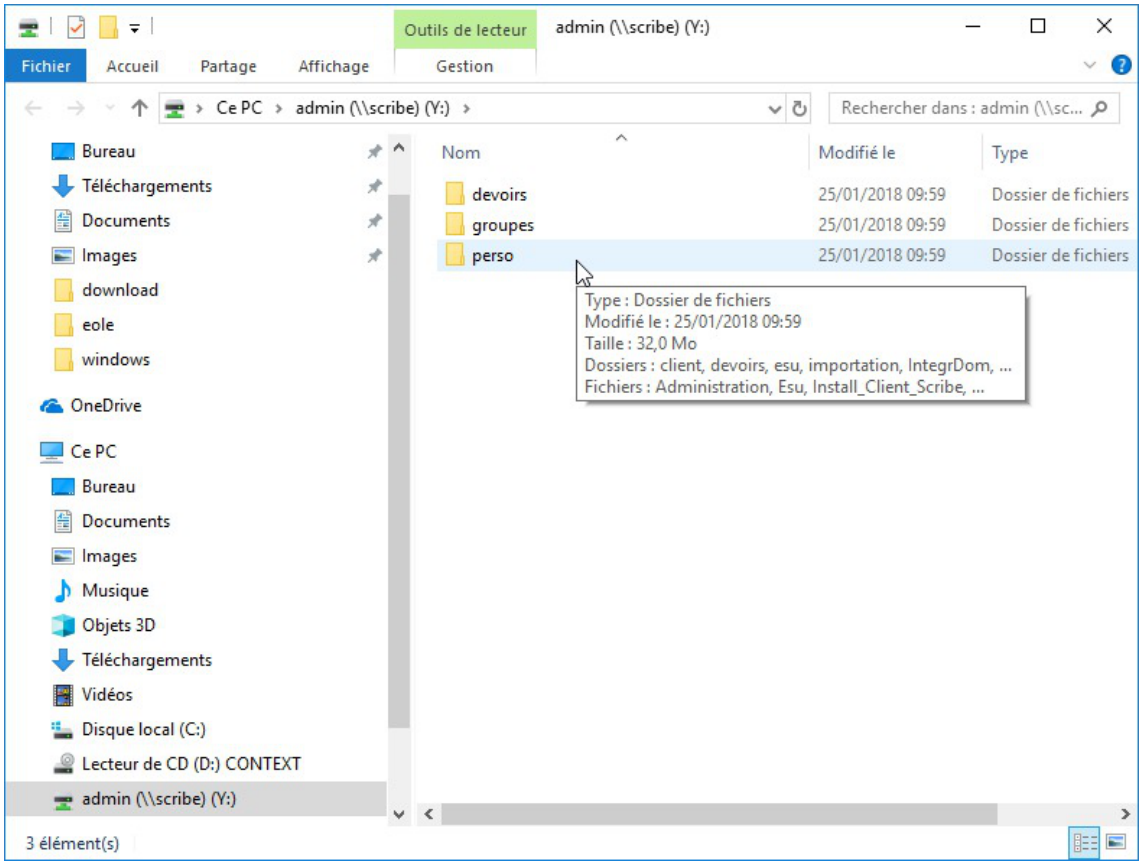


- Saisir `\\scribe\admin` dans le champ `Dossier`, décocher ☑ Se reconnecter lors de la connexion, cocher ☑ Se connecter à l'aide d'informations d'identification différentes et cliquer sur le bouton `Terminer` ;



- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton `OK` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



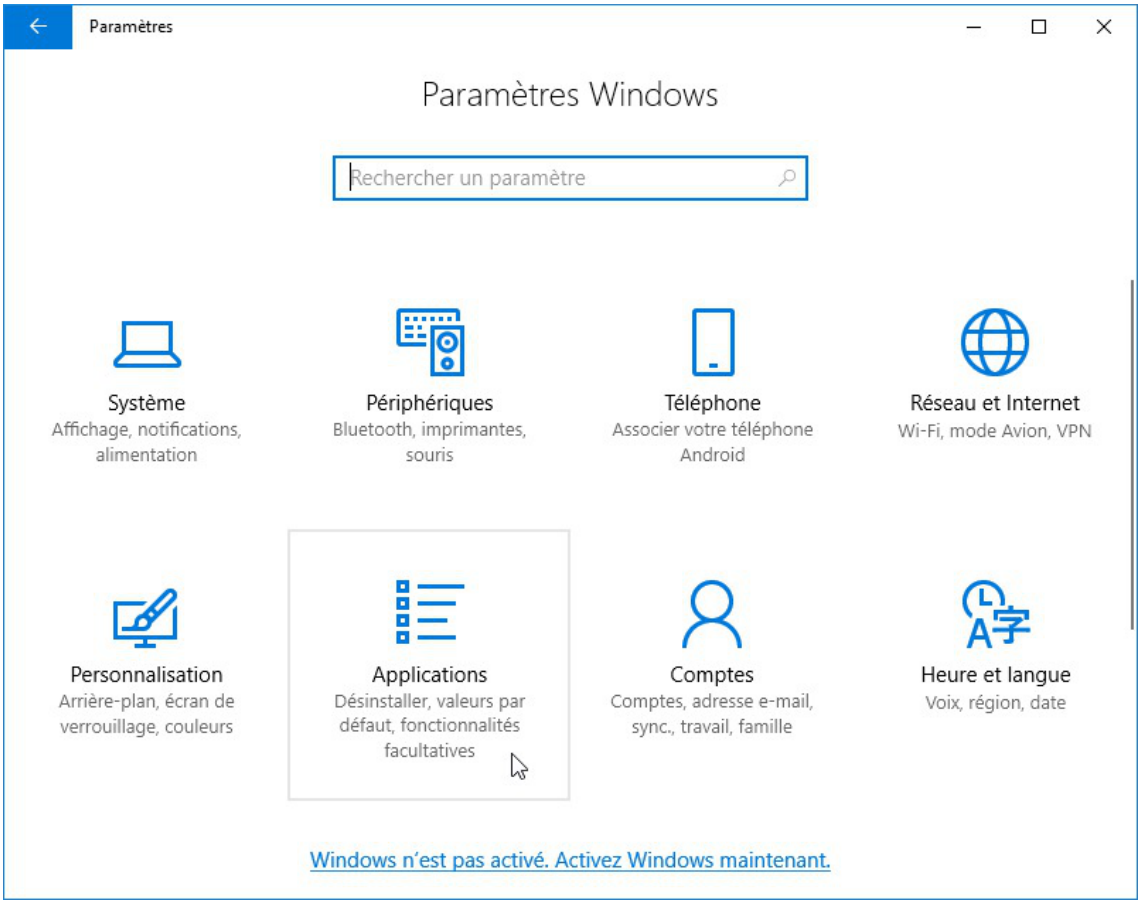
Activer manuellement le support de partage de fichiers SMB 1.0/CIFS

> Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

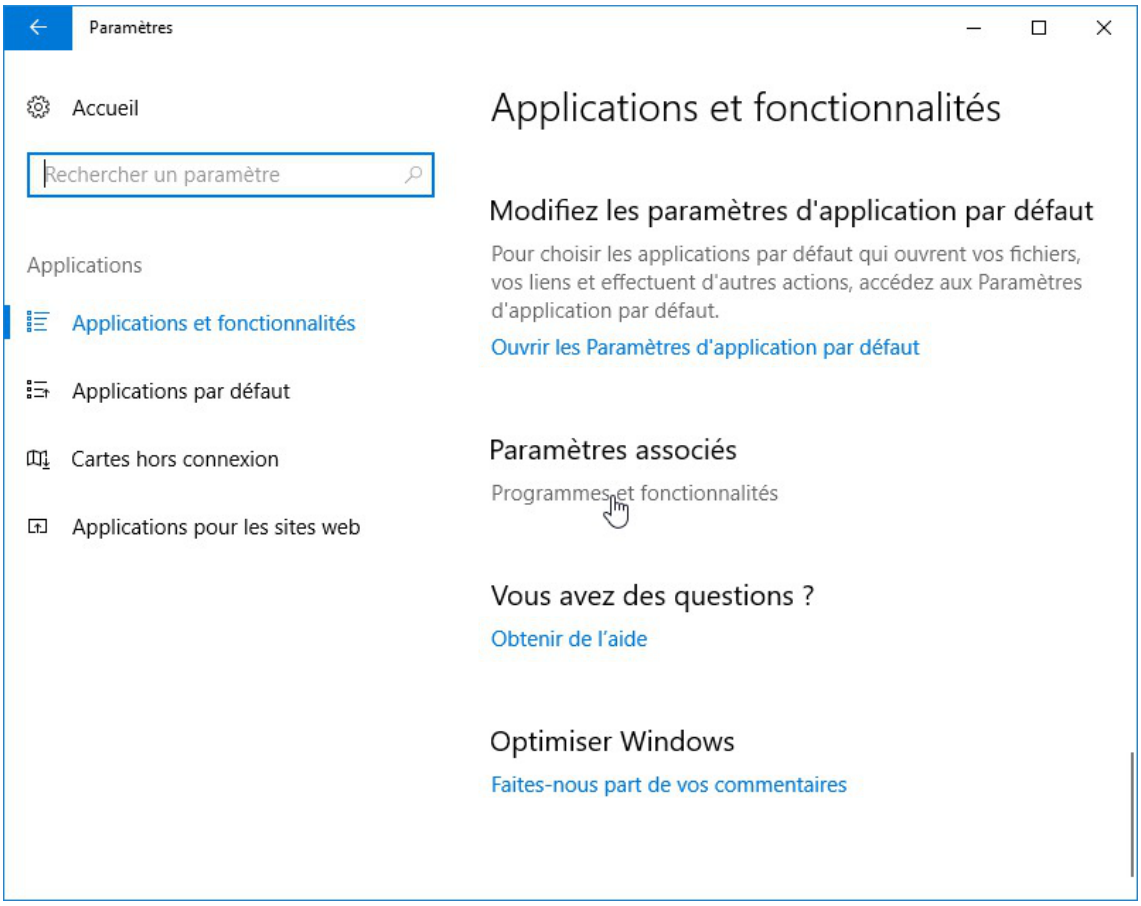
Paramétrer Windows de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

Version : révision : Juin création : Février 2017 2018
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

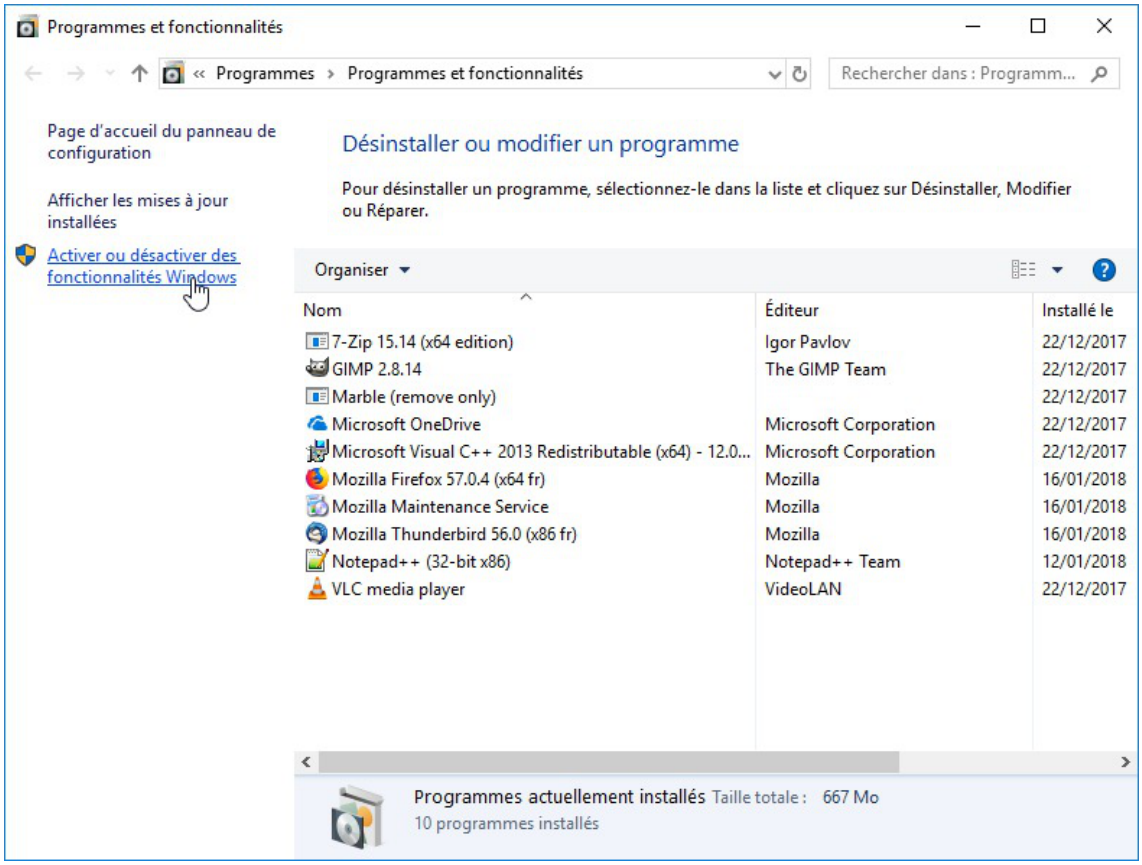


- Cliquer sur `Applications` ;

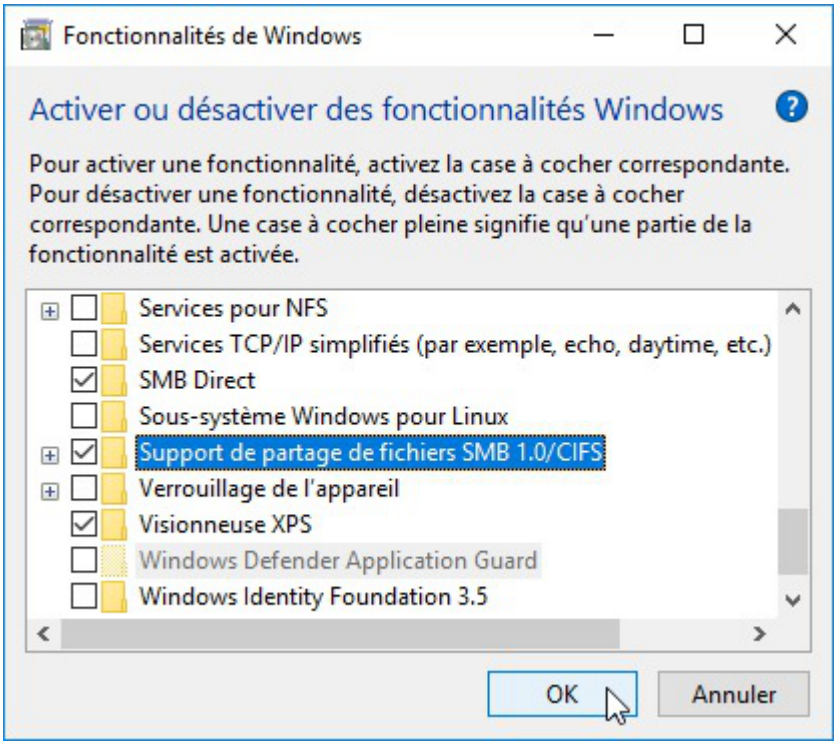


- Descendre et cliquer sur `Programmes et fonctionnalités` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

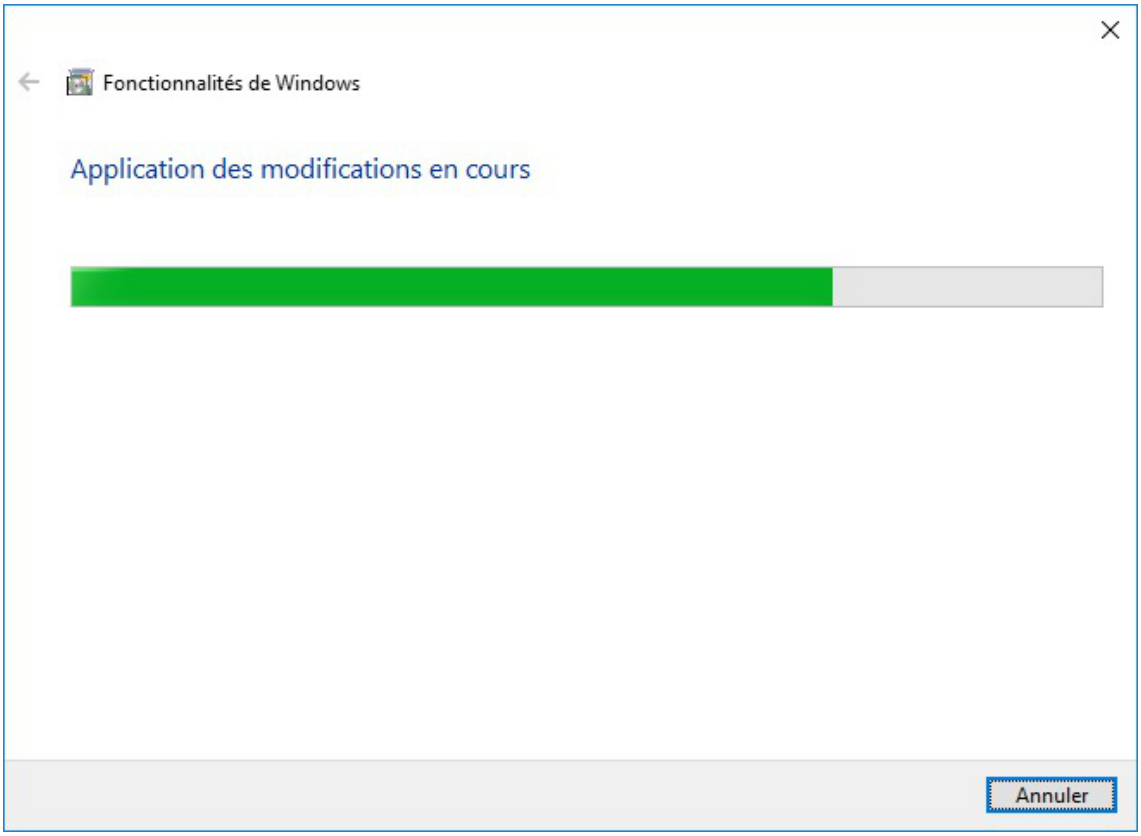


- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;



- Descendre dans la liste et cocher ☑ Support de partage de fichiers SMB 1.0/CIFS , cliquer sur `OK`, les modifications s'appliquent ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Utilisation de JoinEOLE

À partir de la version 2.5.2 du module, PrepaWin et IntegrDom ont été supprimés au profit du script JoinEOLE qui est disponible dans le dossier `IntegrDom` situé dans le répertoire perso de l'`admin`.

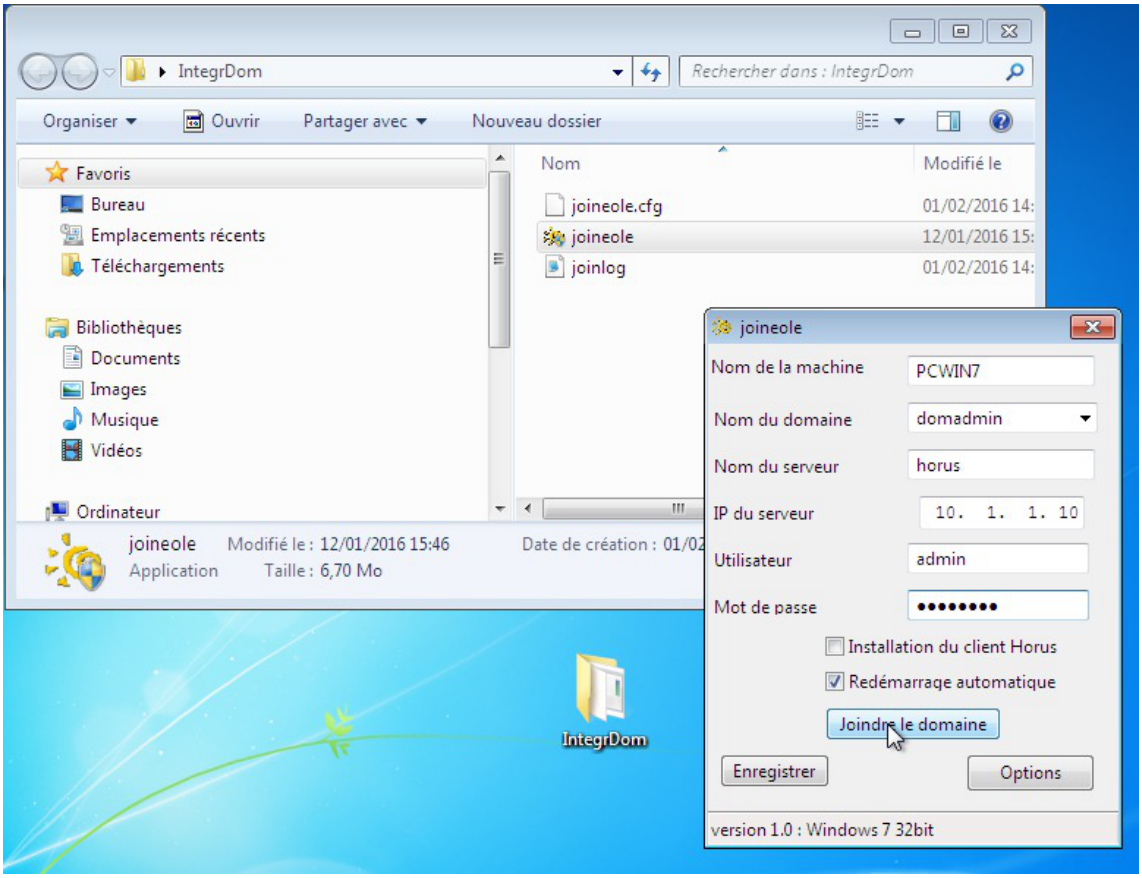
L'outil JoinEOLE prépare la station, la joint au domaine et installe de façon optionnelle le client pour Scribe ou Horus. De ce fait, il peut également être utilisé pour joindre les postes à un domaine Horus sur lequel l'outil ESU[p.761] n'est pas activé.

Le logiciel JoinEOLE est une contribution de Christophe Dezé de l'académie de Nantes.

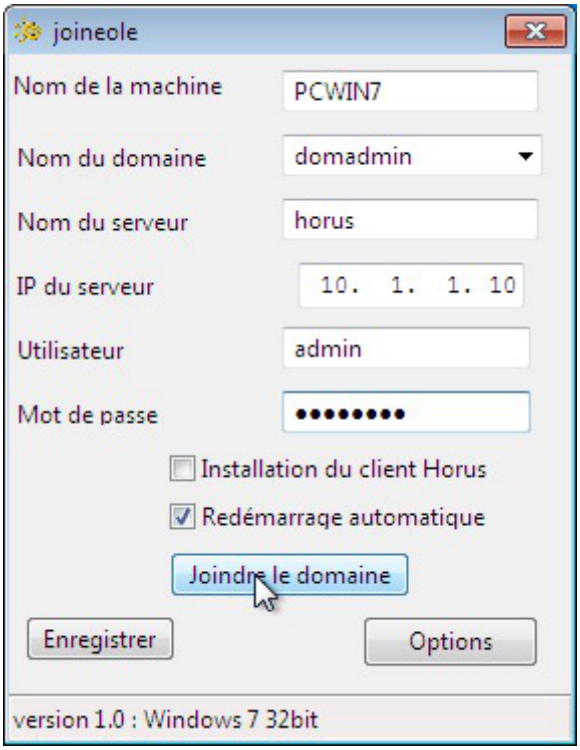
Il n'est pas possible de lancer l'exécution de JoinEOLE directement depuis le lecteur réseau car l'utilitaire ne gère par les chemins UNC[p.782].

Il faut donc copier l'utilitaire en copiant le répertoire `IntegrDom` sur la machine cliente et lancer son exécution.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Il faut préciser le nom de la machine à intégrer, le nom du domaine auquel la machine doit être raccrochée, le nom NetBIOS[p.770] du serveur ainsi que l'adresse IP du serveur Scribe ou Horus.



L'utilitaire permet l'intégration au domaine et installe directement le client si ☑ Installation du client est cochée.

La case Redémarrer automatiquement est précochée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une fois les paramètres renseignés il faut cliquer sur Joindre le domaine et cliquer sur Enregistrer. La machine affiche un message indiquant qu'elle va redémarrer.

8.1.4. Intégration et installation du client Horus manuelle

Intégration au domaine avec Windows 10

Préparation de Windows 10

L'intégration au domaine d'une station Windows 10 nécessite l'application préalable des clés de registre suivantes :

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters]
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths]
"\\\\*\\netlogon"="RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0"
```

Le fichier `Win_Samba3DomainMember.reg` mis à disposition dans `/home/esu/Console/` et accessible dans le répertoire `IntergrDom` situé dans le dossier personnel de l'utilisateur `admin` contient ces clés de registre.

L'intégration au domaine d'une station Windows 10 nécessite également l'exécution en tant qu'Administrateur des commandes suivantes

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc.exe config mrxsmb20 start= disabled
powershell.exe -Command "Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart"
```

Le script `Win10.bat` mis à disposition dans `/home/esu/Console/` et accessible dans le répertoire `IntergrDom` situé dans le dossier personnel de l'utilisateur `admin` contient ces commandes.



Depuis la version 1709 de Windows 10, l'intégration au domaine d'une station nécessite au préalable d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.



Depuis la version 1903 de Windows 10, le fonctionnement des profils obligatoires n'est plus garanti.

Accéder au répertoire personnel de l'administrateur du domaine

Depuis la version 1709 de Windows 10, il est impossible d'accéder au lecteur réseau en mode invité.

Pour accéder au répertoire de l'administrateur avant la jonction au domaine il faut :

- soit appliquer une clé de registre pour supprimer cette interdiction ;
- soit monter un lecteur réseau en spécifiant les identifiants de connexion.

https://support.microsoft.com/de-ch/help/4046019/guest-access-smb2-disabled-by-default-in-windows-1(

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Réactiver l'accès aux partages guest via une clé de registre

La clé de registre suivante permet de réactiver la possibilité de se connecter à un partage non sécurisé.

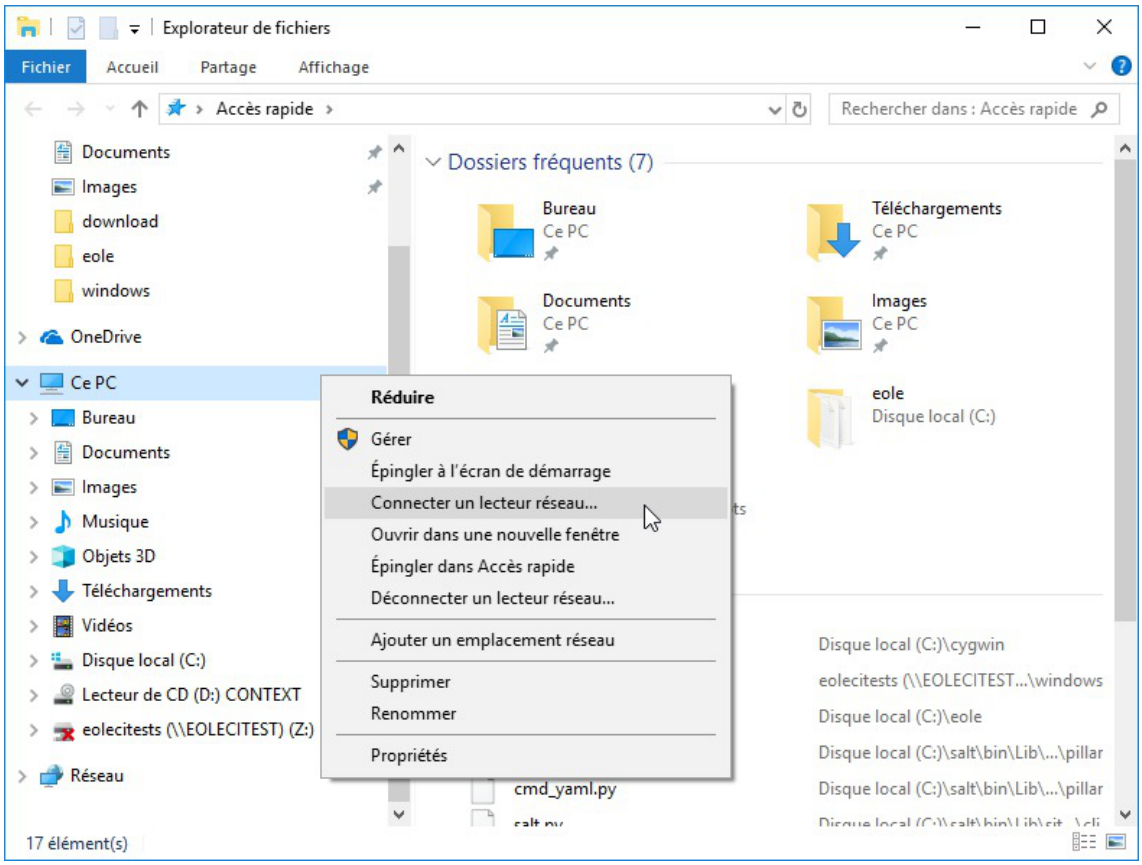
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

Monter un répertoire en spécifiant les identifiants de connexion

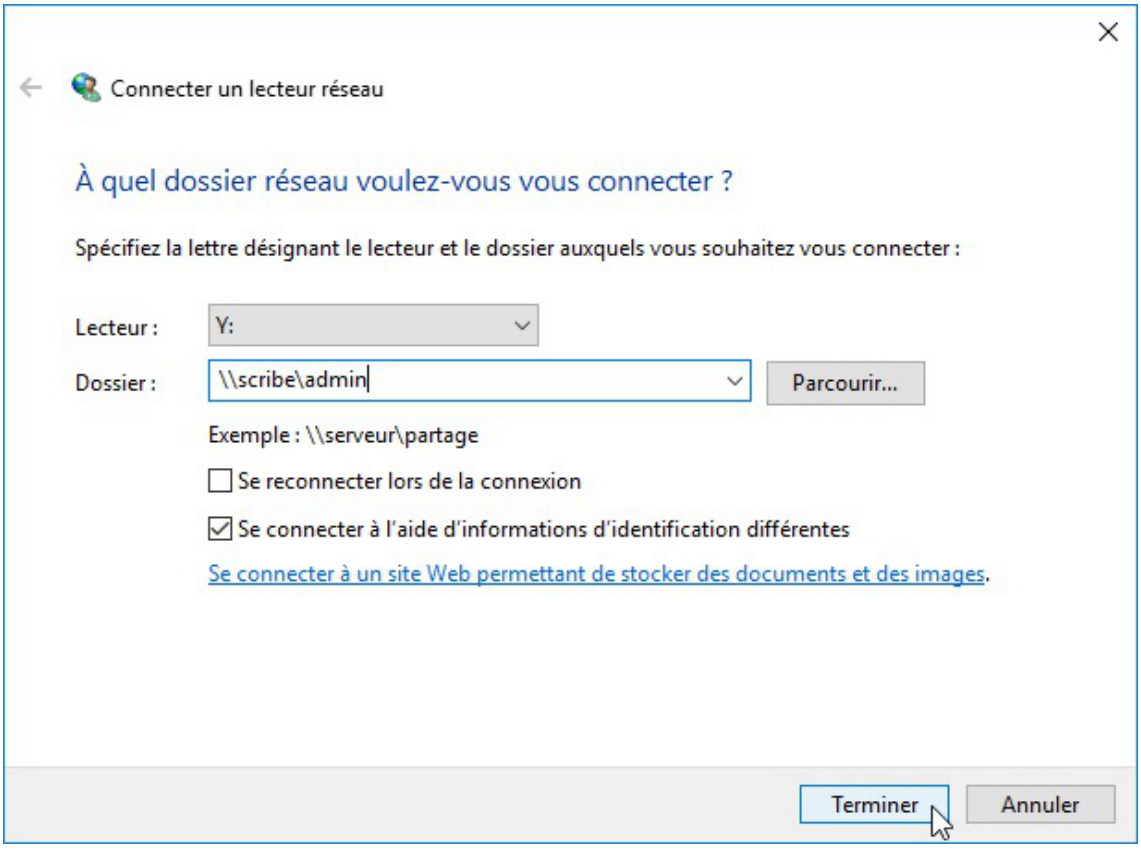
Pour accéder au répertoire personnel de l'administrateur :

- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;

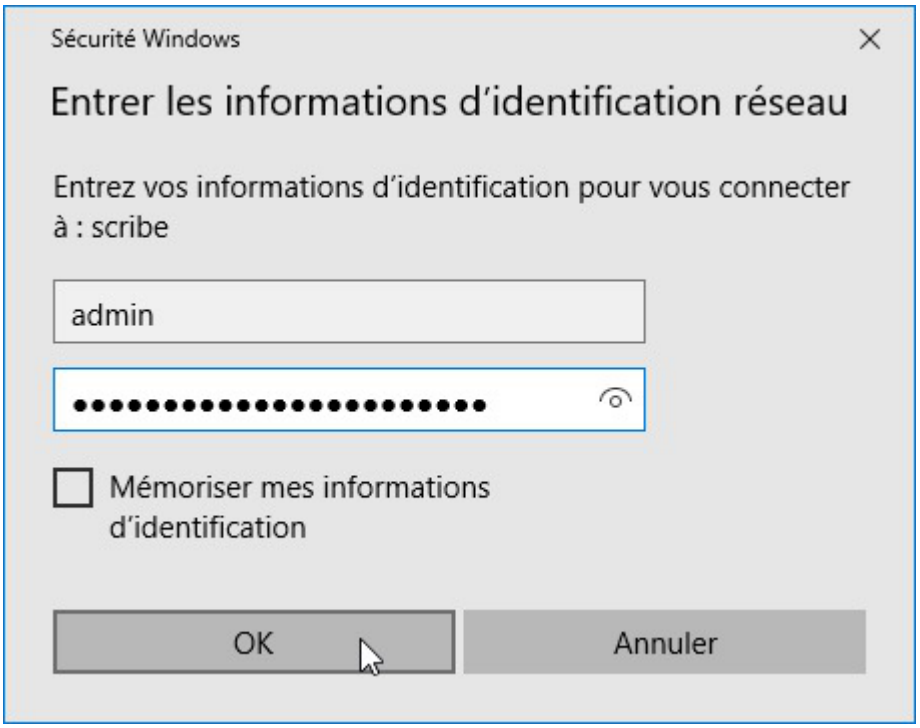


- Faire un clique droit sur `Ce PC` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

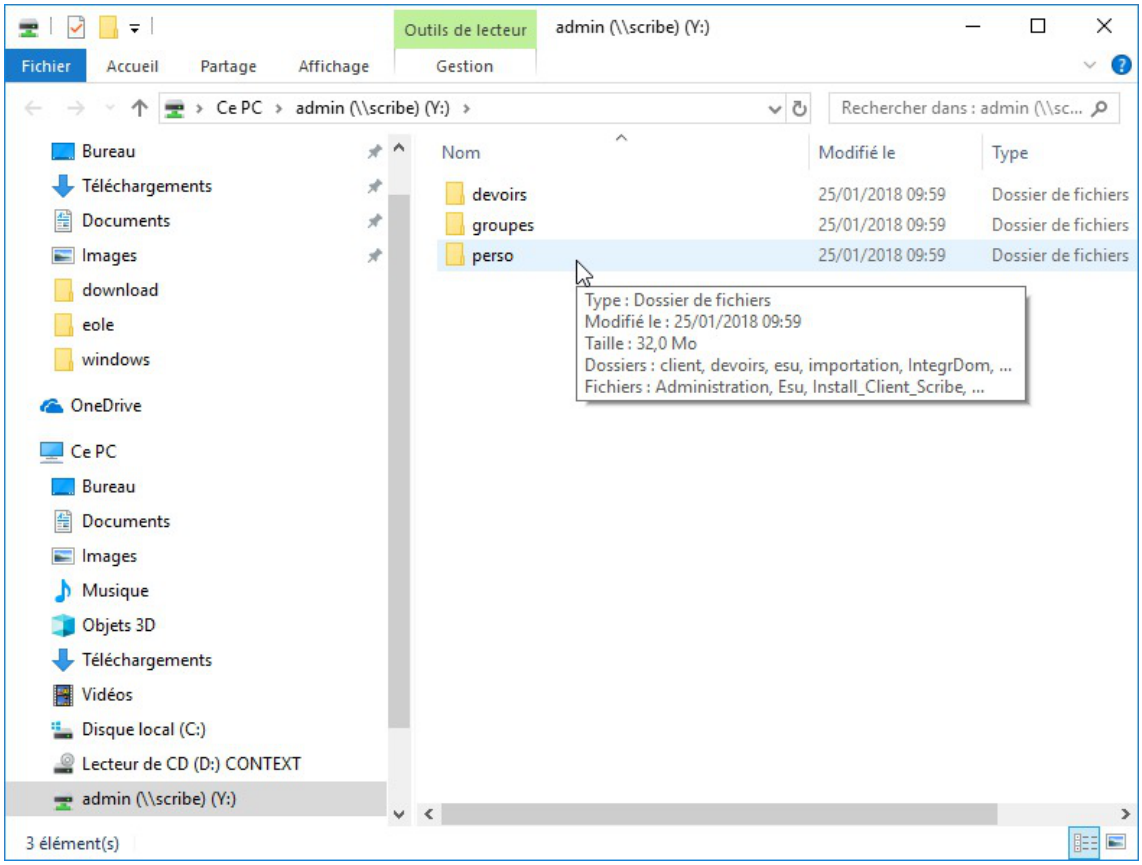


- Saisir `\\scribe\admin` dans le champ `Dossier`, décocher ☑ Se reconnecter lors de la connexion, cocher ☑ Se connecter à l'aide d'informations d'identification différentes et cliquer sur le bouton `Terminer` ;



- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton `OK` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



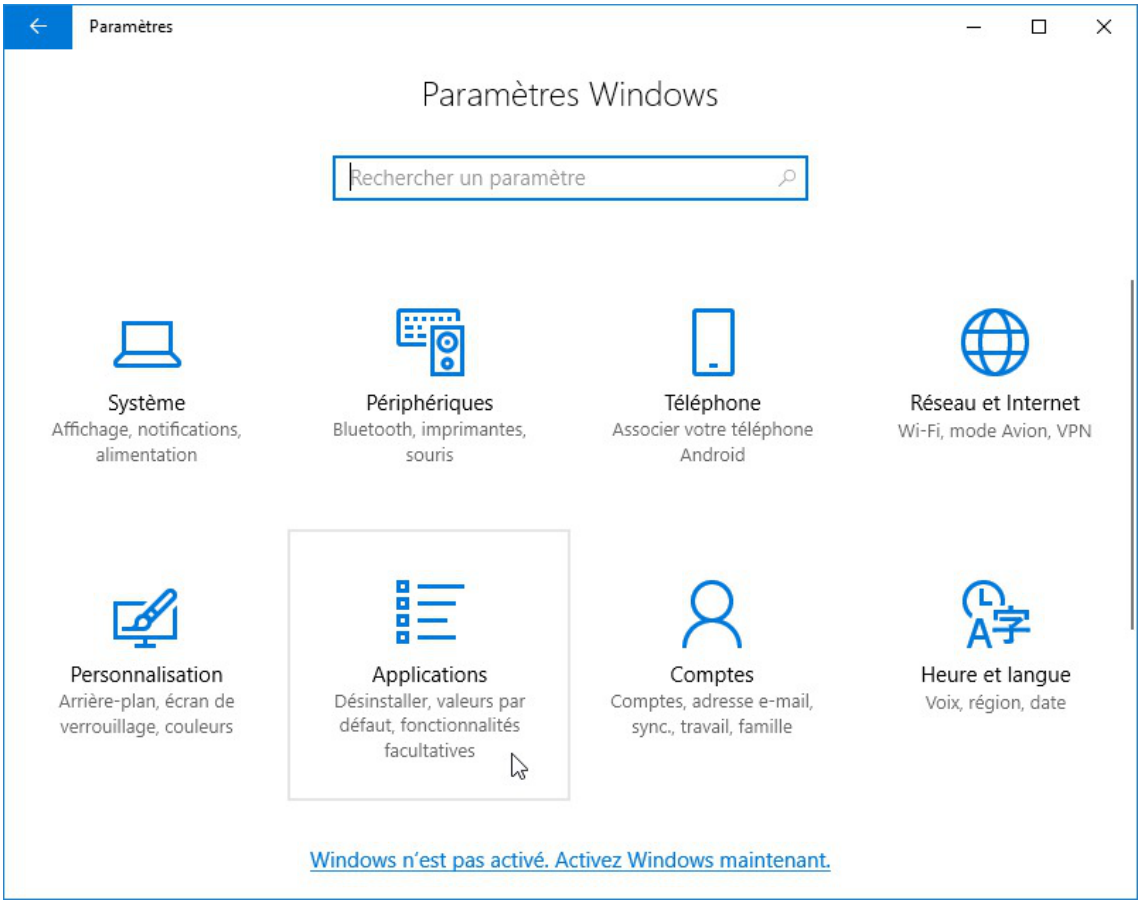
Activer manuellement le support de partage de fichiers SMB 1.0/CIFS

> Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

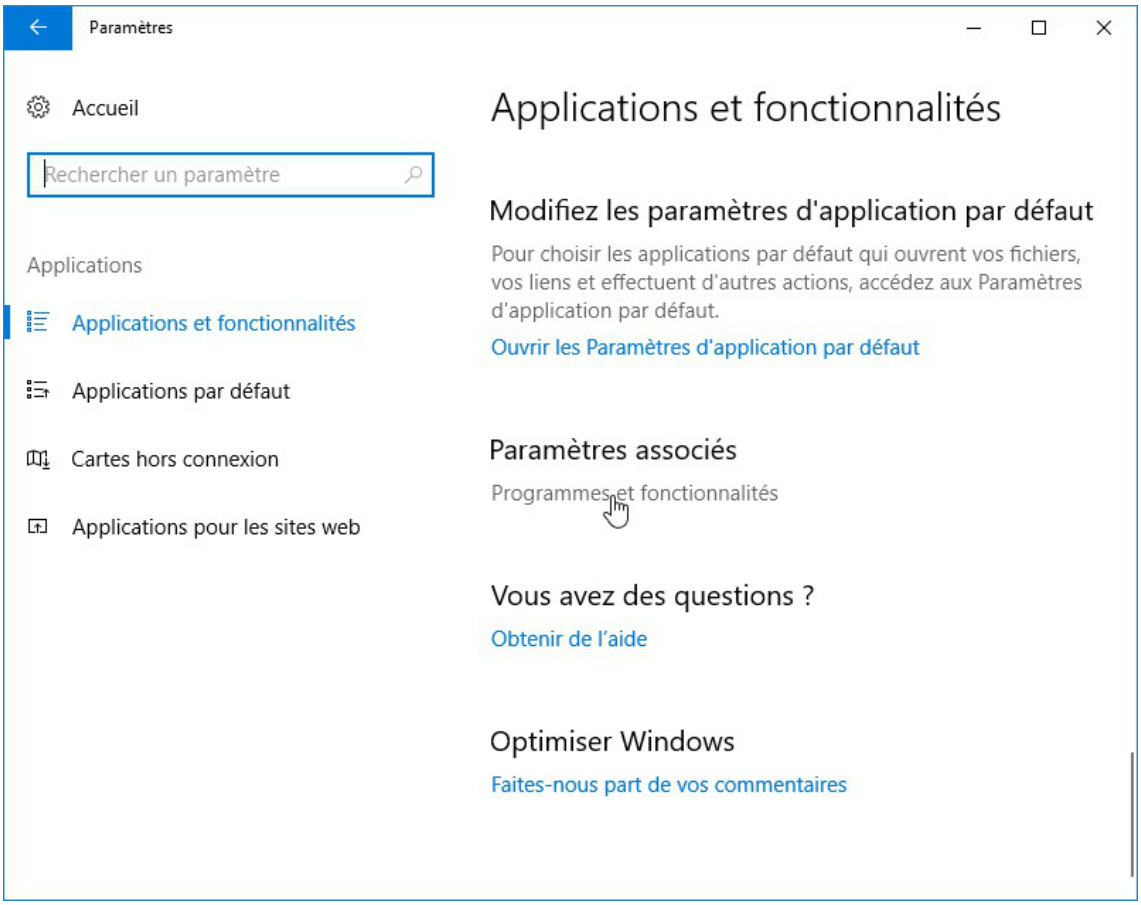
Paramétrer Windows de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

Version : révision : Juin création : Février 2017 2018
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

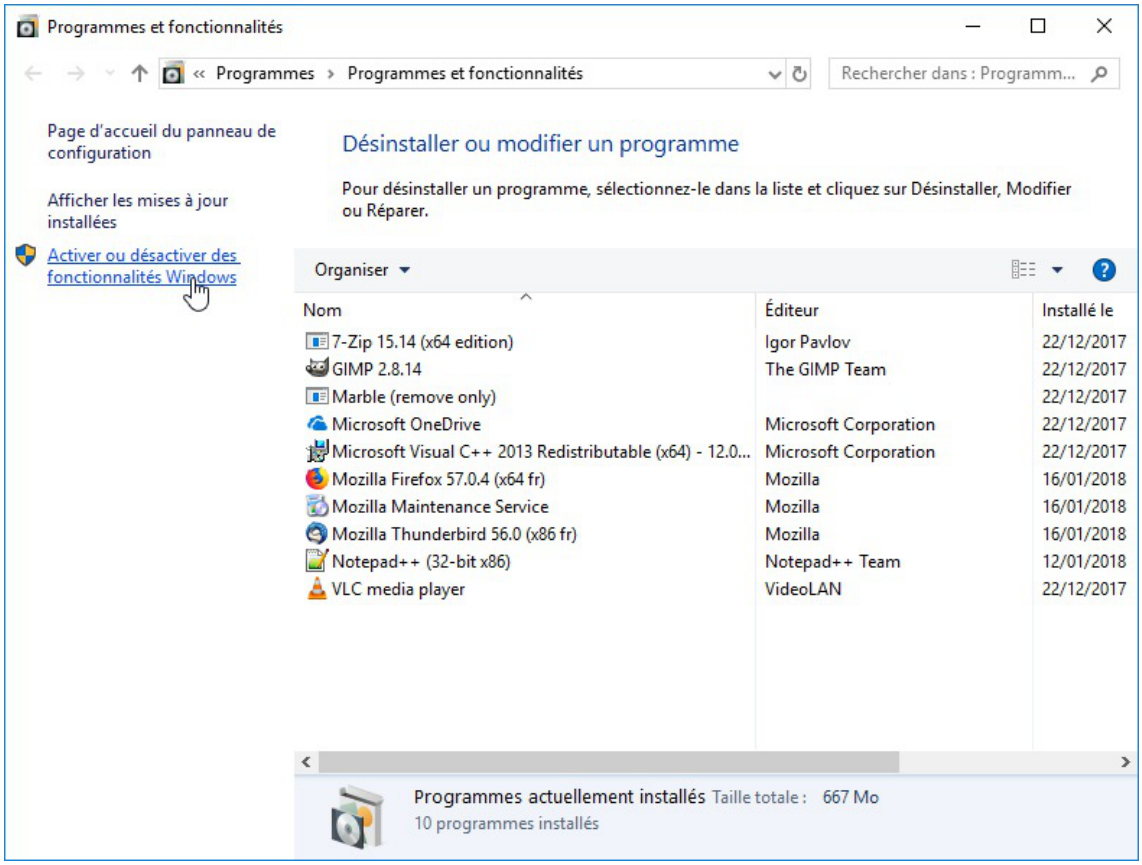


- Cliquer sur `Applications` ;

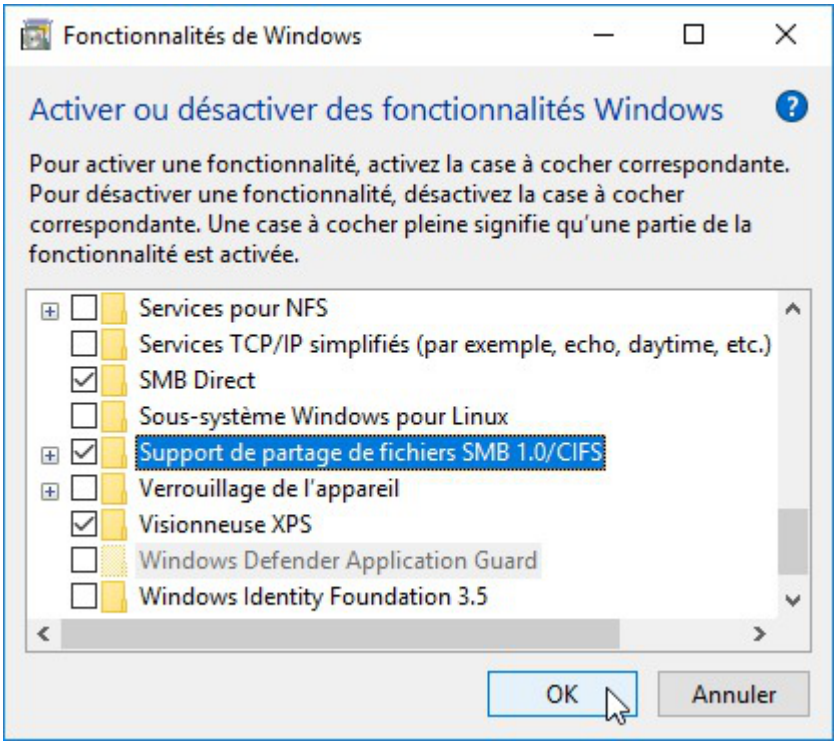


- Descendre et cliquer sur `Programmes et fonctionnalités` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

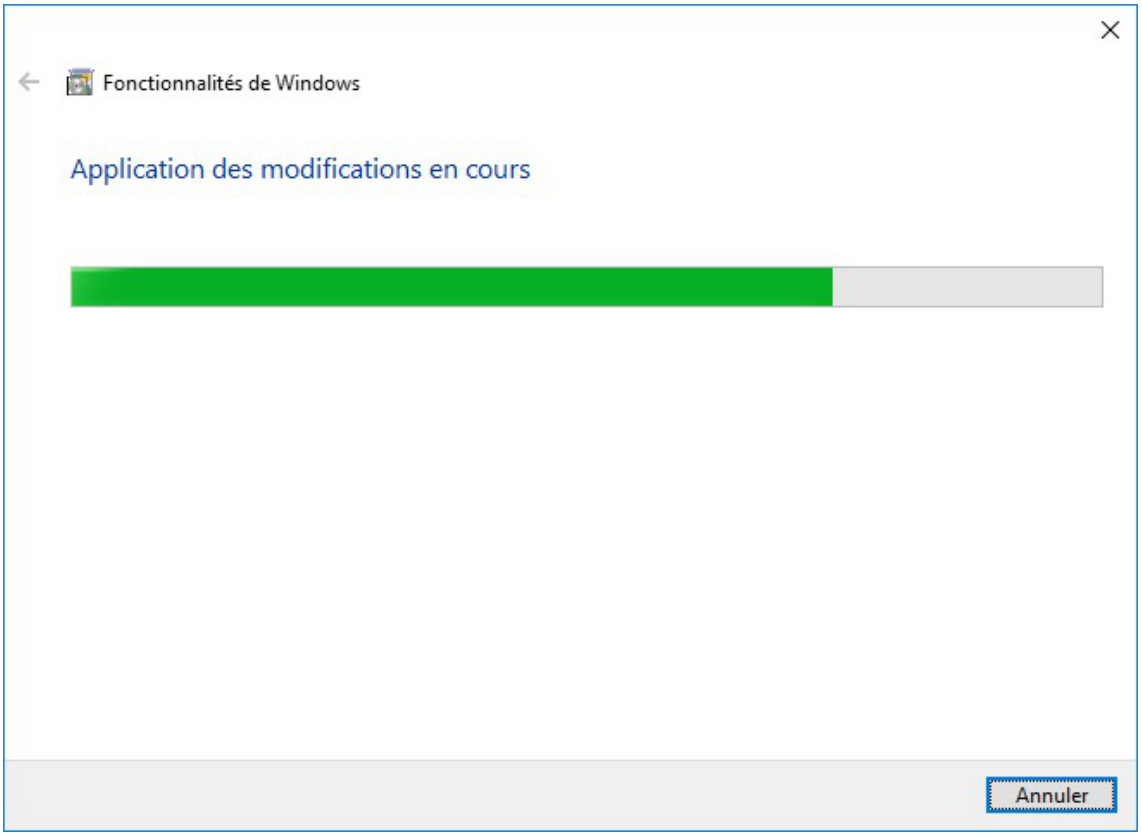


- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;



- Descendre dans la liste et cocher ☑ Support de partage de fichiers SMB 1.0/CIFS , cliquer sur `OK`, les modifications s'appliquent ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

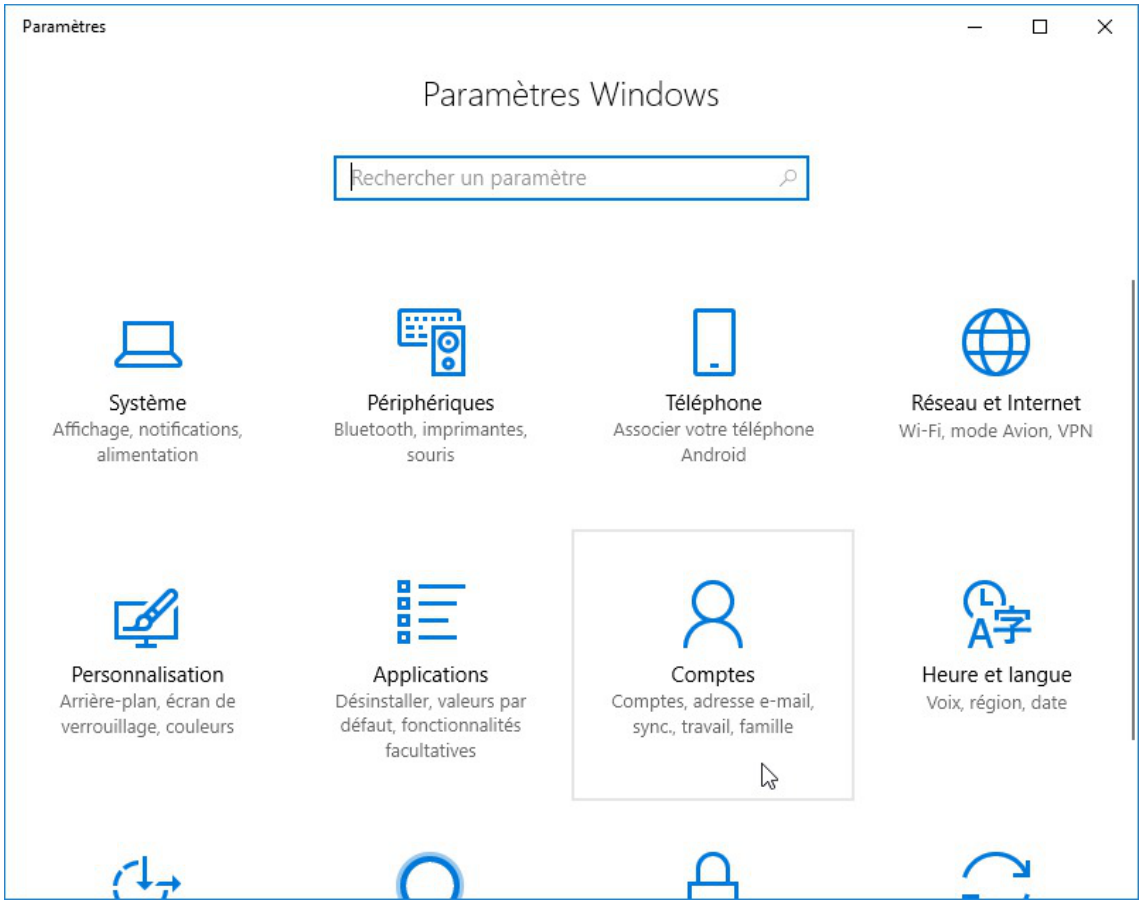


Jonction au domaine

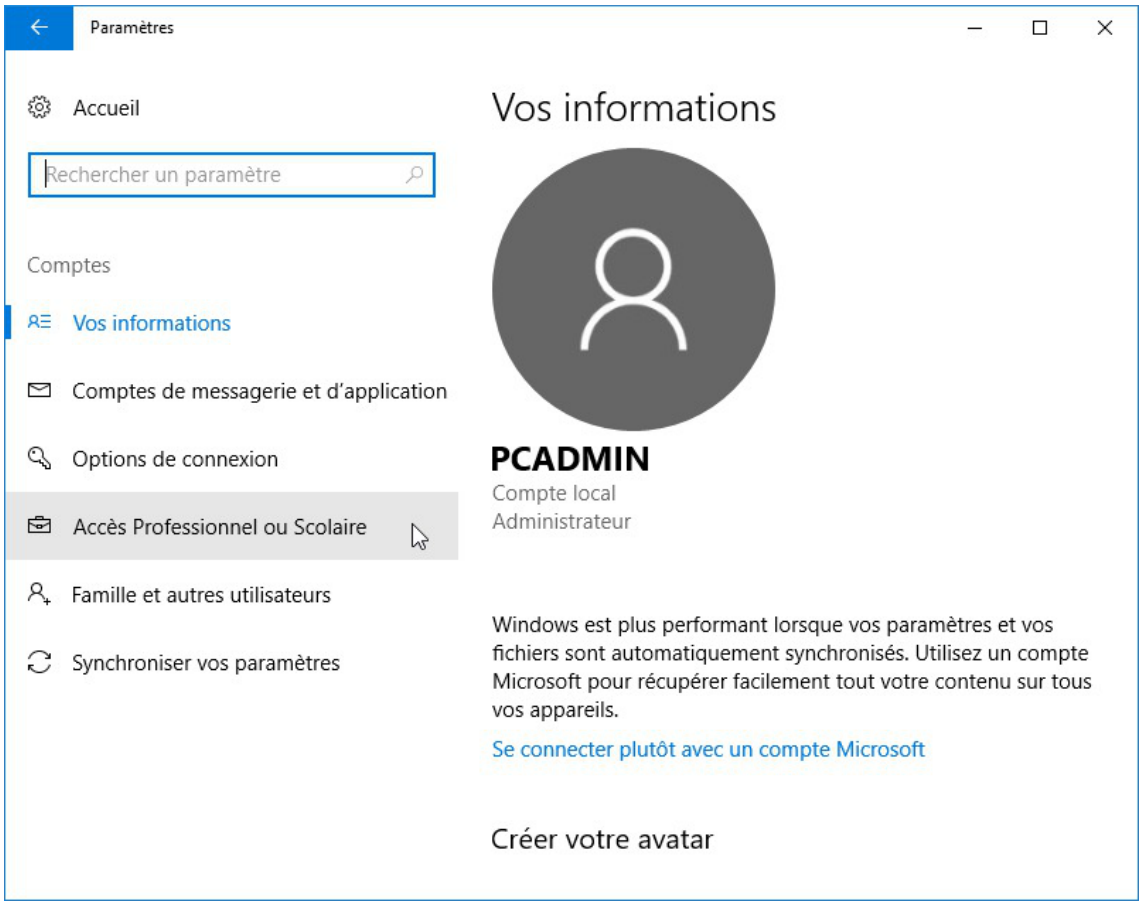
Ajouter la station au domaine de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

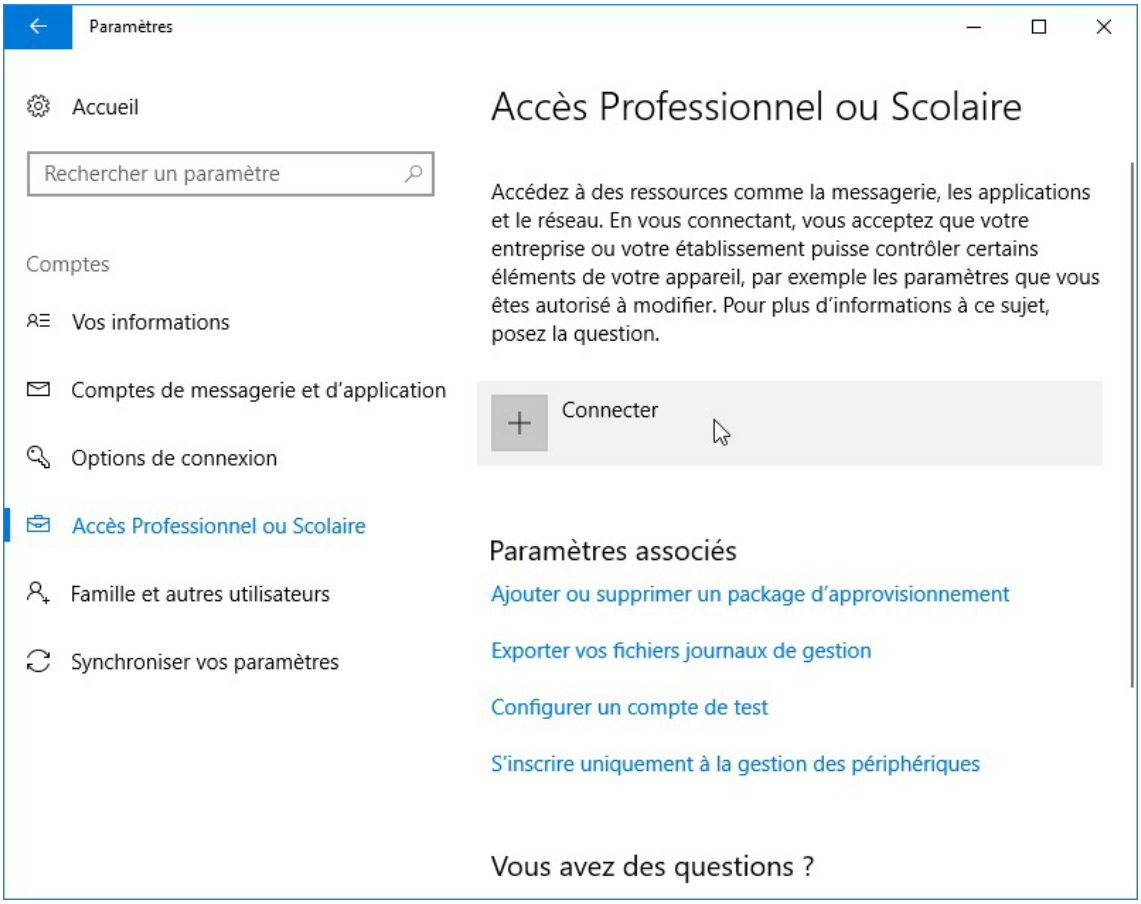


- Cliquer sur `Comptes` ;



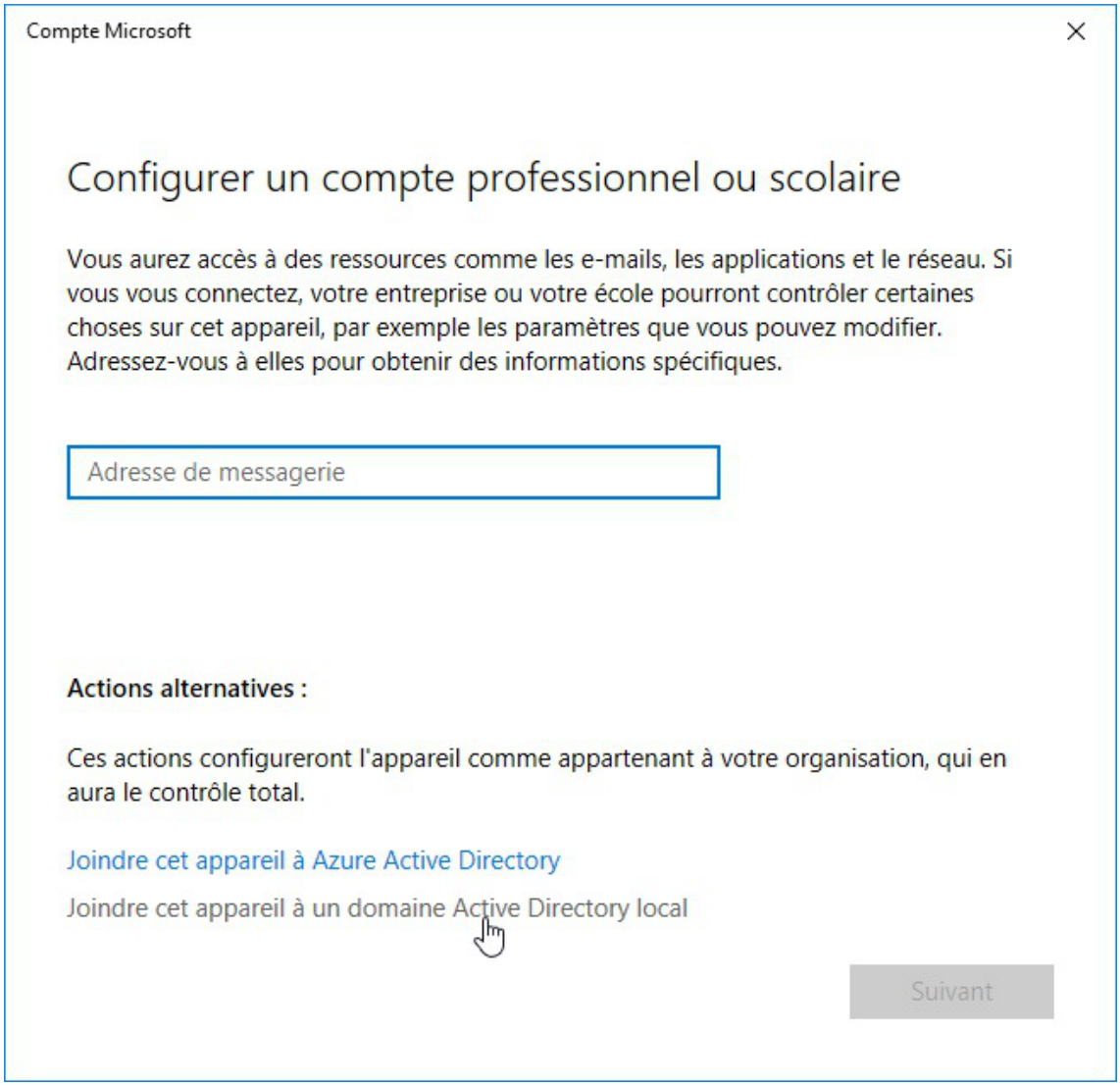
- Cliquer sur `Accès Professionnel ou Scolaire` dans le menu de gauche ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

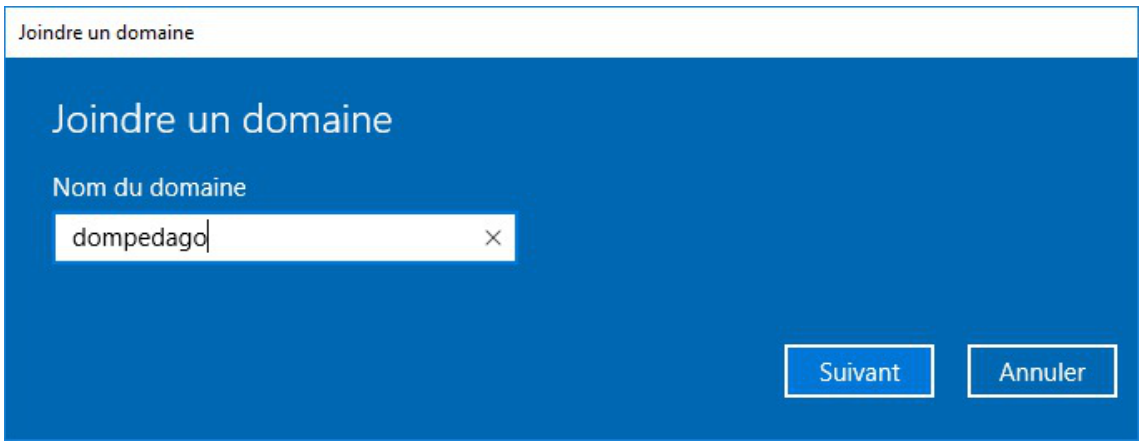


- Cliquer sur Connecter ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

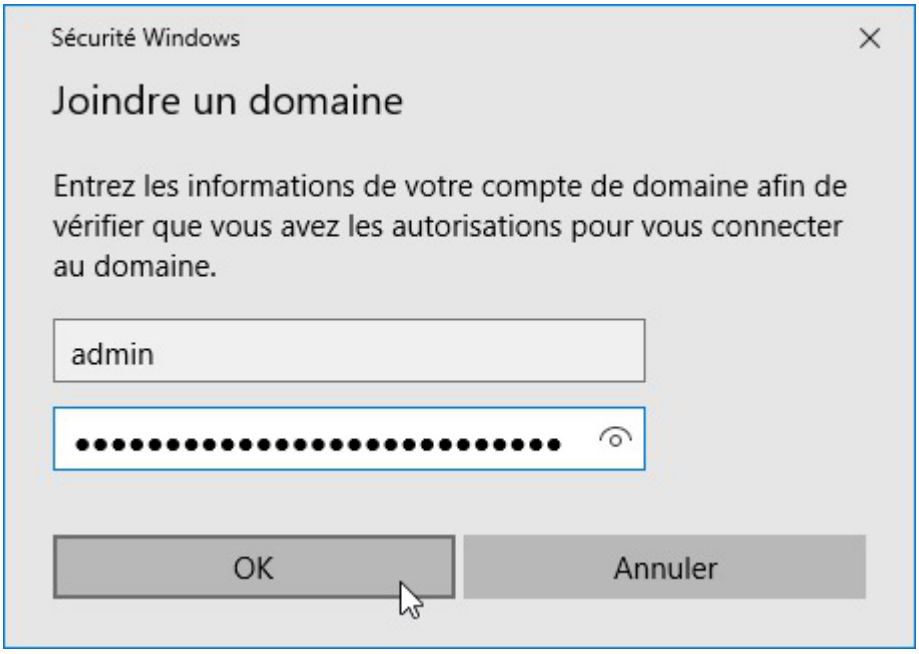


- Cliquer sur `Joindre cet appareil à un domaine Active Directory local` ;

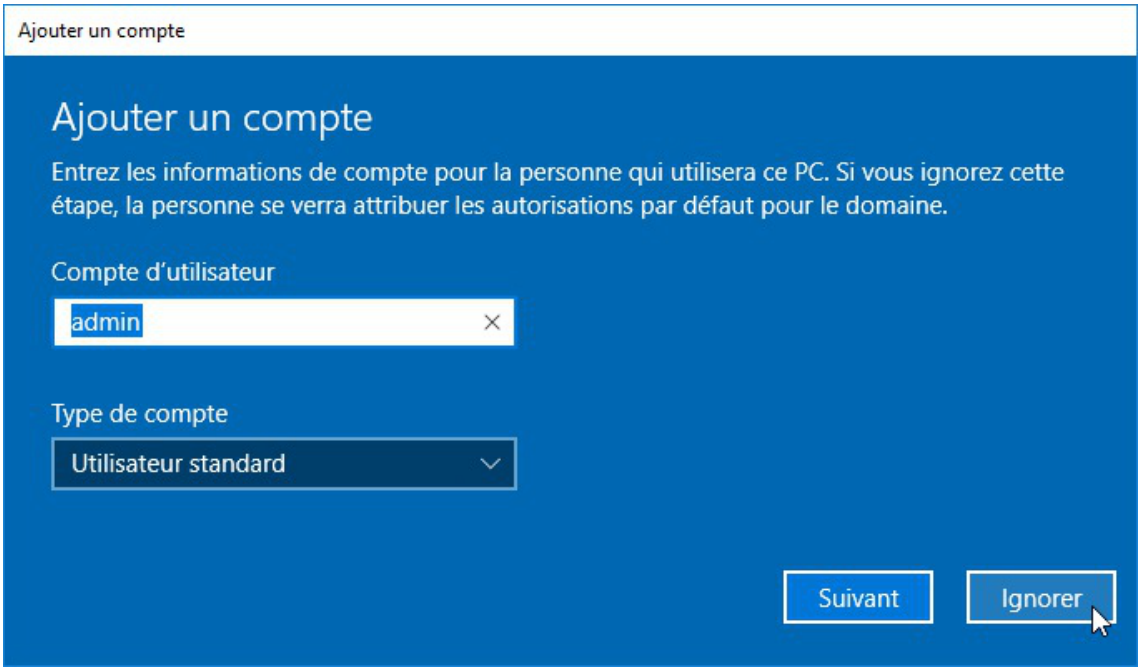


- Saisir le nom du domaine et cliquer sur `Suivant` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

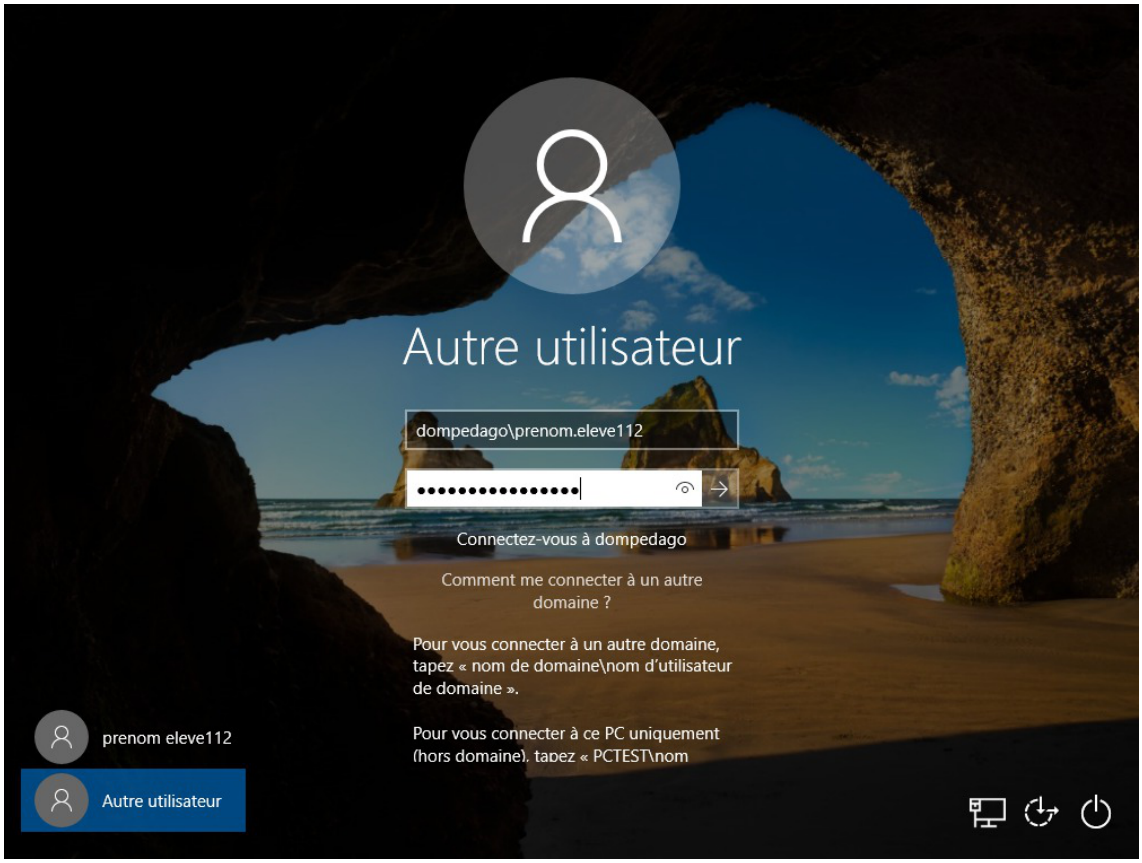


- Saisir le nom du compte administrateur du domaine ainsi que la clé secrète ("mot de passe") associée au compte et cliquer sur le bouton `OK` ;



- 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.

Intégration au domaine avec Windows 7

Préparation de Windows 7

L'intégration au domaine d'une station Windows 7 nécessite l'application préalable des clés de registre suivantes :

```
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManWorkstation\Parameters]
"DNSNameResolutionRequired"=dword:00000000
"DomainCompatibilityMode"=dword:00000001


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths]
"\\\\*\\netlogon"="RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0"
```

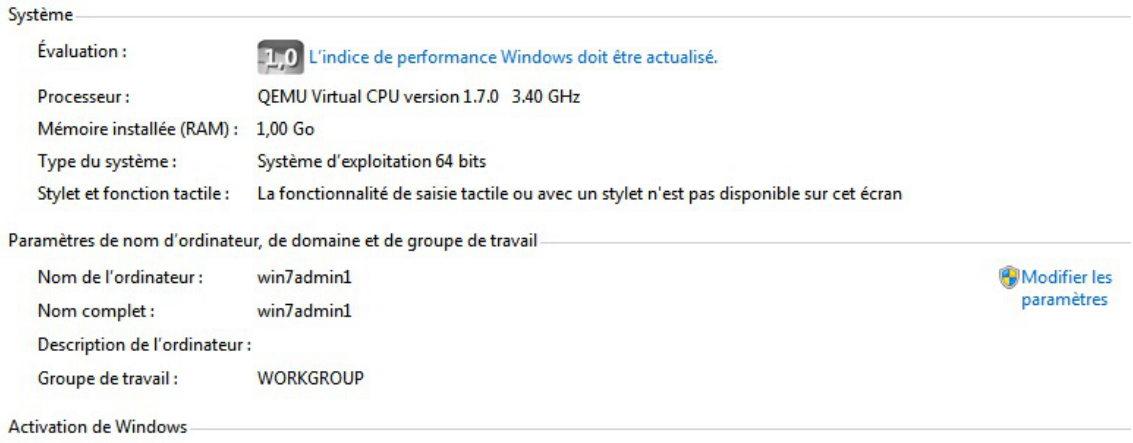
Le fichier `Win_Samba3DomainMember.reg` mis à disposition dans `/home/esu/Console/` et accessible dans le répertoire `IntergrDom` situé dans le dossier personnel de l'utilisateur admin contient ces clés de registre.

Jonction au domaine

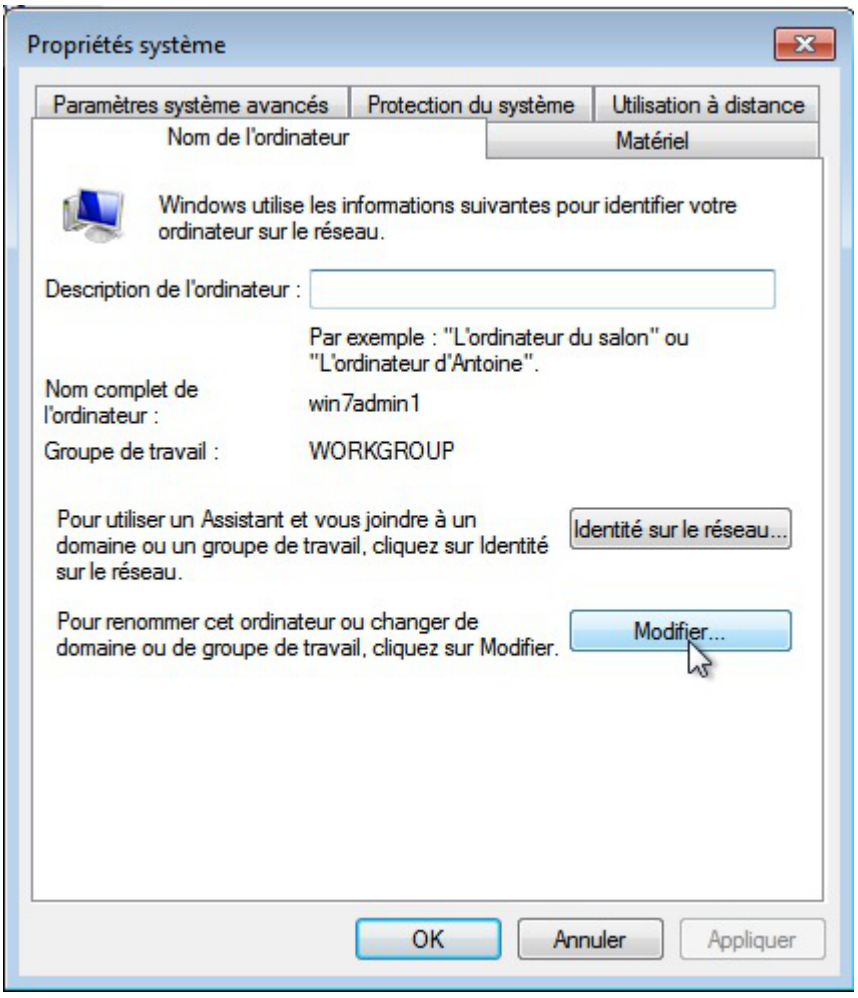
Ajouter la station au domaine de la façon suivante :

- Aller dans le menu `Démarrer` ;
- Clic droit sur `Ordinateur` et sélectionner `Propriétés` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

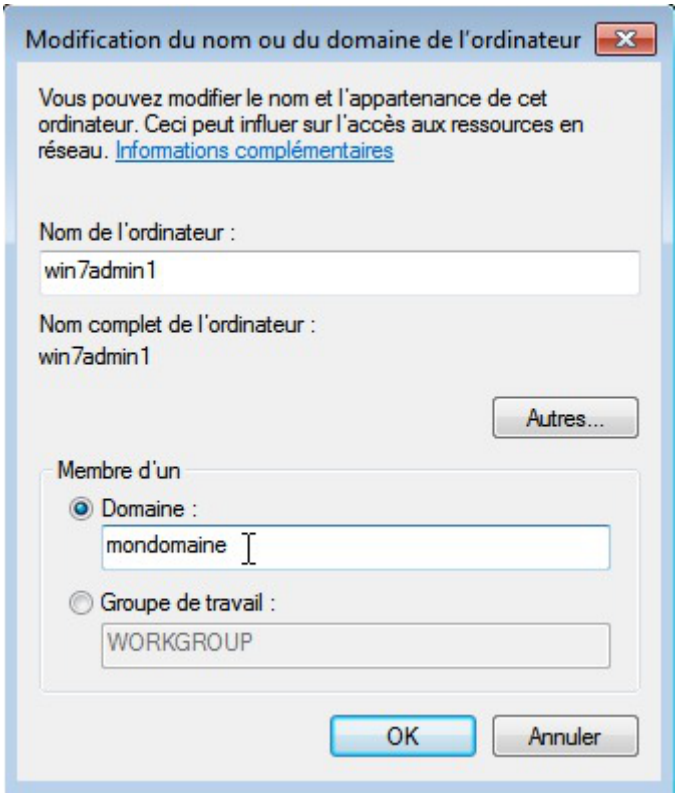


- Cliquer sur Modifier les paramètres ;

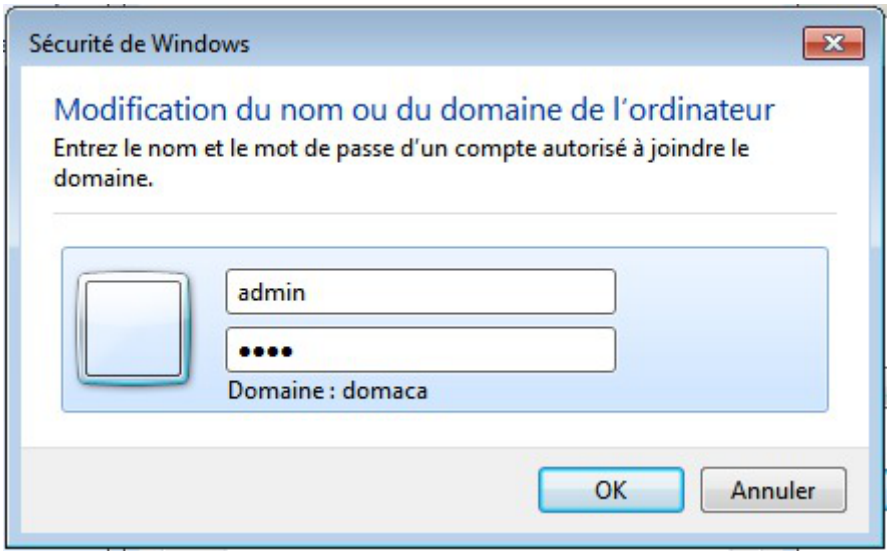


- Cliquer sur le bouton Modifier... ;

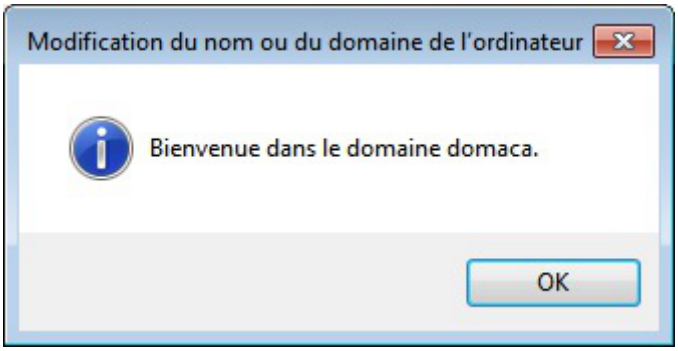
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Renseigner le nom de domaine Samba et cliquer sur `OK` ;

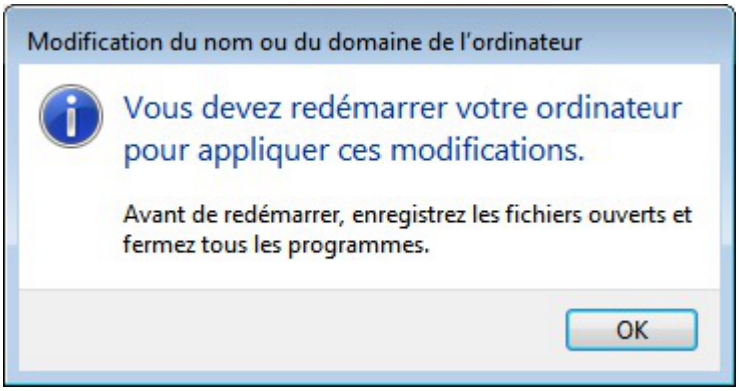


- Utiliser le compte `admin` ou un compte ayant les droits suffisants pour finaliser l'intégration ;

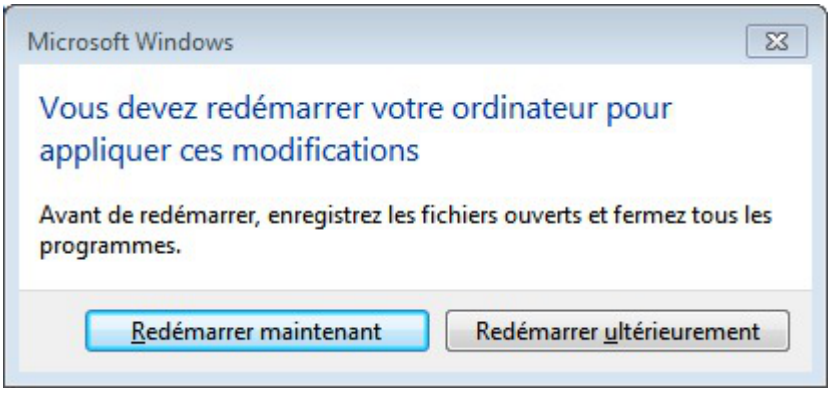


- Confirmer le message de bienvenue ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Confirmer le message d'avertissement ;

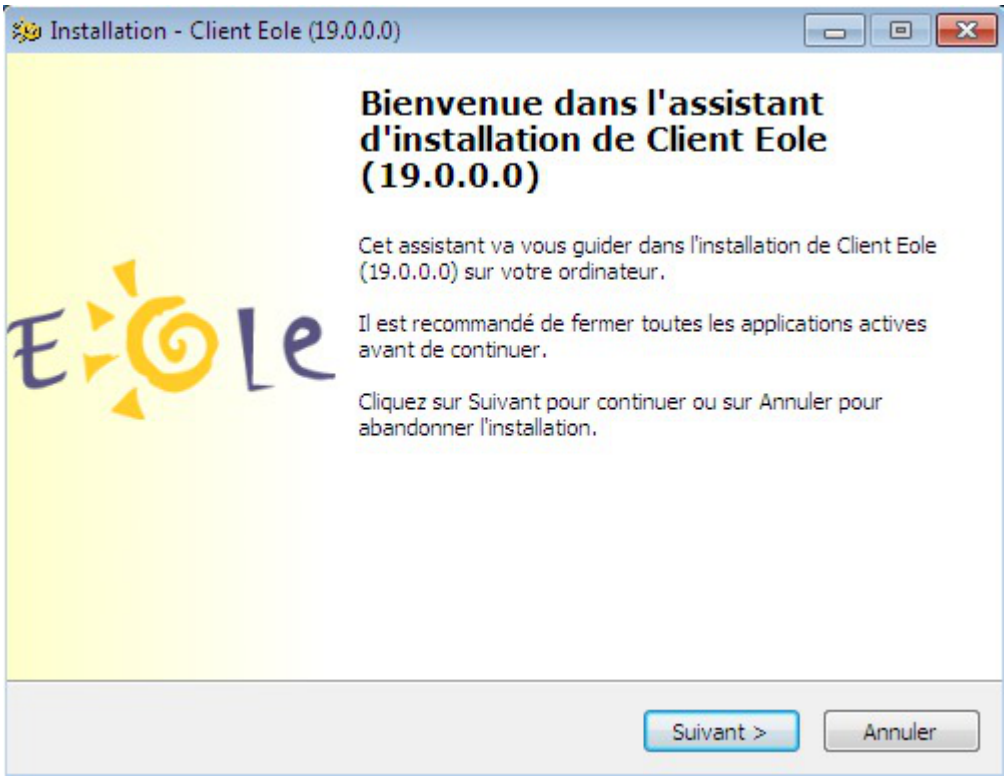


- Redémarrer maintenant.

Installation du client Horus

Installation manuelle du client

L'installeur du client possède un raccourci accessible avec l'utilisateur **admin** dans `U:\Install_Eole_Client`.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une fois installé, le programme d'installation demande un redémarrage.

Après cela, l'ouverture de session suivante devrait ressembler à cela :



Bureau par défaut de l'utilisateur "admin"

Installation et redémarrage automatique

Il est possible d'installer le client en mode automatique à l'aide d'un fichier `.bat` contenant ceci :

```
echo off
rem il faut empecher le redemarrage par le premier installeur
echo Installation du service de mise a jour
U:\client\cliscribe-updater-setup.exe /VERYSILENT /NORESTART
echo Installation du client
U:\client\cliscribe-setup.exe /VERYSILENT
echo redemarrage...
echo on
```

En fin d'installation le système redémarrera sans poser de question.

8.1.5. Mise à jour du client Horus

Le client Horus installé sur les stations Windows est automatiquement mis à jour si une nouvelle version est disponible sur le serveur. L'installeur du client Horus présent sur le serveur est fourni par le paquet *controle-vnc-client*. Autrement-dit, si le paquet *controle-vnc-client* est mis à jour sur le serveur, les clients Windows se mettront automatiquement à jour au prochain redémarrage.

Principe de la mise à jour du client :

- lors de l'installation du client Horus, le fichier `%WINDIR%\Eole\install.ini` est créé. Ce fichier contient la version du client installé ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- à chaque démarrage de la station le service de mise à jour du client vérifie sur le serveur si une nouvelle version est disponible en téléchargeant le fichier `http://<adresse_module>:8790/install.ini` ;
- si une nouvelle version est disponible, le service désinstalle l'ancienne version, redémarre, installe la nouvelle version et redémarre à nouveau.

Le fichier de référence du serveur est `/home/client_horus/install.ini`. (lié pour "*admin*" dans `U:\client\install.ini`).

Les opérations effectuées par le service de mise à jour du client Horus sont journalisées dans `%WINDIR%\cliscribe_updater.log`.

Le service de mise à jour du client Horus est accompagné d'une fenêtre d'indication de l'avancement qui s'affiche lorsqu'un utilisateur ouvre une session pendant la mise à jour du client Horus.



Fenêtre d'avancement de la mise à jour

Si pour une raison précise la mise à jour des clients doit être **ponctuellement** désactivée, il est possible de le faire :

- par station, en renseignant "VERSION = 0" dans le fichier `%WINDIR%\Eole\install.ini` ;
- pour toutes les stations, en renseignant "VERSION = 0" dans le fichier `/home/client_scribe/install.ini`.

Il est fortement déconseillé de désactiver la mise à jour du client parce que :

- le serveur sera à jour et pas le client, certaines actions risquent de ne plus fonctionner ;
- les nouvelles fonctionnalités ne seront pas disponibles ;
- les mises à jour peuvent contenir des corrections de sécurité.

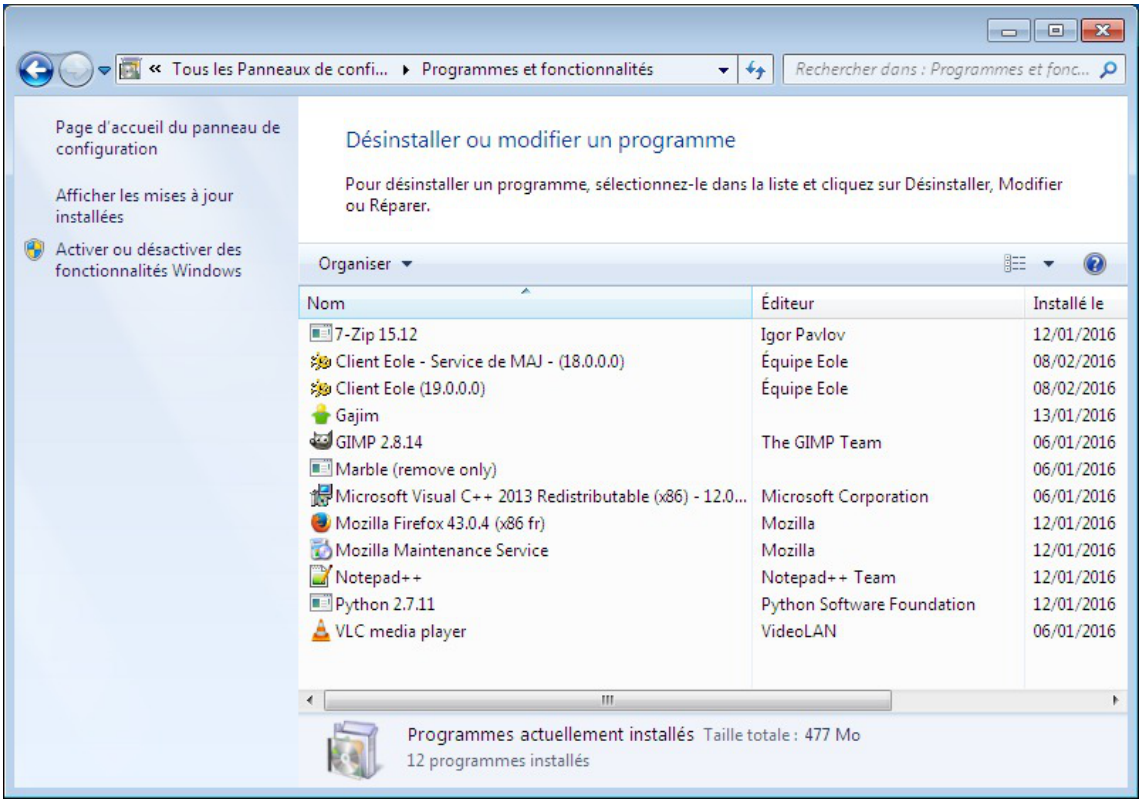
Aucune aide ne pourra être apportée si le client n'est pas à jour.

8.1.6. Désinstallation du client Horus

La désinstallation du client EOLE s'effectue dans :

- `Panneau de configuration`
- `Ajout/Suppression de programmes`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le client EOLE est composé de deux parties :

- le client ;
- le service de mise à jour du client.

Elles sont installées simultanément mais demandent une désinstallation séparée.

Le service de mise à jour du client doit être désinstallé avant le client car, au démarrage de la machine, si le client n'est pas trouvé, le service de mise à jour le réinstallera automatiquement.

8.2. Administration des clients Windows

Afin de faciliter l'administration des clients, divers outils ont été développés et installés sur le module Horus :

- **ESU**, configuration du poste client et de l'environnement de l'utilisateur, composé d'une console et d'un client ;
- l'**EAD**, action sur les postes et les utilisateurs.

Fonctionnement général sous Windows

Sur un module Horus installé de façon standard (pas d'adaptations locales), de l'installation du poste client à sa mise en production, on peut décrire les étapes comme ceci :

- installation du poste client ;
- intégration au domaine Horus ;
- installation du client Horus ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- utilisation.

À cet instant les utilisateurs peuvent utiliser le poste client. Le module Horus est livré avec une configuration ESU par défaut.

Ensuite, via la **console ESU**, l'administrateur ("**admin**" par défaut) peut personnaliser la configuration, ajouter des groupes de machines, des groupes d'utilisateurs, modifier les règles, etc.

Fichiers invisibles sur les partages

Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- desktop.ini : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`). En mode expert, la liste des fichiers cachés peut être personnalisée grâce à la variable `Fichiers à masquer dans le partage` ;
- $recycle.bin : les fichiers `$recycle.bin` générés par le fonctionnement de Windows sont cachés et inaccessibles par l'utilisateur (`veto files = /$RECYCLE.BIN/` dans le fichier `smb.conf`) ;
- .scanned:* : si l'anti-virus temps réel est activé, les fichier `.scanned:*` générés par Scannedonly[p.777] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

8.2.1. Scripts personnalisés

Lorsqu'un utilisateur ouvre une session Windows sur le domaine Horus, le serveur génère un fichier `\\horus\netlogon\<login>.bat`

Ceci est réalisé par l'intermédiaire du programme `/usr/share/eole/fichier/dyn-logon.py` qui génère le script `<login>.bat` en fonction de l'utilisateur, de ses groupes d'appartenance et du système d'exploitation de la station cliente (Win9X, Win2K, WinXP, Vista).

Par défaut, sur le module Horus, seul les lecteurs réseaux des partages de l'utilisateur sont montés par ce script.

Pour ajouter des instructions au fichier `<login>.bat`, il est possible d'utiliser des scripts personnalisés pour :

- un utilisateur particulier : `\\horus\netlogon\users\<login>.bat`
- une machine particulière : `\\horus\netlogon\machines\<machine>.bat`
- un groupe particulier : `\\horus\netlogon\groups\<group>.bat`
- un système d'exploitation particulier : `\\horus\netlogon\os\<os>.bat`
- un groupe et un système d'exploitation : `\\horus\netlogon\os\<os>\<group>.bat`
- un utilisateur et un système d'exploitation : `\\horus\netlogon\os\<os>\<login>.bat`

Le contenu de ces fichiers sera ajouté au fichier `\\horus\netlogon\<login>.bat`



L'éditeur Bloc-note de Windows (`notepad.exe`) ne gère pas correctement les sauts de ligne.

Les fichiers personnalisés édités avec ce logiciel peuvent donc être invalides.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour éditer les fichiers personnalisés sous Windows, il est recommandé d'utiliser `Notepad++` à la place.

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.

Exemples

Pour ajouter une commande à tous les membres du groupe `DomainUsers` mais que pour les postes windows XP, le fichier sera :

`\\horus\netlogon\os\WinXP\DomainUsers.bat`

Pour ajouter une commande à tous les membres du groupe `compta` quelque soit le poste :

`\\horus\netlogon\groups\compta.bat`

Par défaut le contenu sera ajouté au début du fichier et donc avant le montage des lecteurs.

Si vous voulez que le contenu soit ajouté après, il faut insérer `%NetUse%` dans le script personnalisé.

Les lignes suivants cette balise seront ajoutées à la fin du script `<login>.bat`

8.2.2. Les profils utilisateurs

Les profils utilisateurs représentent l'environnement par défaut des utilisateurs.

Il existe trois types de profils qui sont gérés par les modules EOLE :

- le **profil local** :

  il est stocké sur la station Windows, l'environnement est donc différent lorsque l'utilisateur change de poste.

- le **profil itinérant** :

  il est stocké dans le répertoire personnel de l'utilisateur, l'environnement suit l'utilisateur.

- le **profil obligatoire** :

  il est stocké dans un répertoire commun, l'environnement est le même pour tous **mais** il faut générer les profils avant de pouvoir l'utiliser.

Il n'y a rien de particulier à faire pour les profils locaux ou itinérants par contre les profils obligatoires doivent être créés.

Pour plus d'informations concernant les profils d'utilisateurs, veuillez consulter la documentation officielle de Microsoft :

http://technet.microsoft.com/fr-fr/library/cc738303%28v=WS.10%29.aspx

Profils utilisateurs vs ESU

Il est important de distinguer les profils utilisateurs (notion interne à Windows) et ESU.

En effet les profils utilisateurs sont appliqués en premier et définissent un environnement de

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> départ. La configuration ESU est appliquée après et modifie, ajoute ou supprime des paramètres de cet environnement.
>
> Par exemple, le menu démarrer est contenu dans le profil de l'utilisateur mais si un chemin alternatif est défini dans ESU (Console ESU : `Windows => Dossiers`) alors, le menu démarrer utilisé sera celui défini dans ESU, et non celui du profil.

8.2.2.a. Création de profil obligatoire sous Windows XP

Introduction

Le profil obligatoire permet de stocker les paramètres utilisateur et les logiciels installés sur les postes clients. Il est téléchargé depuis le serveur à chaque ouverture de session et supprimé de la station à la fermeture de la session. Les utilisateurs repartent d'un environnement standard à chaque session.

Ces préconisations peuvent être adaptée suivant votre expérience et vos besoins.

Ajout d'un utilisateur spécifique

Il est conseillé d'utiliser un utilisateur fictif pour créer le profil obligatoire.

Cet utilisateur doit être configuré avec un **profil local** et être membre du groupe **DomainAdmins**.

C'est l'utilisateur spécifique **admin.profil** qui sera utilisé pour la suite.

Préparation de la station

Nettoyage de la station

Si des profils autre que locaux (exceptés les profils admin et admin.profil) sont déjà présents sur la machine, il est préférable de les supprimer.

Afin d'éviter des effets de bords, n'installer que les logiciels nécessaires à la génération du profil.

Il arrive que certains logiciels mal programmés paramètrent des valeurs qui provoquent une erreur lorsque le profil est appliqué sur une station où le logiciel n'est pas installé.

Installation des programmes à pré-paramétrer dans le profil obligatoire

Toutes les applications n'ont pas forcément besoin d'être paramétrées dans le profil obligatoire. Il peut arriver que certaines applications n'apprécient pas ce mode de fonctionnement. Il est nécessaire de faire des tests pour en déterminer la liste.



> L'utilisation d'un logiciel de virtualisation (proposant l'enregistrement de l'état à un instant t) permet d'installer une version propre de Windows et de repartir du profil utilisé lors de la dernière copie.

Génération du profil

Pour générer un profil prêt à être copié il faut pré-paramétrer les applications, l'explorateur et le bureau :

- ouvrir une session avec l'utilisateur "*admin.profil*" sur un client XP ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- utiliser les logiciels installés (LibreOffice, Firefox, Encyclopédies, etc.) ;
- supprimer le fond d'écran pour éviter sa diffusion sur les autres profils (paramètres Windows ou clic droit sur le bureau) ;
- fermer la session.

Le profil est prêt à être copié.

Les préférences de vue des fichiers

- ouvrir le poste de travail ;
- dans le menu `Affichage` ;
- sélectionnez `Détails` ;
- fermer la fenêtre

Lorsque les utilisateurs ouvriront le Poste de travail, les informations sur les fichiers seront affichées en "Détails".

La validation d'une licence

Par exemple le logiciel privateur Acrobat Reader demande, lors de son premier lancement, de valider sa licence.

Cette question est posée une fois par session à un utilisateur "profil obligatoire", la validation n'étant pas retenue lors de la fermeture de session.

Pour résoudre ce problème il faut valider la licence lors de la génération du profil avec *admin.profil.*

Ce type de comportement (validation, paramètres non retenus d'une session à l'autre) est généralement lié au profil obligatoire. Les informations sont enregistrées dans une partie du profil fourni par le profil obligatoire.

Ceci est à opposer aux informations stockées dans le répertoire `Applications Data` redirigé par défaut par ESU dans le répertoire `U:\.Config\Applications Data`.

Ces dernières informations sont donc retrouvées lors de la prochaine ouverture de session. Par exemple, LibreOffice enregistre la validation de sa licence une fois pour toutes.

Le fond d'écran bénéficie d'une gestion particulière dans ESU :

- la spécification d'un fichier image à afficher
- l'ajout d'informations textuelles en haut à droite.

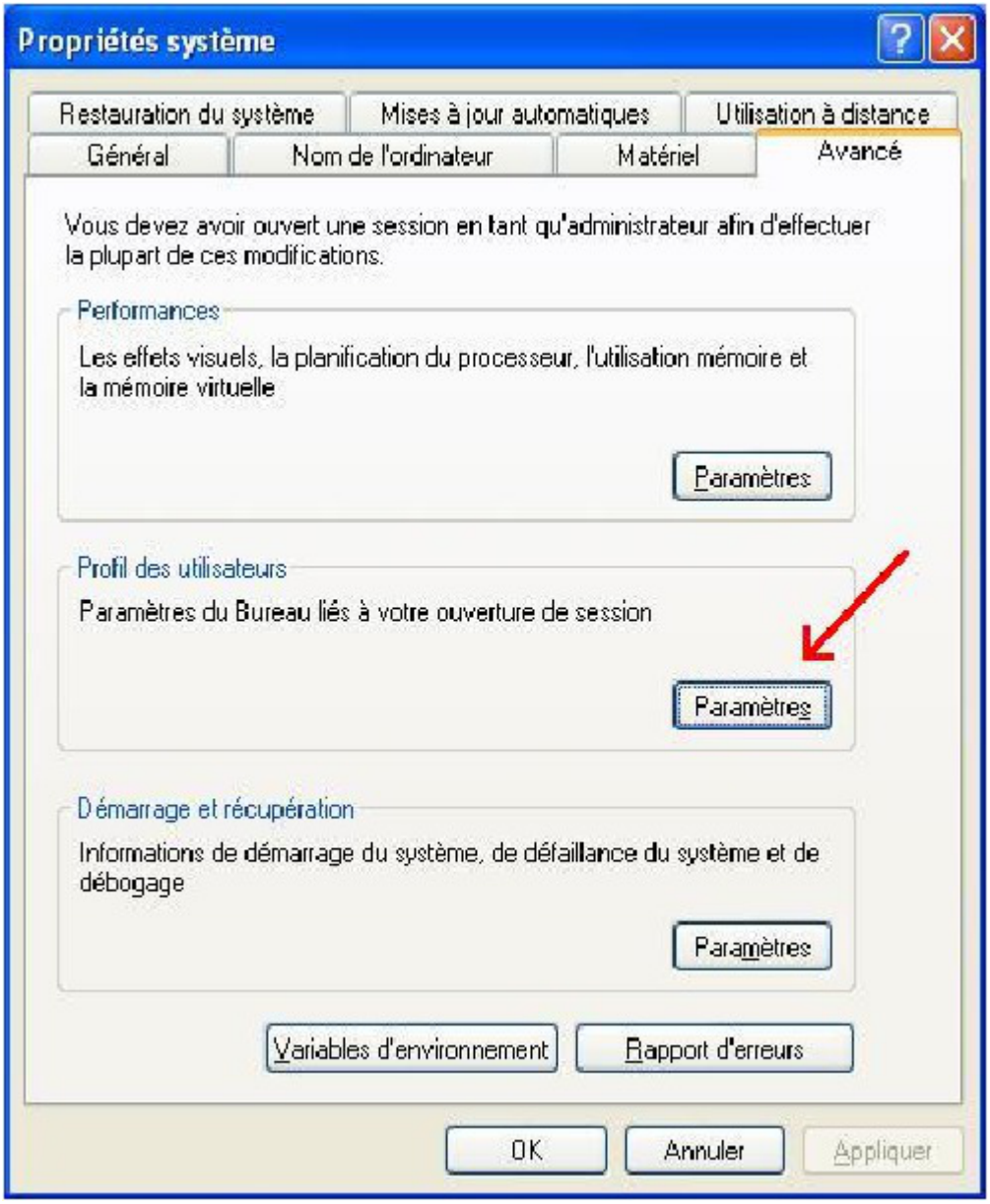
Les deux étant incompatibles, il vaut mieux le désactiver pour éviter tout effet de bord. Pour se faire sélectionner `Aucun` dans `Propriétés de l'affichage/Bureau/Arrière-plan`.

Copie du profil

Ouvrir une session avec l'utilisateur `admin`. Aller dans le `Panneau de configuration` → `Système` → `Propriétés` → `Avancé`. Dans le cadre `Profil des utilisateurs` cliquer sur `Paramètres`.

Dans la nouvelle fenêtre, sélectionner le profil correspondant à l'utilisateur `admin.profil`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



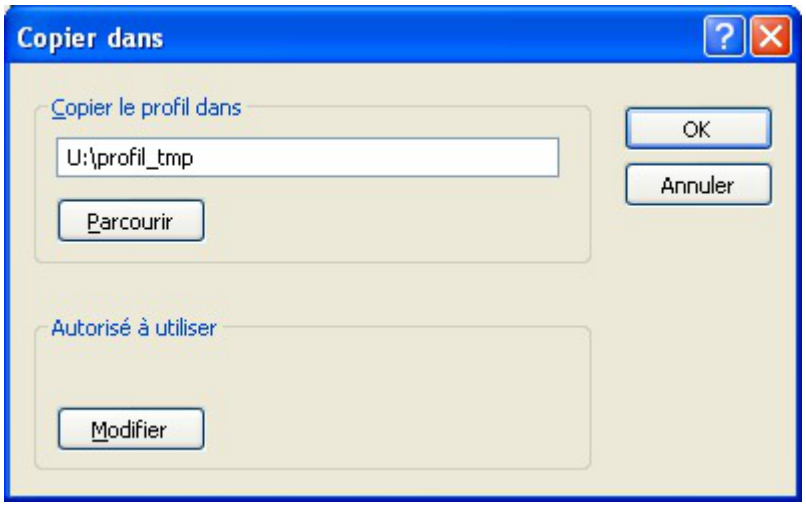
Dans la partie Autorisé à utiliser cliquer sur Modifier. Entrer tout le monde puis cliquer sur Vérifier les noms.



Et cliquer sur OK.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Dans le champ Copier le profil dans indiquer un répertoire temporaire non existant ou vide (un sous répertoire du répertoire personnel de l'utilisateur `admin` par exemple) et cliquer sur OK.



Une fois le profil copié la dernière fenêtre se ferme automatiquement.

Copier ensuite le contenu du dossier dans : \\<adresse_serveur>\netlogon\profil

Sur le module Scribe, il est également possible d'utiliser le dossier \\<adresse_serveur>\netlogon\profil2

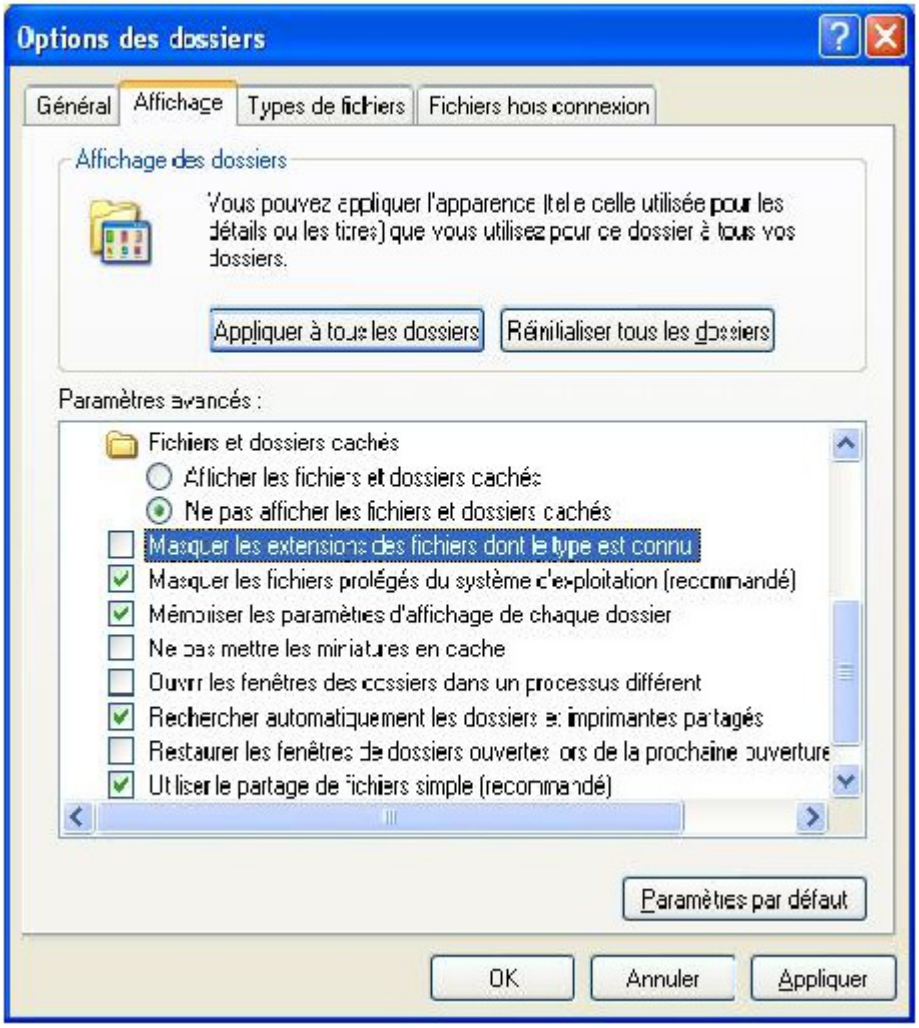
Ceci permet de spécifier un profil différent pour certains utilisateurs (ex. : profil pour les professeurs et profil2 pour les élèves).

> Lorsque le profil est copié directement sur le serveur dans le répertoire \\<adresse_serveur>\netlogon\profil\ , Windows applique automatiquement les droits d'écriture à tout le monde sur le dossier profil.
>
> Le passage par un répertoire temporaire évite d'avoir à manipuler les droits et diminue le risque d'erreur.

Dans le dossier \\<adresse_serveur>\netlogon\profil\ renommer le fichier ntuser.dat en ntuser.man (ne pas confondre avec un éventuel fichier ntuser.dat.txt).

Pour y parvenir il faut d'abord afficher les extensions des fichiers connus (dans l'explorateur, " Outils/Options des dossiers.../Affichage ", décocher "☑ Masquer les extensions des fichiers dont le type est connu ").

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le profil obligatoire est désormais fonctionnel.

Si des difficultés sont rencontrées lors de la copie du profil sur le serveur, une solution consiste à renommer le dossier et à en créer un nouveau.

8.2.2.b. Création de profil obligatoire sous Windows 7

Pour générer un profil obligatoire sous Windows 7, la marche à suivre est à peu près la même que pour Windows XP :

1. créer un utilisateur `admin.profil` possédant un profil local ;
2. ouvrir une session avec `admin.profil` ;
3. paramétrer le profil et fermer la session ;
4. ouvrir une session avec `admin` pour copier le profil.

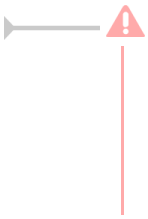
La subtilité se trouve ici, sous Windows 7 le bouton `Copier vers` est grisé pour les utilisateurs du domaine.

Une des solutions permettant de contourner le problème est d'utiliser un utilitaire nommé `Windows Enabler`.

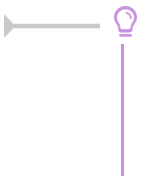
Sous Windows 7 SP1, pour que `Windows Enabler` fonctionne, il faut impérativement désactiver l'

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

UAC[p.781] et redémarrer la machine.



Comme pour Windows XP, il ne faut pas copier le profil directement vers `\\scribe\netlogon\profil.V2` mais plutôt passer par un dossier temporaire (exemple `U:\profil_seven`). Sans ça Windows va automatiquement placer des ACLs trop permissives sur le dossier `profil.V2` ce qui risque d'entraîner des dysfonctionnements.



Pour Windows Vista et Windows 7, le suffixe `.V2` est ajouté à la fin du chemin du profil.

A part ajouter cette extension au dossier dans lequel le profil est copié, il n'y a rien à paramétrer.

8.2.2.c. Les sessions locales

Si des chemins ont étés modifiés par ESU (`Groupe de machine` → `Windows` → `Dossiers`), à l'ouverture d'une session locale le programme `logon.exe` redéfinit les chemins d'accès aux icônes du *Menu démarrer* et du *Bureau* avec leurs valeurs par défaut.

En effet, les lecteurs réseaux peuvent être indisponibles lors de l'ouverture d'une session locale.

Sous Windows Vista et Windows 7 ce processus nécessite une élévation de droits au niveau de l'U[p.781]AC[p.781].

Le programme `logon.exe` affiche alors la question : `Ré-initialiser le Menu démarrer et le Bureau` ? suivit par celle de l'UAC[p.781] (si il est activé) pour la validation de l'action.

L'UAC[p.781] est un mécanisme censé protéger le système d'actions malencontreuses ou frauduleuses.

Lorsqu'un utilisateur, même *Administrateur*, effectue une action requérant des privilèges d'administrateur (lancement de `regedit.exe`, configuration du réseau, installation de nouveaux programmes, etc.), l'UAC bloque l'action et affiche une demande de confirmation pour l'exécution de l'action.

L'UAC n'est pas indispensable, il peut donc être désactivé.

8.2.3. Gestion des configurations clientes avec ESU

8.2.3.a. Introduction

Présentation

ESU[p.761] pour Environnement Sécurisé des Utilisateurs est une application de gestion avancée des postes clients.

Il permet de configurer le poste de travail à l'ouverture de session en fonction du nom de l'utilisateur ou des groupes dont il est membre et du nom de la machine cliente.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les fonctionnalités principales d'ESU sont :

- paramétrage des restrictions sur le poste (par exemple : désactivation de la modification de l'heure, masquer des lecteurs dans le poste de travail, etc.) ;
- affichage d'un fond d'écran avec possibilité d'y inscrire des informations complémentaires ;
- installation d'imprimantes réseau (possibilité de coupler avec l'auto-installation des pilotes) ;
- paramétrage d'applications (par exemple : page de démarrage Firefox) ;
- redirection de dossiers vers un lecteur réseau (Ex. : Mes Documents, Bureau, Menu Démarrer) ;
- interdiction d'accès à un groupe de machines à certains utilisateurs.

Ces fonctionnalités sont représentées sous forme de règles dans le fichier de référence `\\<adresse_serveur>\esu\Console\ListeRegles.xml`

ESU est pleinement compatible Windows 98/Me/2k/2k3/XP/Vista.

Structure générale de l'outil

ESU se compose de deux parties :

- la console, qui sert à paramétrer l'ensemble des règles ;
- le client, qui applique les règles sur le poste.

Le dossier `\\<adresse_serveur>\esu\Console` contient la console, des modèles de groupes de machines et d'utilisateurs et l'éditeur de la liste de règles.

Le dossier `\\<adresse_serveur>\esu\Base` contient les paramètres définis dans la console ESU.

8.2.3.b. La console ESU

> Présentation

La console ESU sert à paramétrer les règles qui seront appliquées sur les machines clientes lors de l'ouverture de session. La liste des règles disponibles est définie dans le fichier `\\<adresse_serveur>\esu\Console\ListeRegles.xml`. Elles sont réparties en deux groupes :

- les règles "machines" définissant le comportement global des machines, elles sont appliquées quelque soit l'utilisateur qui se connecte ;
- les règles "utilisateurs" définissant l'environnement de l'utilisateur comme les restrictions, le paramétrage de l'explorateur et du fond d'écran, etc.

Par défaut, seul l'utilisateur **admin** a accès à la console. Pour faciliter l'accès un raccourci est créé dans son répertoire personnel (U:).

La console est organisée en trois parties :

- la première liste les groupes de machines du domaine, et les utilisateurs/groupes gérés dans ce groupe de machines ;
- la seconde contient les différentes catégories de règles. Ces catégories peuvent comporter des sections ;
- la troisième partie affiche les règles et leur paramétrage.

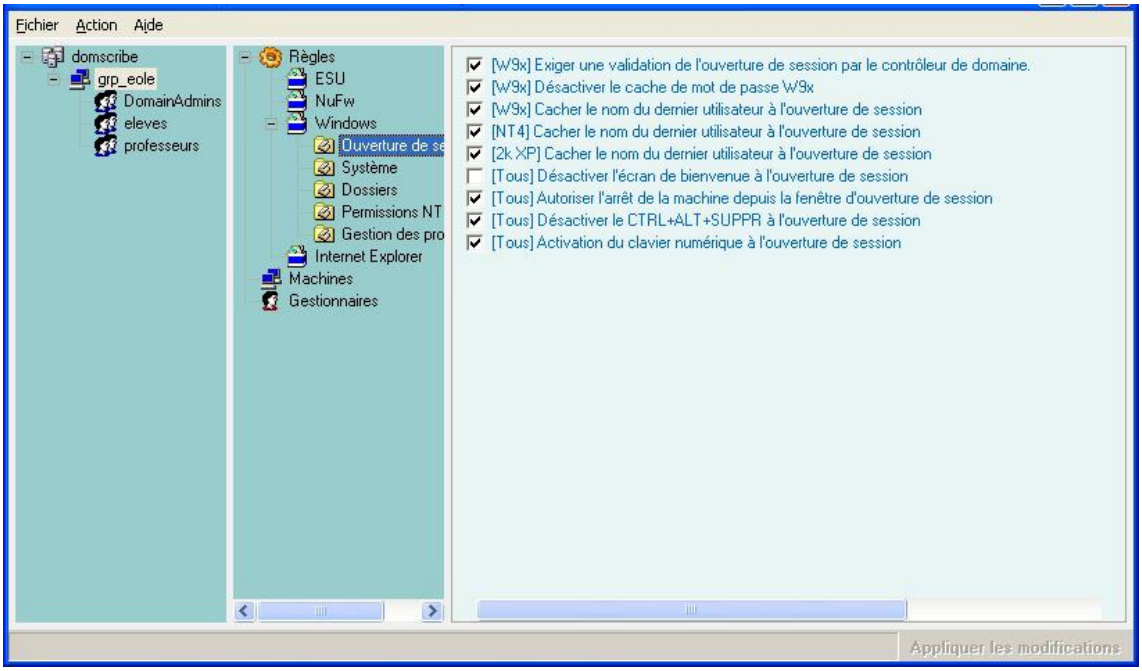
La première colonne montre l'organisation générale d'ESU. La première ligne indique le nom du domaine.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Celui-ci contient un ensemble de groupes de machines définis en fonction du nom des machines. Chaque groupe de machine contient des utilisateurs ou des groupes d'utilisateurs.

Lors de l'ouverture de session, ESU va chercher à quel groupe de machines appartient la machine sur laquelle l'utilisateur se connecte. Si un groupe de machine est trouvé, ESU va chercher s'il contient l'utilisateur ou un des groupes auxquels l'utilisateur appartient.

La liste des groupes de machines et des utilisateurs est parcourue du haut vers le bas. Si une machine appartient à plusieurs groupes, le premier sera utilisé, les autres ignorés. Il en va de même pour les utilisateurs/groupes d'utilisateurs.



Fenêtre principale d'ESU

> Les groupes de machines

Création d'un nouveau groupe de machines

Les groupes de machines servent à regrouper les machines dans une même configuration en fonction de leur nom.

A l'installation du module, ESU est pré-configuré avec un groupe de machines *grp_eole* paramétré afin de prendre en compte toutes les machines du domaine (Simplement le caractère "*****").

Ce groupe de machines a été pré-créé afin de servir d'exemple et pour que l'installation du client Scribe soit suffisante pour obtenir une station pleinement fonctionnelle dès la première ouverture de session.

Pour créer votre propre groupe, faites un clic droit sur le *domaine* et sélectionnez "**Nouveau groupe de machines**" ou sélectionnez le domaine et utilisez le raccourci clavier Ctrl+N .

Renseignez le nom du groupe de machine (ici *technologie*) et paramétrez les noms des machines à ajouter au groupe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ajout des noms de machines appartenant au groupe

Par défaut les nouveaux groupes de machines sont créés en utilisant le modèle ESU `U:\esu\Console\Modeles\GM\GroupeMachine_[Scribe].xml`.

Ce modèle ajoute automatiquement les groupes *DomainAdmins*, *eleves* et *professeurs* avec un ensemble de règles pré-configurées (dossier redirigés, restrictions, etc.).

Il est possible de prendre en compte plusieurs machines en une fois en utilisant le caractère étoile, exemple : "techno*".



Utilisation du jocker (*) pour paramétrer les noms de machines prises en compte par le groupe

Une fois le groupe de machines créé, il faut établir sa priorité par rapport au groupe de machine *grp_eole* (si il n'a pas été supprimé) : clic droit sur le groupe de machine et choisir "**Augmenter la priorité**".



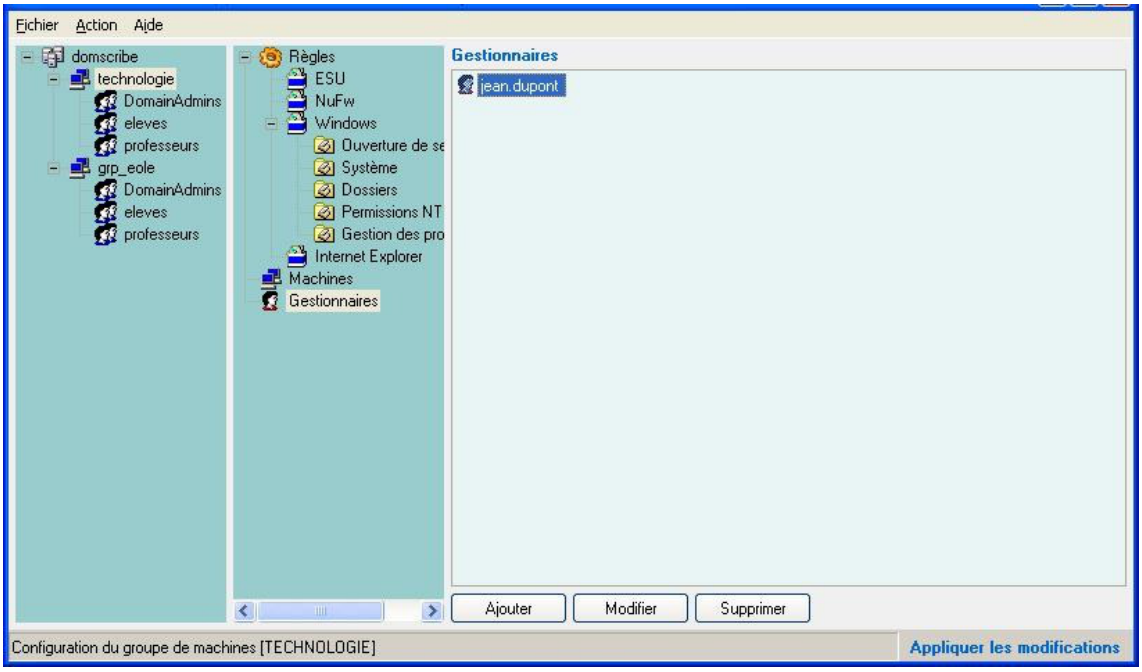
Augmenter la priorité d'un utilisateur

Les Gestionnaires

L'item "**Gestionnaires**" permet de déléguer l'administration d'un ou plusieurs groupes de machines à un autre utilisateur ou à un autre groupe. Lorsqu'un utilisateur lance la console, il n'a accès qu'aux groupes de machines pour lesquels il est défini comme gestionnaire.

Le gestionnaire peut modifier la configuration ESU de son groupe de machines et a aussi accès en écriture au répertoire contenant les icônes (`I:\<nom_du_groupe_de_machines>\`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ajout de gestionnaires dans un groupe de machines

Il est également possible d'ajouter un gestionnaire au niveau du domaine. Il aura le droit d'administrer l'ensemble des groupes de machines définis dans ESU et d'en ajouter

Lorsqu'un utilisateur est gestionnaire ESU il est automatiquement inscrit au groupe `Administrateurs` de la ou des machines Windows concernées.

Le groupe DomainAdmins

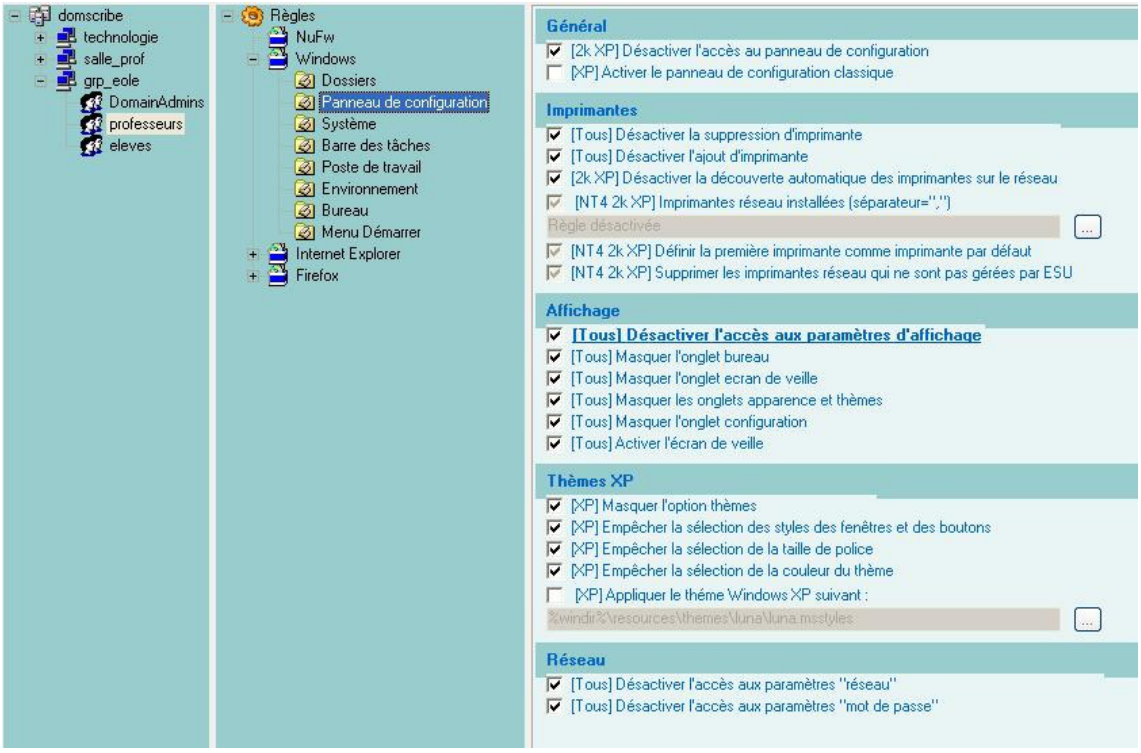
Les membres du groupes DomainAdmins ont un accès complet à la console Esu sans qu'il ne soit nécessaire de les ajouter comme gestionnaires.

D'une manière générale, les membres du groupe DomainAdmins ont les droits d'écriture (donc de suppression) sur l'ensemble des partages du serveur (partages groupe, dossiers personnels, Esu, etc.).

> Les utilisateurs et groupes d'utilisateurs

Un environnement différent peut être appliqué en fonction du nom de l'utilisateur ou des groupes auxquels il appartient.

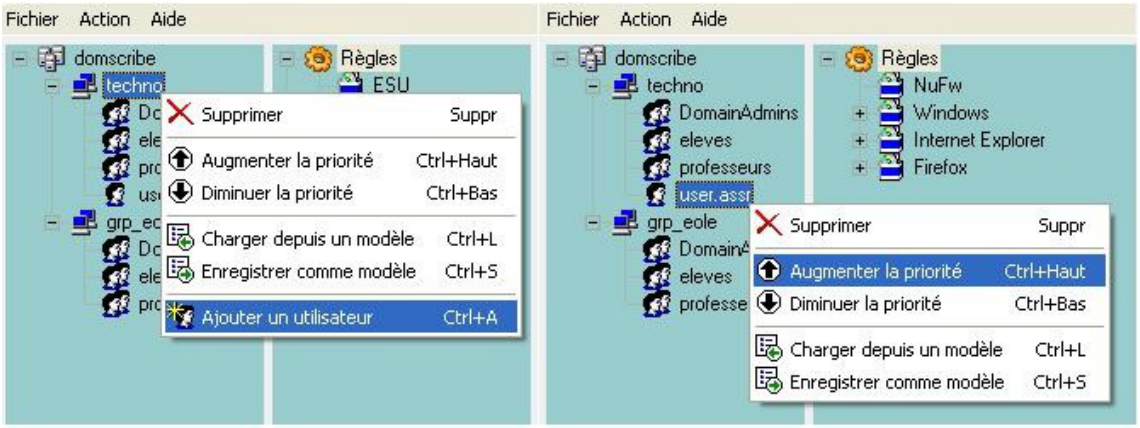
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Exemple de paramétrage de règles pour un utilisateur ou un groupe d'utilisateurs

Création d'un nouveau groupe d'utilisateurs dans un groupe de machines.

Un clic droit sur le nom du groupe de machine permet d'ajouter un utilisateur ou un groupe. Un clic droit sur l'utilisateur ou le groupe permet de le supprimer ou de régler sa priorité.



Ajouter un utilisateur ou un groupe d'utilisateurs

Comme pour les groupes de machines, les utilisateurs et groupes sont parcourus de haut en bas. ESU s'arrête à la première correspondance.

Ici, l'utilisateur *user.assr* fait partie du groupe *eleves*. Pour lui appliquer une configuration spécifique, il faut lui affecter une priorité supérieure à celle du groupe *eleves*.



Augmenter la priorité d'un utilisateur

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Les imprimantes

Dans la partie règle utilisateurs, que l'on obtient en cliquant sur un groupe d'utilisateurs dans la colonne de gauche, sélectionner "*Panneau de Configuration*" section "*Imprimantes*".

A cet endroit vous pouvez spécifier le chemin UNC (\\<scribe>\<imprimante>) d'accès aux imprimantes disponibles pour ce groupe de machine et ce groupe d'utilisateur.

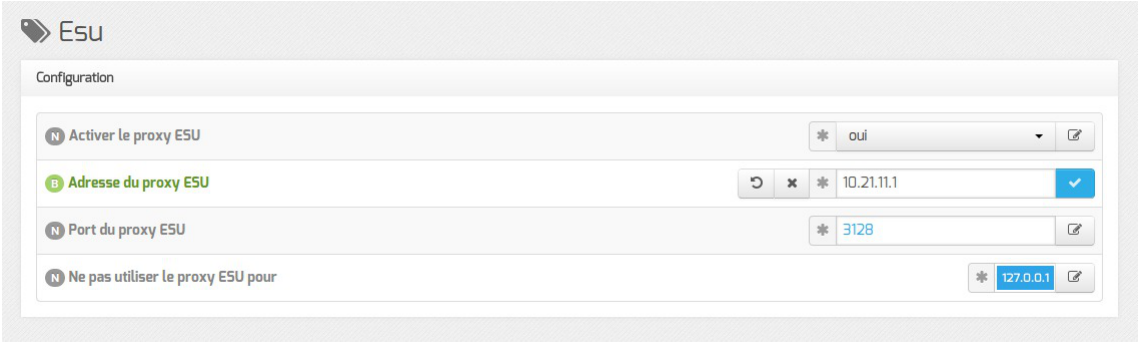
Ainsi élèves et professeurs peuvent avoir des imprimantes différentes sur un même poste et un utilisateur peut avoir des imprimantes différentes en fonction du poste et du groupe de machines auquel il appartient.

> Le proxy

Depuis la version EOLE 2.3, la configuration du proxy ESU s'effectue dans l'interface de configuration du module.

Sur les modules Scribe, AmonEcole et AmonEcole+, l'utilisation du couple ESU / ClientScribe est obligatoire pour les stations Windows Microsoft rattachées au domaine et l'onglet `Esu` est d'emblée visible.

Sur les autres modules, l'onglet `Esu` n'est visible qu'après activation du service dans l'onglet `Services` en passant l'option : `Utiliser le logiciel ESU` à `oui`.



Vue de l'onglet Esu de l'interface de configuration du module

La configuration du proxy pour des stations clientes gérées par ESU s'effectue au niveau de l'interface de configuration du module dans l'onglet `Esu`.

Après avoir passé la variable `Activer le proxy ESU` à `oui` il faut saisir l'adresse IP ou le nom du proxy ESU dans le champ `Adresse du proxy ESU` et si besoin changer le port 3128 proposé par défaut.

Le champ `Ne pas utiliser le proxy ESU pour` permet d'ajouter plusieurs adresses IP, réseaux, noms de domaine et noms de machines pour lesquels le proxy ESU ne sera pas utilisé (exemple de valeurs : `mozilla.org`, `asso.fr`, `192.168.1.0/24`).

Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet `Interface-1` (variable : `adresse ip eth1 proxy link`).

L'utilisation du logiciel ESU modifie profondément la configuration des stations clientes

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

(emplacement des icônes, ...) et sa désactivation ne restaure pas leur configuration d'origine.

Pour récupérer une station utilisable hors du domaine, vous pouvez :

- ré-activer ESU, renseigner les options telles qu'elles sont sur un Windows par défaut (cases décochées), ouvrir une session et désactiver ESU ;
- restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG[p.752] tels que celui fourni par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

Dans le cas où, sur le module Horus, on active ESU, il devient obligatoire d'installer le logiciel client Horus.

À l'inverse, l'installation du client sans procéder à l'activation d'ESU n'a pas de sens.

> Trucs et astuces

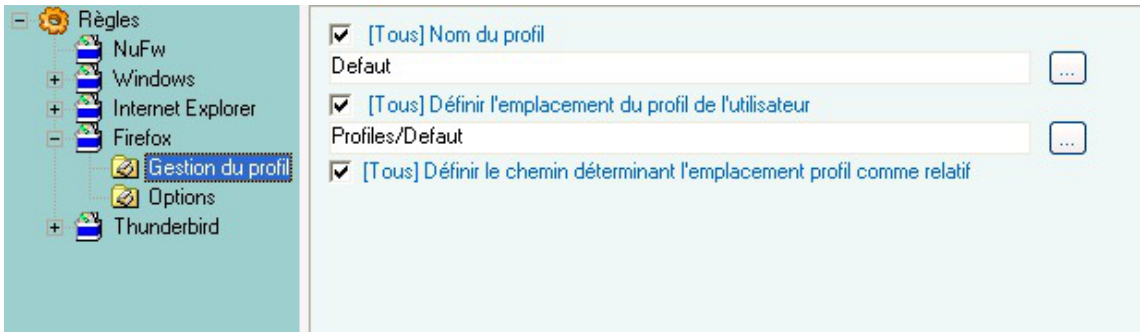
Les dossiers d'icônes

- les icônes placées dans `R:\grp_eole\_Machine\Bureau` seront visibles par tous les utilisateurs ;
- les icônes placées dans `R:\grp_eole\professeurs\Bureau` ne seront visibles que par les professeurs.

Attention, l'utilisateur *admin* fait partie du groupe *professeurs* mais, il est également membre du groupe *DomainAdmins*. Au vu des priorités, c'est le dossier défini d'icônes du groupe *DomainAdmins* (`R:\grp_eole\professeurs\Bureau`) qui lui sera proposé.

Firefox

Afin de paramétrer correctement la *Gestion du profil* Firefox avec ESU, il faut sélectionner au moins une *Option*, la page de démarrage par exemple.



Configuration ESU du profil Firefox

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

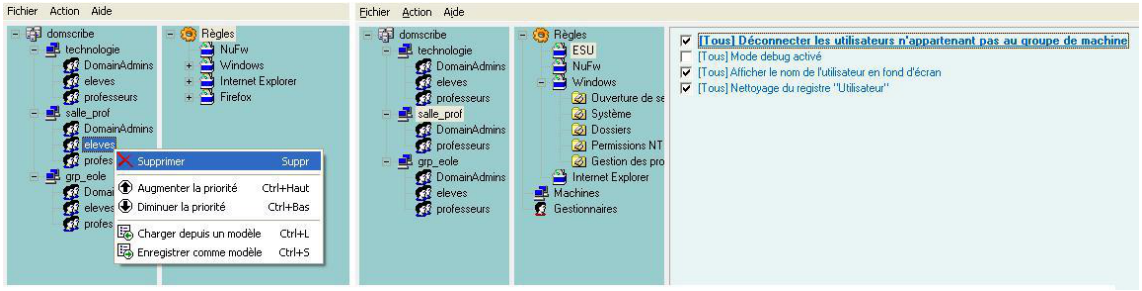


Configuration ESU des options Firefox

Accès limité à un poste en fonction de l'utilisateur

Pour limiter l'accès à un poste, il suffit de ne configurer que les groupes d'utilisateurs autorisés et de cocher *Déconnecter les utilisateurs n'appartenant pas au groupe de machines*.

Ici les utilisateurs ne faisant pas partie des groupes *DomainAdmins* ou *professeurs* (par exemple les élèves) seront déconnectés automatiquement.



Limiter l'accès à un poste

Modèles de restrictions

Des modèles pré-configurés sont livrés avec ESU :

Pour les groupes de machines

- U:\esu\Console\Modeles\GM\GroupeMachine_[Scribe].xml

Ce modèle est utilisé par défaut lors de la création d'un groupe de machines.

Pour les groupes d'utilisateurs

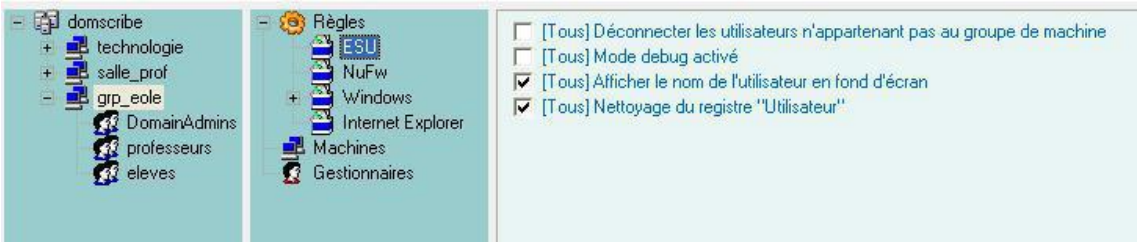
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_DomainAdmins[Scribe].xml
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_eleves[Scribe].xml
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_professeurs[Scribe].xml

Ces modèles peuvent être utilisés lors de l'ajout d'un utilisateur ou d'un groupe dans un groupe de machines (ex. *user.assr*).

8.2.3.i. Personnalisation du fond d'écran

Il est possible de modifier le contenu du texte à afficher sur le fond d'écran lorsque l'option *Afficher le nom de l'utilisateur en fond d'écran* est cochée dans la Console ESU.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



La personnalisation s'effectue par utilisateur ou groupe d'utilisateurs à l'aide d'un fichier texte ayant l'extension **.bgd**. Ce fichier doit se trouver dans *U:\esu\Base***<groupe_de_machine>**\ **<utilisateur_ou_groupe>***.bgd*.

Pour modifier le texte du fond d'écran pour les membres du groupe *DomainAdmins* dans le groupe de machine *grp_eole*, créer le fichier **U:\esu\Base\grp_eole\DomainAdmins.bgd**.

Ce fichier peut contenir des variables suivantes :

- Toutes les variables d'environnement Windows (%WINDIR%, %PATH%, ...)
- %ESU_PROXY_HOST%
- %ESU_PROXY_PORT%
- %ESU_PROXY_BYPASS%
- %ESU_PDC%
- %ESU_DOMAINE%
- %ESU_OS%
- %ESU_PARTAGE_ICONES%
- %ESU_LECTEUR_ICONES%
- %ESU_GU%#%ESU_GM%
- %USERNAME%
- %USERLNAME%
- %GROUPES%
- %SID%
- %IP%

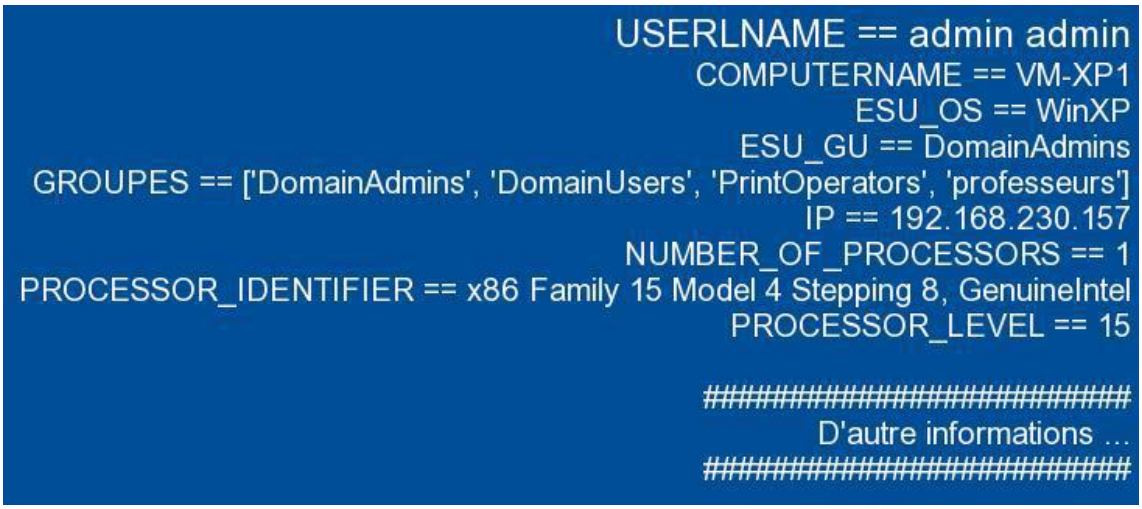
Exemple de configuration personnalisée du texte en fond d'écran

Contenu du fichier :

USERLNAME == %USERLNAME%
COMPUTERNAME == %COMPUTERNAME%
ESU_OS == %ESU_OS%
ESU_GU == %ESU_GU%
GROUPES == %GROUPES%
IP == %IP%
NUMBER_OF_PROCESSORS == %NUMBER_OF_PROCESSORS%
PROCESSOR_IDENTIFIER == %PROCESSOR_IDENTIFIER%
PROCESSOR_LEVEL == %PROCESSOR_LEVEL%
########################

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

D'autre informations ...
##########################
Résultat :



Si l'utilisateur possède un profil local et que l'option ESU `GroupeMachine > GroupeUsers > Windows > Bureau > Papier peint > Chemin vers l'image appliquée en fond d'écran` est grisée, le texte par défaut et le texte personnalisé se superposent.

8.3. Déploiement d'applications pour Windows avec WPKG

WPKG est une application de déploiement d'applications pour Windows.
Elle permet l'installation, la mise à jour et la dés-installation automatique de logiciels.
http://wpkg.org/
L'application WPKG est composée d'un exécutable (`wpkg.js`) et de fichiers de configuration XML copiés dans un dossier partagé sur le serveur de fichier.
Les fichiers XML sont séparés en 3 parties :

- **packages**, les applications installables ;
- **hosts**, les postes ou groupes de postes ;
- **profiles**, la liste de packages à installer pour un host.

Le fichier `wpkg.js` doit être exécuté sur les postes Windows. Il lit les fichiers XML (`config/host/profiles/packages`) et installe en conséquence les applications sur les postes.
Afin d'exécuter `wpkg.js` automatiquement il faut utiliser un lanceur, au choix :

- WPKG Client ;
- Wpkg-GP ;
- une tâche planifiée Windows ;
- n'importe quel autre programme capable d'exécuter wpkg.js.

Dans le cas de l'utilisation de WPKG Client et de Wpkg-GP, ils s'installent sous forme de service Windows et s'exécute au démarrage de la machine.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

WPKG Client peut également s'exécuter à l'arrêt du poste.

Les fichiers de configuration sont les suivants :

- wpkg.js (ou moteur WPKG) : `config.xml` ;
- WPKG Client : `settings.xml` ;
- Wpkg-GP : `wpkg-gp.ini`.

8.3.1. Installation et configuration

Installation et utilisation de WPKG sur un serveur EOLE

WPKG peut être utilisé sur un serveur Scribe ou Horus si le paquet `eole-wpkg` est installé.

Le paquet s'installe avec la commande :

```
# apt-eole install eole-wpkg
```

L'application WPKG est alors est stockée dans le répertoire partagé `\\<SERVEUR>\wpkg`

Elle est paramétré en accès anonyme et en lecture seule (lecture/écriture pour DomainAdmins).

L'accès au répertoire partagé wpkg n'étant pas très pratique, on peut ajouter un lien symbolique dans le dossier personnel (U:) de l'utilisateur admin (comme c'est déjà le cas pour le partage esu) :

```
# ln -s /home/wpkg/ /home/a/admin/perso/wpkg
```



Le paquet `eole-wpkg` fournit les dictionnaires et templates permettant de gérer la configuration de WPKG depuis le serveur Zéphir.

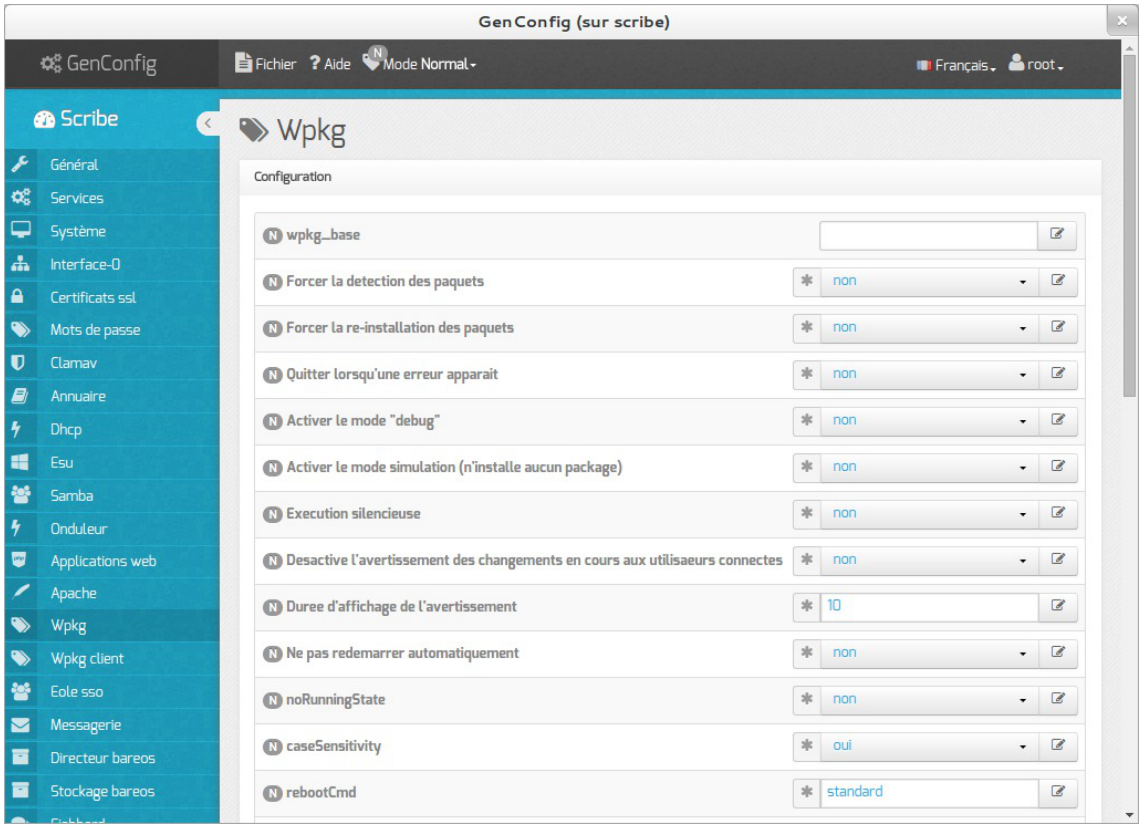
Configuration

L'outil de gestion de la configuration est l'interface de configuration du module.

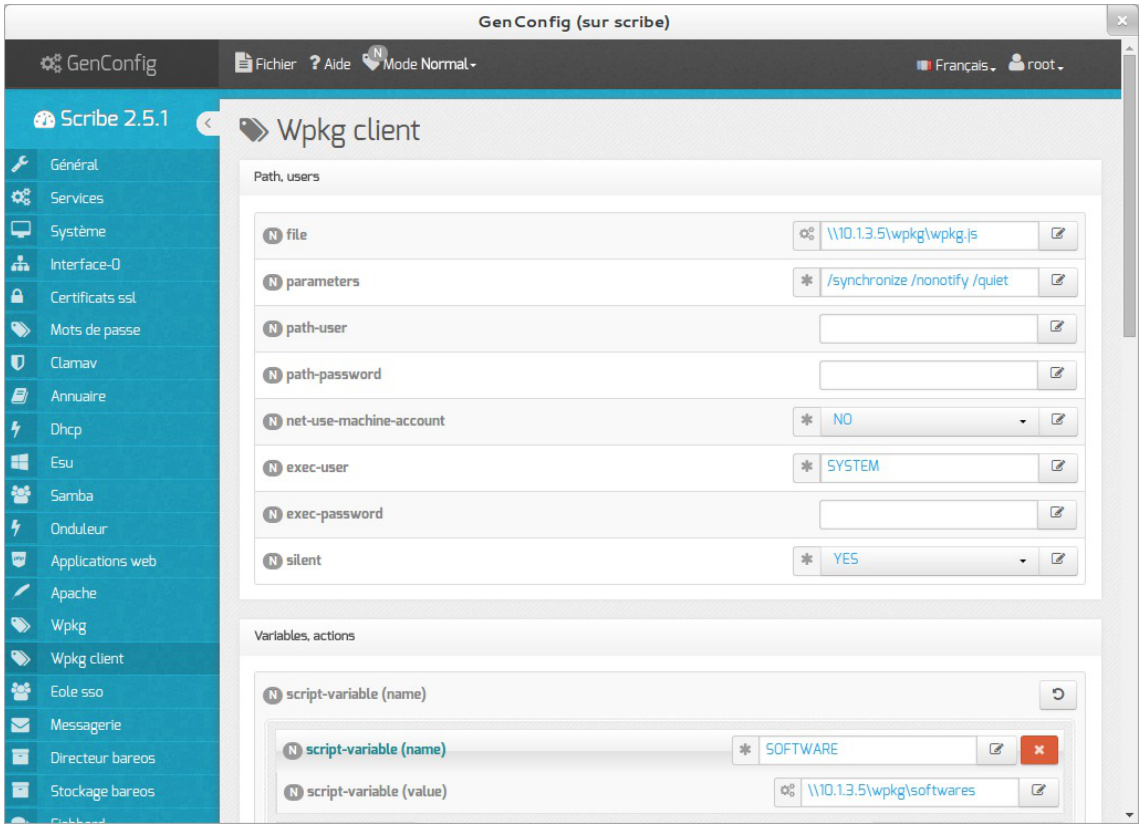
Dans l'interface de configuration du module, dans l'onglet `Services`, le service `Gérer la configuration WPKG` est à `oui` par défaut et 2 onglets concernant WPKG sont visibles :

- Wpkg : les options paramétrables du fichier `config.xml` (options de wpkg.js)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Wpkg client : les options paramétrables des fichiers `settings.xml` (WPKG Client) et `wpkg-gp.ini` (Wpkg-GP)



#fixme compléter l'essentiel de la configuration

Il faut ensuite reconfigurer le serveur à l'aide de la commande `reconfigure` :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# reconfigure
```

Installation du client WPKG

Il existe plusieurs façons d'exécuter le moteur `wpkg.js` sur un poste Windows. Il est recommandé d'utiliser les applications suivantes :

- WPKG Client pour Windows XP : http://wpkg.org/files/client/stable/
- Wpkg-GP pour Windows Vista et supérieurs : https://drive.google.com/folderview?id=0B9Eadi-crzpOVEtTM01aYm5YNm8&usp=drive_web



Il ne faut installer que l'un des deux, installer WPKG Client et Wpkg-GP sur la même machine provoque des comportements inattendus.

Des scripts `.bat` permettent une installation des clients sans question. Pour que ces scripts fonctionnent il faut télécharger les clients en prenant soin de les placer au bon endroit et de bien les nommer.

Après avoir téléchargé les clients (Wpkg-GP et WPKG Client), pour que les scripts fonctionnent il faut les renommer en :

- `WPKG_Client32.msi`
- `WPKG_Client64.msi`
- `Wpkg-GP_x86.exe`
- `Wpkg-GP_x64.exe`

Depuis un poste Windows, télécharger les 4 installeurs (2 en 32bits et 2 en 64bits) et les copier de manière à obtenir :

- `\\<SERVEUR>\wpkg\WPKG_Client32.msi`
- `\\<SERVEUR>\wpkg\WPKG_Client64.msi`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x86.exe`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x64.exe`

Configuration du contenu de WPKG avec l'application Wpkg-Manage

Un fois WPKG installé, il faut configurer les applications et leurs dépendances ainsi que les machines sur lesquelles elles seront installées.

Wpkg-Manage est une application écrite par Christophe Dezé de l'académie de Nantes permettant de gérer la configuration utilisateur de WPKG.

La configuration consiste à définir :

- des hosts, liste de machines associés à un profile ;
- des profiles, liste de paquets à installer ou à mettre à jour ;
- des packages, descriptions des applications à installer (commandes, tests, etc.).

http://eole.ac-dijon.fr/pub/Outils/Wpkg-manage/

Wpkg-Manage permet de gérer le contenu de WPKG, ses fonctionnalités principales sont :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- import des groupes de machines ESU dans WPKG ;
- association des groupes de machines avec les paquets ;
- possibilité de génération de nouveau paquets ;
- téléchargement semi-automatique des installeurs (`.exe` , `.msi`) ;
- fichiers exemples de paquets.

L'installation de l'application Wpkg-Manage doit se faire manuellement depuis le serveur :

```
# wget http://eoleng.ac-dijon.fr/pub/Outils/Wpkg-manage/wpkg-manage.zip
# unzip wpkg-manage.zip
# mv wpkg-manage /home/wpkg/
```



WPKG utilise les notions suivantes :

- hosts (nom de la machine, possibilité d'expression régulière. Ex.: "cdi.*")
  http://wpkg.org/Hosts.xml:fr
- packages (description d'une application, version, chemin vers .exe, etc.)
  http://wpkg.org/Packages.xml:French
- profiles (association entre les "hosts" et les "packages" à y installer)
  http://wpkg.org/Profiles.xml:French

Tests et exécutions manuelles

Il est parfois nécessaire d'exécuter WPKG manuellement sur un poste client pour faire des vérifications.

Il est possible d'exécuter directement le moteur WPKG sans utiliser le client à condition de renseigner les variables WPKG :

```
set ip-scribe=<ADRESSE IP SCRIBE>
set SOFTWARE=\\%ip-scribe%\wpkg\softwares
cscript \\%ip-scribe%\wpkg\wpkg.js /synchronize /nonotify /quiet
```

WPKG Client

Si le client est paramétré pour s'exécuter à l'arrêt de la station, il suffit d'arrêter le service WPKG :

```
net stop wpkgservice
```

Si le client s'exécute au démarrage de la station, il suffit de redémarrer le service :

```
taskkill /F /IM WPKGSrv.exe
net start wpkgservice
```

Wpkg-GP

Pour exécuter Wpkg-GP :

```
C:\Program Files\Wpkg-GP\Wpkg-GP-Test.exe
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

8.3.2. Les packages WPKG

Présentation

Les packages WPKG sont les fichiers décrivant l'installation et la désinstallation des applications Windows. Ils sont contenus dans le répertoire `wpkg/packages/`.

Les packages contiennent, entre autres, la version du logiciel et le chemin vers le programme d'installation.



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- OpenSource -->
<packages>
<package id="7zip"
name="7-Zip"
revision="%version%"
reboot="false"
priority="0">
<variable name="version" value="922" />
<variable name="longversion" value="9.22" />
<variable architecture="x86" name="platf" value="" />
<variable architecture="x64" name="platf" value="-x64" />
<check type="logical" condition="or">
<check type="file" condition="versionequalto"
path="%PROGRAMFILES%\7-Zip\7zFM.exe" value="%longversion%.0.0" />
<check type="file" condition="versionequalto"
path="%PROGRAMFILES(x86)%\7-Zip\7zFM.exe" value="%longversion%.0.0"
/>
</check>
<download
dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio
destname="7zip/7z%version%.msi" />
<download
dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio
destname="7zip/7z%version%-x64.msi" />
<install cmd='msiexec /qn /norestart /i
"%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
<upgrade cmd='msiexec /qn /norestart /i
"%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
<remove cmd='msiexec /qn /x
"%SOFTWARE%\7zip\7z%version%%platf%.msi"' />
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
</package>
</packages>
```



Explication sur les balises :

- id : identifiant WPKG de l'application ;
- name : nom de l'application à afficher ;
- revision : nombre entier définissant la version de l'application, il doit être incrémenté pour que WPKG mette l'application à jour ("upgrade") ;
- check : test(s) pour vérifier la présence d'une application (si elle est déjà installée) ;
- install : commande(s) à exécuter pour installer l'application ;
- upgrade/downgrade : commandes pour mettre à jour / rétrograder une application ;
- remove : commande pour désinstaller une application.

Davantage d'explications sur le site officiel de WPKG : http://wpkg.org/Packages.xml:French

Le projet EOLE wpkg-package propose des packages adaptés à l'environnement EOLE :
http://dev-eole.ac-dijon.fr/projects/wpkg-package/
Il contient des fichiers `<package>.xml` directement fonctionnels dans un environnement Horus/Scribe, à quelques (exceptions) près, ainsi que des icônes, des scripts et des outils (dans le dossier `softwares`).
http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/
Liste des applications supportées :
http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/revisions/master/show/packages

Téléchargement du projet wpkg-packages

Sous Windows

Le logiciel TortoiseGit permet de récupérer les `.xml` sur nos dépôts : http://tortoisegit.org/
Une fois installé, récupérer le projet `wpkg-packages` à l'adresse http://dev-eole.ac-dijon.fr/git/wpkg-package.git

Sous GNU / Linux

La manipulation peut se faire depuis le serveur Scribe/Horus.
Il est nécessaire d'installer Git :

```
# apt-eole install git-core curl
```

Pour télécharger l'ensemble des fichiers `<packages>.xml` du dépôt il faut le cloner :

```
# cd /root
# git clone https://dev-eole.ac-dijon.fr/git/wpkg-package
```

Lorsque que le dépôt est déjà cloné il faut le mettre à jour :

```
# cd /root/wpkg-package
# git pull
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

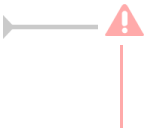
Les fichiers `<packages>.xml` sont à copier dans le dossier d'installation de WPKG, la commande rsync permet de ne copier que les nouveaux paquets :

```
# cd /root/wpkg-package
# rsync -Cav . /home/wpkg
```

Certains fichiers <packages>.xml contiennent une balise `<eoledl>`. Cette balise indique l'URL où télécharger le ou les installeurs de l'application.

Pour télécharger l'ensemble des installeurs :

```
# cd /home/wpkg/packages/
# ./download installers.py
```



Certains installeurs nécessitent un traitement particulier avant de pouvoir être exécutés automatiquement par WPKG, c'est le cas par exemple du logiciel Java.

Icônes

Le projet wpkg-package contient un dossier nommé icones avec les icônes du Bureau et du Menu démarrer correspondantes aux packages.

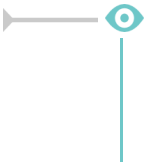
Ce dossier contient les icônes pour Windows 32-bits et 64-bits dans des sous-dossiers séparés, les chemins de ces icônes pouvant être différents.

Softwares

Le projet `wpkg-package` contient un dossier nommé Softwares nécessaire à l'exécution de certains packages. Il faut en copier le contenu dans le dossier wpkg\softwares\ (dossier correspondant à la variable `%SOFTWARE%`). Ce dossier contient notamment un sous-dossier nommé tools qui rassemble divers outils comme par exemple nircmd, setacl, wget...

Fonctionnement du téléchargements des installeurs

Le fichier .xml contient une ou plusieurs balises `<eoledl>`.



```
<  e  o  l  e  d  l
dl="http://launchpad.net/ocsinventory-windows-agent/2.0/2.0.3/+down
destname="ocsinventory\" unzip='1' />
```


- dl : lien vers le fichier à télécharger ;
- destname : nom d'un dossier ou d'un fichier ;

  Dans le cas d'un dossier aucun changement de nom est effectué, le fichier est seulement placé dans le dossier. Dans le cas d'un nom de fichier, le fichier téléchargé est renommé.

  Dans tous les cas, si le dossier n'existe pas il est créé. Pour qu'un nom soit considéré

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

comme un dossier il doit se finir par le caractère `/` ou `\`.

- unzip : indique s'il faut désarchiver le fichier téléchargé.

Contributions

Il est possible de contribuer à la maintenance de ces fichiers et à l'ajout de nouveaux packages. Il faut demander l'ouverture d'un accès sur la forge ou communiquer sur les listes de discussion.

Pour la création d'un nouveau paquet, voici quelques recommandations.

Convention de nommage

Certaines règles sont à respecter lors de la création d'un nouveau package afin de garder un système unifié et pérenne.

Un package est identifiable par les deux balises suivantes :

- id : identifiant unique de l'application dans WPKG (sensible à la casse) ;
- name : nom de l'application.

Le champ id est le plus important, il doit respecter les conventions suivantes :

- sans espace ;
- tout en minuscules ;
- sans numéro de version (`firefox` et non `firefox15`).

Tests des packages : check

La plupart des installeurs ajoute une entrée `Uninstall` pour apparaître dans la section `Ajout/Suppression de programmes` de Windows.

On peut utiliser cette clé pour tester la présence d'une application. Mais une clé de registre ne prouve pas qu'une application est réellement présente. Il faut aussi tester l'existence des fichiers de l'application.

```
<check type="uninstall" condition="exists" path="QT Lite %version%" />
<check type="file" condition="exists" path="%progfiles%\QT Lite\QuickTimePlayer.exe" />
```

Validation de la syntaxe XML

Il est toujours possible de faire une faute de frappe dans un fichier XML, un validateur XML en ligne permet de vérifier la syntaxe XML du fichier : http://xmlvalidation.com/.

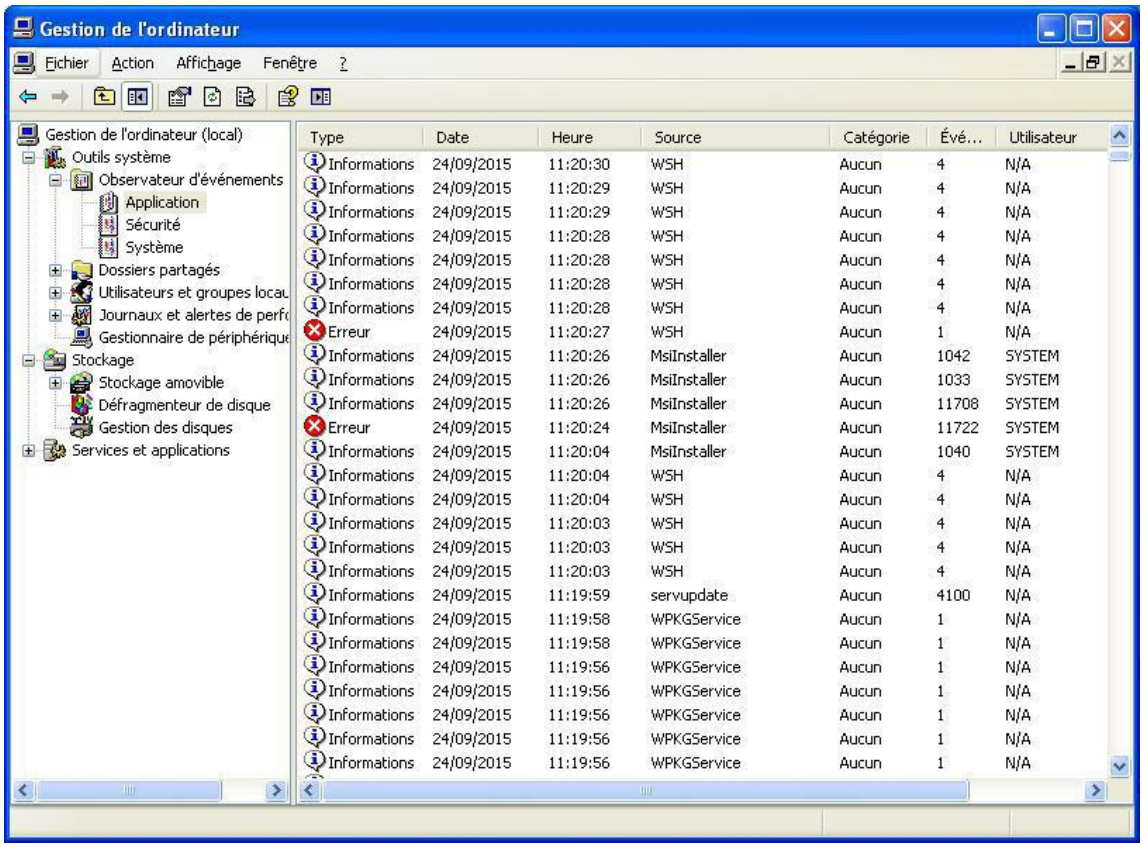
Voir aussi...

WPKG logiciels avec traitement particulier [p.576]

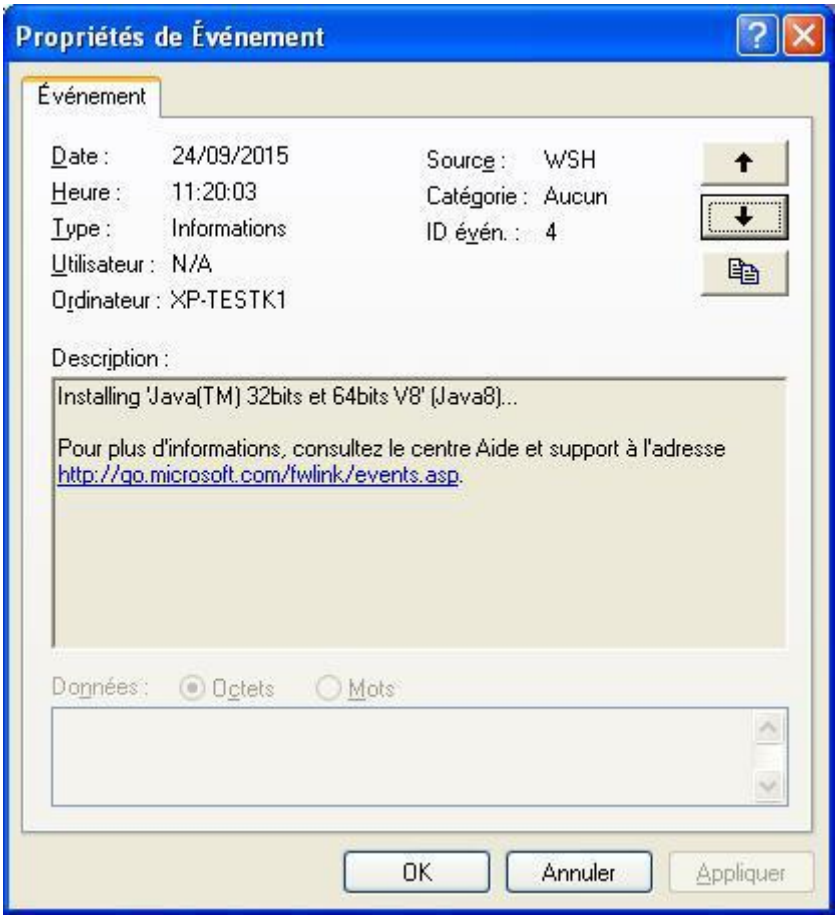
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

8.3.3. Journalisation des actions WPKG

Par défaut WPKG journalise ses actions dans l'observateur d'événements Windows, accessible dans la console de gestion de l'ordinateur (Microsoft Management Console) qui s'obtient avec un clic droit sur le `Poste de travail` puis `Gérer` dans le menu contextuel.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Il est possible d'activer le mode debug pour avoir plus d'informations dans la console de gestion de l'ordinateur. Pour se faire il faut passer la variable `Activer le mode "debug"` à `oui` dans l'onglet `Wpkg` de l'interface de configuration du module.

Pour corriger les erreurs et les dysfonctionnement d'une application ou simplement pour connaître le détail de ce qu'effectue WPKG, on peut activer la création d'un fichier de journalisation. La quantité d'informations journalisées est paramétrable.

Pour une station particulière

Lors de sa prochaine exécution, WPKG va créer un fichier de log : `C:\wpkg-[HOSTNAME].log`

WPKG Client

- Ouvrir `%PROGRAMFILES%\wpkg\wpkginst.exe` ;
- Dans WPKG parameters renseigner :
  `/synchronize /nonotify /quiet /log_file_path:c: /logLevel:31`
- Sauver à l'aide de l'action `Save` et fermer `wpkginst.exe`.

Wpkg-GP

- Ouvrir `%PROGRAMFILES%\wpkg-gp\Wpkg-gp.ini` ;
- À la fin de la ligne commençant par "WpkgCommand =" ajouter :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`/log_file_path:c: /logLevel:31`

- Sauver et fermer le fichier.

Pour toutes les stations

Sur le serveur il faut utiliser l'interface de configuration du module en mode normal et se rendre dans l'onglet `Wpkg`.

Il faut placer la variable `logLevel` à la valeur 31 et remplir si besoin les variables `log_file_path` et `logfilePattern`.



Enregistrer et quitter l'interface de configuration du module.

Pour appliquer la configuration il faut reconfigurer le module à l'aide de la commande reconfigure :

```
# reconfigure
```

Par défaut les journaux se trouveront dans `C:\wpkg-<nom-poste>.log`



Granularité des logs

La variable `logLevel` permet d'indiquer le niveau de détails de la journalisation souhaité sous forme d'un nombre.

Ce nombre est le résultat d'une opération de masquage, il faut additionner les valeurs suivantes pour choisir le niveau de journalisation souhaité :

- 0 désactive la journalisation ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 1 erreurs ;
- 2 avertissements ;
- 4 informations ;
- 8 audit success ;
- 16 audit failure.

- variable `logLevel` à 31 (1 + 2 + 4 + 8 + 16) → journalise tout
- variable `logLevel` à 3 (1 + 2) → journalise seulement les erreurs et les avertissements

8.3.4. WPKG scripts de pre et post installation

L'utilisation de dossiers dans un lecteur réseau pour les icônes du Menu Démarrer et du Bureau pose problème avec WPKG.

Une erreur se produit lorsque WPKG installe une application dont l'installeur crée des icônes dans le Menu démarrer et sur le Bureau et qu'une session sur le domaine Scribe est ouverte avant ou pendant l'installation.

Problématique

Voici l'exemple de l'erreur rencontrée à l'installation d'OpenOffice avec WPKG.

```
Type de l'événement : Erreur
Source de l'événement : MsiInstaller
Catégorie de l'événement : Aucun
ID de l'événement : 11327
Date : 08/02/2011
Heure : 11:52:19
Utilisateur : AUTORITE NT\SYSTEM
Ordinateur : POSTE-ADMIN1
Description :
Produit : OpenOffice.org 3.3 -- Erreur 1327.Lecteur R:\ non valide
```

Lors de l'ouverture de session, ESU ré-écrit les chemins d'accès aux dossiers contenant les icônes du "Bureau" et du "Menu Démarrer" en les faisant pointer sur le lecteur `R:`.

Sous Windows il existe 2 type de chemins :

- utilisateur, ces chemins peuvent varier d'un utilisateur à l'autre, on y place les icônes qu'on ne veut rendre visible que pour un groupe donné ("gestion-postes" pour les professeurs par exemple) ;
- machine, ces chemins sont les mêmes pour tous les utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les chemins utilisateur sont dans HKEY_CURRENT_USER et les chemins machine dans HKEY_LOCAL_MACHINE.

WPKG est exécuté dans le contexte de l'utilisateur BUILTIN\SYSTEM.

Sous Windows (de 2000 et supérieurs) existe la notion d'environnement utilisateur.

Les lecteurs réseaux, par exemple, ne sont disponibles que pour l'utilisateur qui les a connectés.

Ici, le lecteur `R:` n'est accessible que pour l'utilisateur qui a ouvert la session et n'est pas disponible pour l'utilisateur BUILTIN\SYSTEM.

On peut constater le phénomène de visu :

- activer le Bureau à distance sur un poste ;
- ouvrir, sur ce même poste, une session sur le domaine ;
- aller sur un autre poste et ouvrir une session **administrateur local** via une connexion Bureau à distance.

Dans le poste de travail de la session du domaine on voit le lecteur `R:`, il est absent dans la session **administrateur local**.



L'installeur OpenOffice, par défaut, lorsqu'il est exécuté en mode silencieux (comme avec WPKG), veut créer des icônes dans le Menu démarrer.

Il regarde dans HKEY_LOCAL_MACHINE et trouve `R:\%ESU_GM%\Menu Démarrer`.

S'exécutant dans l'environnement BUILTIN\SYSTEM l'installeur ne trouve donc pas le lecteur `R:` et annule sa procédure d'installation. On peut observer le dossier `%PROGRAMFILES%\OpenOffice\` qui grossi à l'installation et qui disparaît ensuite avec l'annulation de l'installation.

Solutions

Le principe est d'éviter qu'un utilisateur n'ouvre une session pendant l'installation d'un programme et permette à l'installeur de créer des icônes dans HKEY_LOCAL_MACHINE avec des chemins qui pointent vers le lecteur `C:`.

Augmenter le temps de blocage pendant lequel WPKG accède au poste de travail

Il est possible d'allonger le temps maximal pendant lequel WPKG bloque l'accès au poste de travail pendant son exécution, ceci se paramètre dans l'interface de configuration du module, dans l'onglet `Wpkg client` avec la variable `logon-delay`.

Il faut ensuite appliquer la nouvelle configuration sur les clients, voir la section Application de la nouvelle configuration WPKG sur les clients.

#fixme

Le blocage du poste fait apparaître une boîte de dialogue qui affiche "WPKG installe les applications et applique les paramètres..."/"Veuillez patienter et ne pas redémarrer votre ordinateur...".

Scripts de pre et de post-installation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une deuxième solution consiste à restaurer les chemins par défaut des icônes du Bureau et du Menu démarrer avant l'installation du logiciel et exécuter WPKG à l'arrêt du poste plutôt qu'au démarrage.

Deux scripts permettent de sauvegarder et de restaurer les chemins :

- script de pré-installation va sauvegarder les chemins pour les dossiers d'icônes du Bureau et du Menu Démarrer et placer les chemins par défaut ;
- script de post-installation va restaurer les chemins sauvegardés en pré-installation (facultatif si on exécute WPKG à l'arrêt de la station).

Malgré l'utilisation de ces scripts, il est quand même possible de faire planter l'installation. Il suffit qu'un utilisateur ouvre une session pendant l'installation, juste après le script de pré-installation. À ce moment le chemin pointe quand même vers le lecteur `R:` et l'installation échouera.

Exécuter WPKG lors de l'arrêt de la machine permet d'éviter ce dernier cas de figure. Cela permet aussi d'accéder directement à l'ordinateur plutôt que de devoir attendre l'installation des logiciels.

On peut alors expliquer aux utilisateurs qu'ils peuvent :

- accéder immédiatement au poste avec des logiciels par forcément à jour ;
- redémarrer la machine pour avoir des logiciels à jour si besoin.

Préparation des scripts

Il faut placer les 3 fichiers suivants à la racine du partage `\\scribe\wpkg` :

- `preinstall.bat`
- `postinstall.bat`
- `bureau-menu_demarrer.reg`

Remplacer dans l'exemple suivant ADRESSE_IP_SCRIBE par la valeur correspondante à votre serveur et enregistrer le résultat dans un fichier nommé `preinstall.bat`

```
rem remet les chemins par defaut avant l'installation
regedit /E %WINDIR%\sauv_menu-dem.reg "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explo
Shell Folders"
regedit /S "\\ADRESSE_IP_SCRIBE\wpkg\bureau-menu_demarrer.reg"
```

Copier l'exemple suivant et enregistrer le résultat dans un fichier nommé `postinstall.bat`

```
rem remet les chemins comme ils etaient avant l'installation
regedit /S %WINDIR%\sauv_menu-dem.reg
del /F %WINDIR%\sauv_menu-dem.reg
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le fichier `bureau-menu_demarrer.reg` est téléchargeable à l'adresse :
http://dev-eole.ac-dijon.fr/attachments/download/116/bureau-menu_demarrer.reg

Utilisation des scripts `preinstall.bat` et `postinstall.bat`

Deux méthodes sont possibles pour utiliser ces scripts :

- appeler `preinstall.bat` et `postinstall.bat` depuis `<nom_du_package>.xml` dans les balises `<install>` et `<update>`

  Cette méthode présente l'avantage de ne pas avoir à modifier la configuration des clients WPKG mais présente l'inconvénient de devoir les appeler pour chaque application dont l'installeur crée des icônes sur le Bureau et/ou dans le Menu démarrer.
- utiliser les actions `pre-action` et `post-action` de WPKG

  Cette méthode a l'avantage d'être faite une bonne fois pour toute mais demande à mettre la configuration WPKG à jour sur chaque poste.

Configuration des clients WPKG

Il faut modifier la configuration des clients WPKG pour qu'ils exécutent les 2 scripts en pre et post installation, pour cela il faut utiliser l'interface de configuration du module et vérifier dans l'onglet `Wpkg client` les chemins des variables `pre-action` et `post-action`.



Il faut également passe la variable `run-on-shutdown` à `YES`.



Ne pas hésiter à augmenter la valeur de la variable `shutdown-delay`.

Principe de fonctionnement des délais dans WPKG :

- s'il n'y a aucune installation ou mise à jour à faire alors l'arrêt est immédiat ;
- s'il y a une installation ou une mise à jour est à faire WPKG exécute les installeurs et attend qu'ils se terminent le temps défini dans la variable `shutdown-delay`. Si le temps est dépassé WPKG force l'arrêt de la station même si l'installation du logiciel n'est pas terminée. Si il reste du temps et que l'installation des logiciels est terminée la station s'éteindra.

Le principe est le même pour `logon-delay` qui est utilisé si WPKG s'exécute au démarrage de la station (`run-on-shutdown` à `NO`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Application de la nouvelle configuration WPKG sur les clients

Il faut appliquer la nouvelle configuration en exécutant `wpkg_client_update_conf.bat` sur chacun des clients WPKG.



La mise à jour des clients un par un peut paraître fastidieuse, il existe des outils pour faciliter cela :

- Winexe ;
- cliscribe.py.

8.3.5. WPKG logiciels avec traitement particulier

Java

Sur Windows Vista/Seven il faut décompacter l'installeur Java pour récupérer le `.msi` et les fichiers qui l'accompagnent. Cette manipulation doit être effectuée sur un poste Vista ou supérieur.

Lancer manuellement l'installeur `jre-7uX-windows-XXX.exe` (en double-cliquant dessus).

Une fois que la fenêtre de l'installeur s'affiche, ne cliquer sur aucun bouton. Il faut se rendre dans le menu `Démarrer` puis `Exécuter` : `%USERPROFILE%\AppData\LocalLow\Oracle\Java\`

Déplacer le dossier `jre1.7.0_XX` qui s'y trouve dans `\\<SERVEUR>\wpkg\softwares\java\`



Si vous avez une version 64bits de Windows, il faut effectuer deux fois cette manipulation. Une fois pour la version i586 et une fois pour la version x64.

8.3.6. Quelques références

Documentation écrite par la DANE de l'académie de Lyon

WPKG sur un environnement Scribe

http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/doku.php?id=scribe:wpkg

Documentation écrite par l'académie de la Réunion

WPKG - Généralités

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:1.principe&ticket=

WPKG - Installation sur un serveur Scribe

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:2.installation_sur_scribe&ticke

Wpkg-Manage : interface de gestion des packages à installer

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:3.wpkg_manage

WPKG - Mise à jour des XML et installeurs

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:4.maj

WPKG - Tests

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:5.tests

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

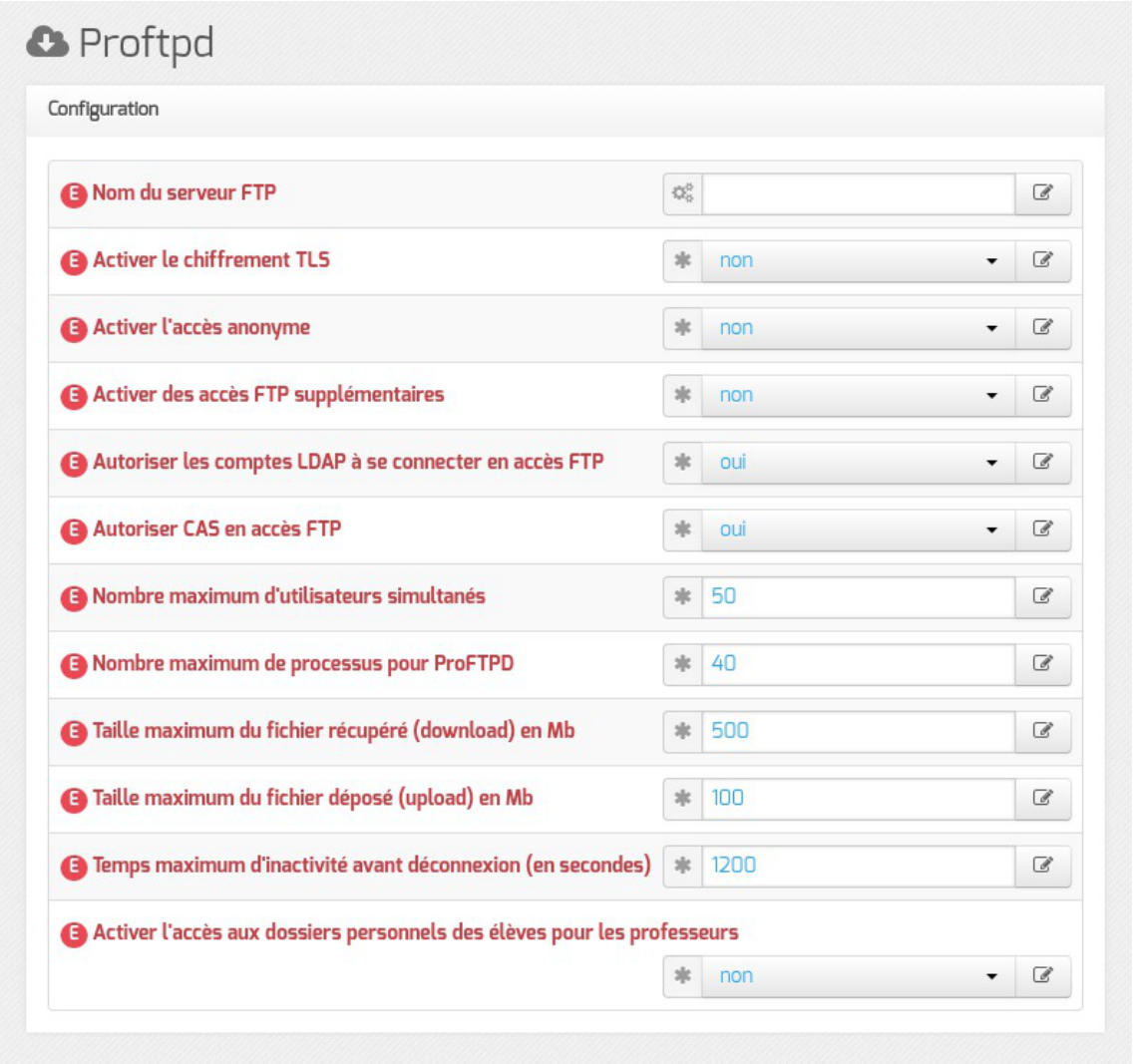
Mise à jour des clients Wpkg-GP (Seven et Windows 8) en version 0.17
http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:6.maj_wpkg_gp

9. Les clients FTP

Les utilisateurs peuvent accéder à leurs données par l'intermédiaire d'un client FTP (gFTP, Filezilla, ...).

Le serveur FTP est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option `Activer l'accès FTP`. Le serveur FTP est basé sur le logiciel libre ProFTPD.
http://www.proftpd.org/

L'onglet `Proftpd` n'apparaît en mode expert que si le service est activé.



Vue de l'onglet Ftp de l'interface de configuration du module

Paramétrage du serveur ProFTPD

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Nom du serveur FTP

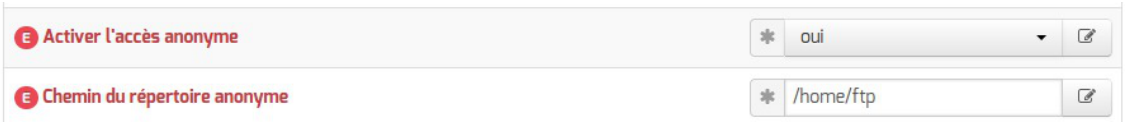
Ce paramètre permet de personnaliser le nom du serveur FTP. Ce nom apparaît lorsqu'on se connecte en FTP sur le serveur avec un client ou en ligne de commande.

Activer le chiffrement TLS

Passer cette option à `oui` permet d'activer le chiffrement TLS mais son utilisation est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

Activer l'accès anonyme

L'accès anonyme permet d'ouvrir l'accès en anonyme sur le répertoire de votre choix.



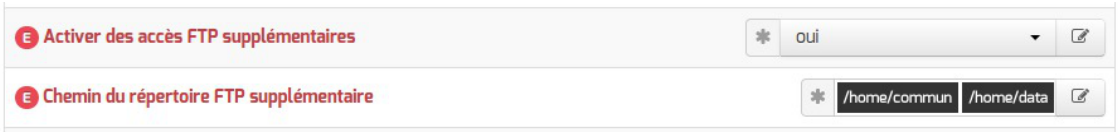
Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire anonyme` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas. L'utilisateur `anonymous` peut télécharger depuis le répertoire spécifié, il n'a pas par défaut les droits d'écriture.

Le fichier de configuration contient la directive `<Limit WRITE>` :

```
<Limit WRITE>
DenyAll
</Limit>
```

Activer des accès FTP supplémentaires

L'accès FTP supplémentaire permet d'ouvrir l'accès à des comptes existants sur le répertoire de votre choix.



Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire FTP supplémentaire` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas et les droits doivent être ajustés. Les utilisateurs du module peuvent lire et écrire dans le répertoire spécifié.

Autoriser CAS en accès FTP

Cette option doit être activée pour l'utilisation de l'application Pydio sur le serveur.

Nombre maximum d'utilisateurs simultanés

Par défaut à `50` cette variable permet d'ajuster le nombre d'utilisateurs simultanés autorisés à se connecter en FTP.

Nombre maximum de processus pour ProFTPD

Par défaut à `40` cette variable permet d'ajuster le nombre maximum de processus simultanés du logiciel ProFTPD.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Taille maximum du fichier récupéré (download) en Mb

Par défaut à `500` cette variable permet d'ajuster la taille maximum des fichiers pouvant être téléchargés.

Taille maximum du fichier déposé (upload) en Mb

Par défaut à `100` cette variable permet d'ajuster la taille maximum des fichiers pouvant être déposés.

Temps maximum d'inactivité avant déconnexion (en secondes)

Par défaut à `1200` secondes (20 minutes) cette variable permet d'ajuster le temps d'inactivité avant déconnexion.

Accès FTP

Une fois l'accès FTP activé, il est possible d'accéder au service avec un client FTP (Filezilla, gFTP), par un navigateur web ou avec une application web FTP (Pydio, anciennement Ajaxplorer, sur le module Scribe).

Accès par un navigateur web

Pour accéder aux documents avec un navigateur web il faut préciser le protocole dans l'URL :

`ftp://user@<adresse_serveur>/`

ou

`ftp://<adresse_serveur>/`

Accès par une application web

Pour accéder aux fichiers par l'application web Pydio, il faut l'activer dans l'onglet `Applications web`. Pydio (anciennement Ajaxplorer) n'est pas pré-installé sur le module Horus (il s'installe avec la commande `apt-eole`, voir la documentation sur les applications web). Suite à une reconfiguration du serveur, l'application sera accessible à l'adresse `http://<adresse_serveur>/pydio/` moyennant l'authentification (mire EoleSSO).



Avec un client FTP (en mode passif par défaut) le mode actif doit impérativement être configuré. Dans ce mode c'est le client FTP qui détermine le port de connexion à utiliser.

Interdire l'accès FTP à des comptes utilisateur

Le fichier `/etc/ftpusers` contient une liste des utilisateurs qui ne doivent pas se connecter via le service FTP. Ce fichier est utilisé non seulement pour l'administration système mais également pour augmenter la sécurité du réseau. Il contient typiquement la liste des utilisateurs qui, soit n'ont rien à faire avec le transfert FTP, soit ont trop de privilèges pour être autorisés à se connecter au serveur. De tels utilisateurs sont en général `root`, `daemon`, `bin`, `uucp` et `news`.

La liste du fichier `/etc/ftpusers` peut être complétée avec des utilisateurs systèmes ou LDAP dont il faut désactiver l'accès au service FTP.



Attention lors des accès FTP, le mot de passe transite en clair sur le réseau.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Anti-virus ClamAV

Si l'anti-virus ClamAV est activé, la recherche de virus en temps réel sur le FTP est activé par défaut. Il est possible de désactiver cette option dans l'onglet `Clamav` en passant `Activer l'anti-virus temps réel sur FTP` à `non`.

Accès au dossier personnel des élèves par FTP

Sur les modules Scribe et AmonEcole, les professeurs n'ont, par défaut, pas accès au dossier personnel de leurs élèves par l'intermédiaire du protocole FTP.

Cette restriction peut être levée en répondant `oui` à la question `Activer l'accès aux dossiers personnels des élèves pour les professeurs`. Cette option diminue légèrement la sécurité du serveur.

10. Les applications web sur le module Horus

Le module Horus supporte nativement certaines applications web dont la plupart sont le résultat de la mutualisation inter-académique Envole[p.760].

Elles sont adaptées pour fonctionner avec un serveur d'authentification unique. Grâce à cette méthode d'authentification unique, les utilisateurs du module Horus se connectent une seule fois pour accéder à l'ensemble des applications. Des rôles sont prédéfinis dans chacune d'elles. Il est possible dans certaines, de modifier les rôles prédéfinis pour l'utilisateur.

Le paramétrage du module Amon permet de rendre ces services web accessibles depuis l'extérieur de l'établissement.

Par défaut, **aucune application par défaut n'est définie** sur le module Horus.

Il est possible de modifier ce comportement en activant le serveur web Apache, dans l'interface de configuration du module, dans l'onglet `Services`, il faut passer la variable `Activer le serveur web Apache` à `oui`. L'onglet `Applications web` apparaît et propose entre autre d'activer l'application web phpMyAdmin. L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Des applications web vous sont proposées dont certaines sont **pré-installées** et doivent être activées lors de la configuration du module.

D'autres sont **pré-packagées** et leur installation est laissée à votre initiative. Vous pouvez également ajouter vos propres applications.



La seule procédure valide pour mettre à jour les applications web d'un module EOLE est la procédure proposée par EOLE.

En aucun cas vous ne devez les mettre à jour par les moyens qui sont proposées via le navigateur.

Vous risquez d'endommager vos applications web et d'exposer votre module à des failles de sécurité.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

10.1. L'authentification unique avec EoleSSO

L'authentification unique

EOLE propose un mécanisme d'authentification unique par l'intermédiaire d'un serveur SSO[p.779].

Ce serveur est compatible CAS[p.754], SAML[p.777] et OpenID[p.772].

L'utilisation d'un serveur SSO permet de centraliser l'authentification. En s'authentifiant auprès du serveur SSO, les utilisateurs peuvent se connecter aux différentes applications web sans avoir à se ré-identifier sur chacune d'elles.

Configuration

Dans l'interface de configuration du module, vous pouvez activer le serveur SSO du module ou utiliser un serveur SSO distant dans l'onglet `Services` → `Utiliser un serveur EoleSSO`

Vous devez ensuite renseigner les paramètres du serveur dont l'adresse IP et le port dans l'onglet `Eole sso` apparu après l'activation du service.

Cette opération nécessite la reconfiguration du module par la commande `reconfigure`.

Comptes utilisateurs pris en compte par le serveur SSO

Le serveur SSO installé sur les modules EOLE peut utiliser plusieurs annuaires LDAP.

Connexion

Une connexion vers une application (`http://<adresse serveur>/application/`) redirige le navigateur vers le serveur SSO (`https://<adresse serveur>:8443/`) afin d'effectuer l'authentification via un formulaire appelé mire SSO :



Formulaire d'authentification SSO

Lorsque le serveur SSO valide le couple identifiant / mot de passe de l'utilisateur, il délivre au navigateur un *jeton* sous forme de cookie et le redirige vers l'application (`https://<adresse serveur>/application/`).

L'application reconnaît le jeton et autorise l'accès à l'utilisateur.

Remarque

Le navigateur doit être configuré pour **accepter les cookies**.

10.2. Applications pré-installées

Il est possible d'ajouter au module Horus des applications web pré-installées.

Il y différentes méthodes de mise en œuvre et les rôles des utilisateurs sont très différents d'une application à l'autre.

Reportez-vous à la documentation de chacune d'elles pour plus d'informations.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

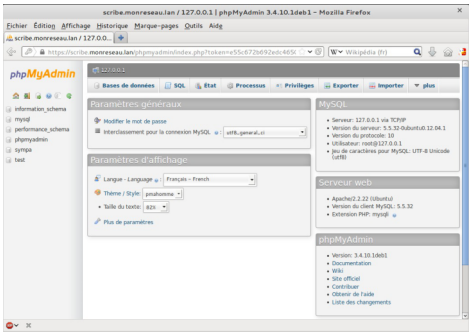
Reconfiguration du module

De nombreuses applications nécessitent d'être activées depuis l'interface de configuration du module et une reconfiguration du serveur est indispensable.

Cette procédure est relativement longue, il est donc possible d'activer plusieurs applications et de ne lancer qu'une fois la commande `reconfigure` .

10.2.1. phpMyAdmin : gestionnaire de base de données MySQL

Présentation



Vue générale dans phpMyAdmin

phpMyAdmin est une application de gestion de base de données MySQL.

Cette interface pratique permet d'exécuter, très facilement et sans grandes connaissances dans le domaine des bases de données, de nombreuses requêtes comme les créations de table de données, les insertions, les mises à jour, les suppressions, les modifications de structure de la base de données.

http://www.phpmyadmin.net

Installation

Cette application est pré-installée sur les modules Scribe, Horus, Seshat ainsi que sur AmonEcole et toutes ses variantes.

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom de l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :

```
# service apache2 reload
```

Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :

```
# a2ensite nom de l'application
```

```
# service apache2 reload
```

Pour désactiver l'application pour une période plus longue voir définitivement, il faut désactiver l'application depuis l'interface de configuration du module, dans l'onglet

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Applications web.

L'opération nécessite une reconfiguration du module avec la commande reconfigure.

Accéder à l'application

Pour accéder à l'application, se rendre à l'adresse : https://<adresse serveur>/phpmyadmin/ (ou https://<adresse serveur>/myadmin/).

L'utilisateur peut être l'utilisateur root de MySQL ou un utilisateur de la base.



L'accès à l'application ne peut se faire que depuis une adresse IP autorisée dans l'interface de configuration du module (Onglet Interface-n, sous-menu Administration distante sur l'interface, mettre Autoriser les connexions pour administrer le serveur à oui, remplir le champ Adresse IP réseau autorisé avec l'adresse IP ou la plage d'adresses IP souhaitée).

Rôles de utilisateurs

Les utilisateurs autorisés à se connecter sont **les utilisateurs de MySQL**.

Il est possible de déléguer tout ou une partie des droits d'administration.

Remarques

Le mot de passe root de MySQL est réinitialisé avec une chaîne de caractères aléatoires à chaque reconfiguration du serveur.

Le mot de passe de l'utilisateur root de MySQL peut être réinitialisé avec la commande :

mysql_pwd.py



Si vous prévoyez d'utiliser régulièrement phpMyAdmin, il est préférable de créer un utilisateur MySQL dédié pour l'administration des bases de données.

Celui-ci ne sera pas écrasé après une reconfiguration du module.

10.3. Prise en charge d'applications supplémentaires

Les modules Scribe, Horus, Seshat et AmonEcole fournissent tous les éléments nécessaires à l'installation d'applications web indépendamment de celles pré-configurées.

Les exemples sont basés sur l'installation du logiciel EGroupware mais sont facilement transposables pour l'installation de n'importe quelle application PHP/MySQL.

EGroupware est un logiciel collaboratif professionnel. Il vous permet de gérer vos contacts, vos rendez-vous, vos tâches, et bien plus pour toute votre activité.

http://www.egroupware.org/



Mode conteneur

L'installation d'applications sur les modules configurés en mode conteneur est plus complexe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Certaines étapes de la mise en place diffèrent selon le mode, conteneur ou non conteneur.
>
> Dans les exemples ci-dessous les modules Scribe et Horus sont en mode non conteneur et AmonEcole en mode conteneur.

10.3.1. Téléchargement et mise en place

Installation des fichiers

Pour télécharger une archive sur le module, il faut utiliser la commande `wget` :

```
# wget downloads.sourceforge.net/project/egroupware/eGroupware-14.2/eGroupware-14.2
```

Il faut ensuite décompresser l'archive à l'aide de la commande `tar` (ou `unzip`, pour le format zip) :

```
# tar xzvf egroupware-epl-14.2.20150310.tar.bz2
```

Dans cet exemple, cela créera le répertoire `egroupware`

Ensuite, il faut envoyer les fichiers dans le répertoire de destination, soit :

- sur les modules Scribe ou Horus :

  ```
  # cp -r egroupware /var/www/html/egroupware
  ```

- sur un module Horus dépourvu d'application web :

  ```
  # mkdir /var/www/html
  # cp -r egroupware /var/www/html/egroupware
  ```

- sur le module AmonEcole :

  ```
  # cp -r egroupware /opt/lxc/reseau/rootfs/var/www/html/egroupware
  ```

Affectation de droits

La plupart des applications nécessitent que l'utilisateur utilisé par le service Apache (ici, l'utilisateur système : ***`www-data`***) ait le droit d'écrire en certains endroits du disque.

Le propriétaire d'un fichier ou d'un répertoire se modifie à l'aide de la commande `chown` :

- sur les modules Scribe/Horus :

  ```
  # chown -R www-data: /var/www/html/egroupware
  # chmod 770 /var/www/html/egroupware
  ```
  (le temps de l'installation)

- sur le module AmonEcole :

  ```
  # ssh reseau
  # chown -R www-data: /var/www/html/egroupware
  # chmod 770 /var/www/html/egroupware
  ```
  (le temps de l'installation)

  `# ctrl + d` pour sortir du conteneur



> Donner trop de droits à l'utilisateur ***`www-data`*** diminue la sécurité du serveur.
>
> Consulter la documentation du logiciel pour n'attribuer que les droits nécessaires au fonctionnement de l'application.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Installation de paquets

Certaines applications nécessitent également des modules apache ou d'autres logiciels qui ne sont pas forcément présents sur le serveur.

Dans la majeure partie des cas, les éléments manquants sont disponibles en tant que paquet de la distribution.

Installation du paquet php5-imap

- sur les modules Scribe ou Horus :

```
# apt-eole install php5-imap
```

- sur le module AmonEcole :

```
# apt-eole install-conteneur web php5-imap
```

Voir aussi...

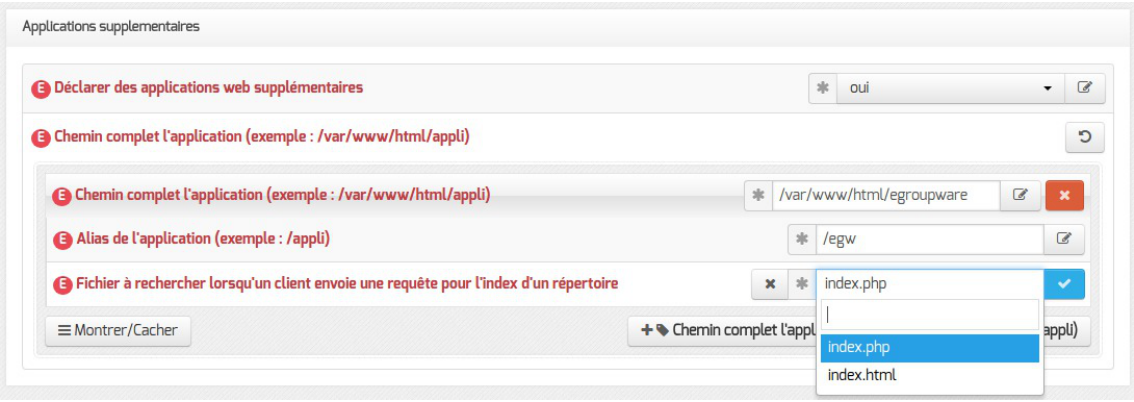
Installation manuelle de paquets [p.439]

10.3.2. Configuration Apache

Méthode Creole

Dans l'interface de configuration du module :

- aller dans l'onglet Apache en mode expert ;
- indiquer le chemin complet de l'application et l'alias de l'application /var/www/html/egroupware ;
- indiquer le chemin de l'alias de l'application /egw ;



Déclaration d'une application web dans gen_config

- enregistrer la configuration et quitter ;
- lancer la commande reconfigure ;
- le logiciel doit répondre à l'adresse : http://<adresse_serveur>/egw

Le fichier de configuration apache pour cette application est /etc/apache2/sites-available/eole

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> La directive `php_admin_flag allow_url_fopen On` est nécessaire au bon fonctionnement d'EGroupware.

Méthode manuelle

- créer le fichier de configuration apache nommé `egroupware`
  - sur les modules Scribe ou Horus : /etc/apache2/sites-available/egroupware.conf
  - sur le module AmonEcole : /opt/lxc/reseau/rootfs/etc/apache2/sites-available/egroupware.conf

```
# Exemple basique de configuration de site #
Alias /egw /var/www/html/egroupware
<Directory "/var/www/html/egroupware">
    php_admin_flag allow_url_fopen On
    AllowOverride None
    DirectoryIndex index.php
    Order Allow,Deny
    Allow from All
</Directory>
```

- activer l'application à l'aide de la commande :
  ```
  # CreoleRun "a2ensite egroupware" web
  ```
- recharger la configuration d'Apache à l'aide de la commande CreoleService[p.757] :
  ```
  # CreoleService apache2 reload
  ```
- le logiciel doit répondre à l'adresse : ***`http://<adresse serveur>/egw`***

> Pour obtenir une configuration apache optimale, consulter la documentation de l'application.
> En cas de problème, consulter le fichier de journal /var/log/rsyslog/local/apache2/apache2.err.log
> Dans le cas d'EGroupware, il est nécessaire de supprimer le fichier ***.htaccess*** situé dans le répertoire racine du logiciel :
> ```
> # rm -f /var/www/html/egroupware/.htaccess
> ```
> La directive `php_admin_flag allow_url_fopen On` est également nécessaire au bon fonctionnement d'EGroupware.

10.3.3. Configuration MySQL

Méthode EOLE

Utiliser le script mysql_add.py :

```
Nom de la base de données à créer : egroupware
Nom de l'utilisateur MySQL administrant la base : egroupware
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`Mot de passe de l'utilisateur Mysql administrant la base : pwdsecret`

`## Création de la base egroupware ##`

Sur le module AmonEcole, il y a une question supplémentaire : `Nom du conteneur source : web`

En répondant ***`web`*** cela permet que les requêtes vers MySQL soient autorisées depuis le conteneur dans lequel se trouvent les applications web.

Méthode semi-manuelle

- utiliser le script `mysql_pwd.py` ;
- réinitialiser le mot de passe `root` de MySQL à la valeur de votre choix ;
- utiliser l'interface de phpMyAdmin pour faire les manipulations nécessaires.



Il est recommandé de créer un utilisateur et une base MySQL spécifiques par application.

Sur le module AmonEcole, il faudra veiller à ce que l'utilisateur MySQL utilisé ait le droit d'accéder à la base de données depuis l'adresse IP du conteneur web, en l'occurrence `192.0.2.51`.

10.3.4. Configuration du logiciel

Vous pouvez maintenant utiliser le système automatique d'installation du logiciel disponible à l'adresse : `http://<adresse serveur>/egw`

Un `/install` ou `/config` sera à ajouter au chemin en fonction de l'application à installer.



Sur le module AmonEcole, l'adresse de la base de données à mettre dans l'interface de configuration de l'application est celle du conteneur `bdd` (`192.0.2.50`) et non `localhost`.

Affectation de droits après l'utilisation du système automatique d'installation du logiciel

Changer les droits d'accès :

`# chmod 750 /var/www/html/egroupware`

Changer le propriétaire des fichiers :

`# chown -R root :www-data /var/www/html/egroupware`

Authentification CAS

Informations utiles à la configuration d'une authentification CAS :

- adresse du serveur CAS : adresse IP (ou nom DNS) de votre module EOLE

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- port d'écoute par défaut du serveur CAS : 8443 (CAS EOLE)
- URI sur le serveur CAS : *rien*
- Destination après la sortie : *rien*



Par défaut EoleSSO, fournit uniquement l'identifiant de l'utilisateur.

Pour chaque application, il est possible d'ajouter des filtres définissant des attributs supplémentaires à fournir.

Pour plus d'informations, consulter la documentation EoleSSO.

Authentification LDAP

Informations utiles à la configuration d'une authentification LDAP :

- adresse du service LDAP :
  - sur le module Scribe/Horus : adresse IP (ou nom DNS) de votre module EOLE
  - sur le module AmonEcole : adresse IP du conteneur bdd : `192.0.2.50`
- port d'écoute du serveur LDAP : 389 (port standard)
- base DN : o=gouv,c=fr



La majeure partie des informations stockées dans l'annuaire est accessible par des requêtes anonymes.

Si l'application a besoin d'accéder à des attributs LDAP protégés par une ACL[p.752] et non fournis par EoleSSO, il est possible d'utiliser le compte spécial `cn=reader,o=gouv,c=fr` dont le mot de passe est stocké dans le fichier `/root/.reader`

Voir aussi...

Utilisateurs spéciaux

Définition de filtres d'attributs

11. Réplication LDAP

Avec le module Scribe ou le module Horus, il est possible de mettre en place rapidement une réplication d'annuaire LDAP vers un module Seshat.

La réplication utilise le mécanisme *syncrepl* (LDAP Sync Replication engine).

Syncrepl est plus robuste que son prédécesseur *slurpd* et permet de mettre en place des architectures beaucoup plus complexes.

La configuration actuelle permet au **client** (serveur Seshat) de venir recopier les informations de son **fournisseur** (serveur Scribe ou Horus).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



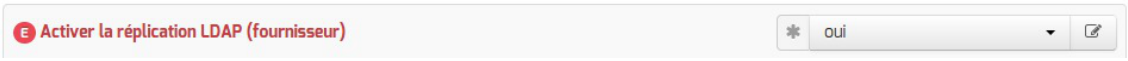
Il est déconseillé de répliquer des serveurs Scribe et des serveurs Horus sur le même client Seshat.

Pré-requis

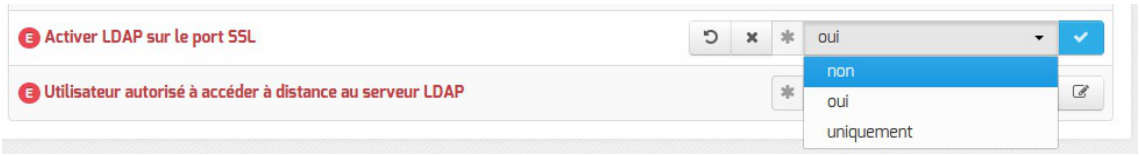
Serveur Scribe ou Horus

Pour configurer le fournisseur il faut adapter les informations dans l'interface de configuration du module en mode expert dans l'onglet `Openldap`.

- la réplication LDAP du côté fournisseur doit être activée



- par défaut, les communications LDAP ne sont pas chiffrées. Pour mettre en place une communication chiffrée entre le fournisseur et le client, il faut passer la variable `Activer LDAP sur le port SSL` à `oui` ou à `uniquement`.





Selon la configuration mise en place le port 389 et/ou le port 636 doivent être ouverts :

- du serveur Seshat vers le serveur Scribe ou Horus ;
- si possible dans le sens inverse.

Mise en place

Génération du fichier de configuration

Sur le module Scribe ou Horus, exécuter la commande `active_replication.py`.

Cette commande permet de générer dans `/root/` le fichier de configuration propre au serveur nommé : `replication-<numero_etab>.conf`.

La commande permet de paramétrer plusieurs éléments :

- `Répliquer également les groupes` : si la réponse est laissée à `non`, seuls les comptes utilisateurs seront répliqués.

  Certains connecteurs EoleSSO disponibles sur le module Seshat nécessitent de répliquer les groupes en plus des utilisateurs ;

- `Ajouter des uid à exclure de la réplication` : en répondant `oui` à cette question, il est possible de saisir une liste de comptes à ne pas répliquer (administrateur locaux, comptes réservés, ...).

  Par défaut seul le compte `admin` n'est pas répliqué ;

- `Adresse utilisée pour accéder au module depuis le client` : adresse IP ou nom de domaine que le client de réplication devra utiliser pour interroger l'annuaire du module. L'adresse proposée par défaut est celle de l'interface eth0 du module mais cette valeur dépend de l'architecture

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

réseau mise en place et notamment de la configuration des pare-feu présents entre le module EOLE et le client de réplication ;

- Selon la configuration du serveur OpenLDAP du module, le choix du protocole à utiliser pour la réplication peut être proposé. Si à la question `Utiliser le protole ldaps (port 636) pour la réplication` la réponse est laissée à `oui`, la réplication utilisera le protocole LDAPS sinon elle utilisera le protocole LDAP.

Mise en place manuelle

Il faut copier le fichier `/root/replication-<numero_etab>.conf` du fournisseur dans le dossier `/etc/ldap/replication` du serveur Seshat.
Puis, sur le module Seshat, il faut exécuter la commande `gen_replication.py`.

Mise en place via Zéphir

Si le serveur fournisseur (Scribe ou Horus) et le serveur Seshat sont enregistrés sur le même serveur Zéphir, celui-ci peut se charger de la mise en place de la configuration sur le serveur Seshat.

La connexion à Zéphir est proposée automatiquement en fin d'exécution du script :
`Veuillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :`



Il est impératif de connaître l'identifiant Zéphir du serveur Seshat pour finaliser la transaction.
`Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :`

Les configurations de réplication envoyées via Zéphir sont consultables dans l'application web Zéphir en utilisant le lien `configurations de réplication LDAP` disponible sur la page décrivant l'état du serveur Seshat.



Consultation des configurations de réplications LDAP dans l'application Zéphir



Les configurations envoyées via Zéphir sont stockées dans le répertoire `/etc/ldap/replication/zephir` du serveur Seshat.

Suivi et débogage



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour obtenir des informations concernant la réplication, il faut paramétrer slapd avec le *log level* 16384.

Cela se traduit par la ligne de commande suivante :

```
slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 16384
```

Attention, ce mode peut être très verbeux.

12. Transformer un module Horus en module HorusAD

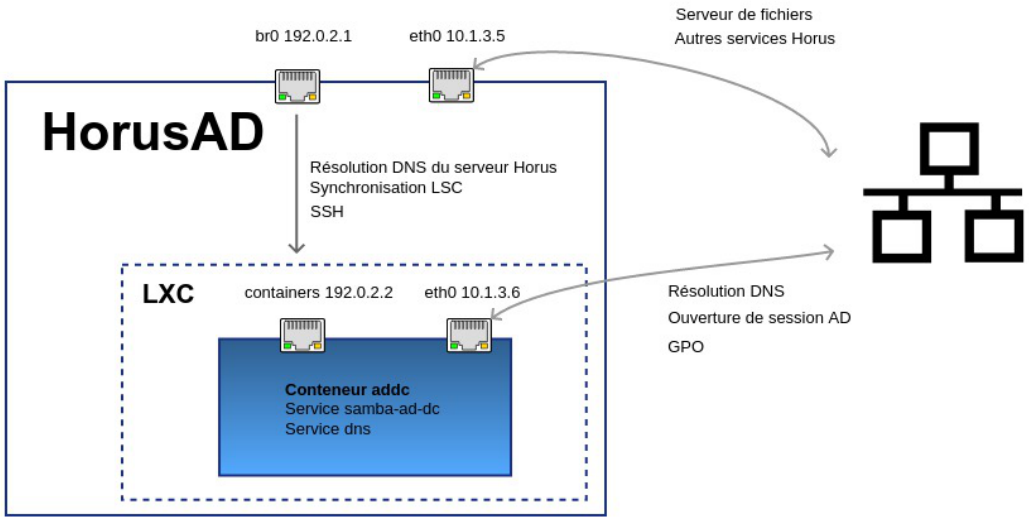
L'ajout du paquet `horus-ad` permet de transformer un module Horus existant en contrôleur de domaine Active Directory[p.752] tout en conservant toutes les fonctionnalités du module Horus : la gestion des utilisateurs et des groupes, EAD, serveur de bases de données...

Grâce à LXC[p.768] tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.



Les flux réseaux entre le conteneur et le maître

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La transformation du module Horus en module HorusAD est irréversible.

Pré-requis

Il faut disposer d'un serveur Horus fonctionnel ou partir d'une nouvelle installation du module Horus, la procédure est la même.

Sur un serveur existant, il faut procéder à une ré-instanciation du serveur tandis que pour une nouvelle installation, il faut installer le paquet et effectuer l'instanciation.

Installation

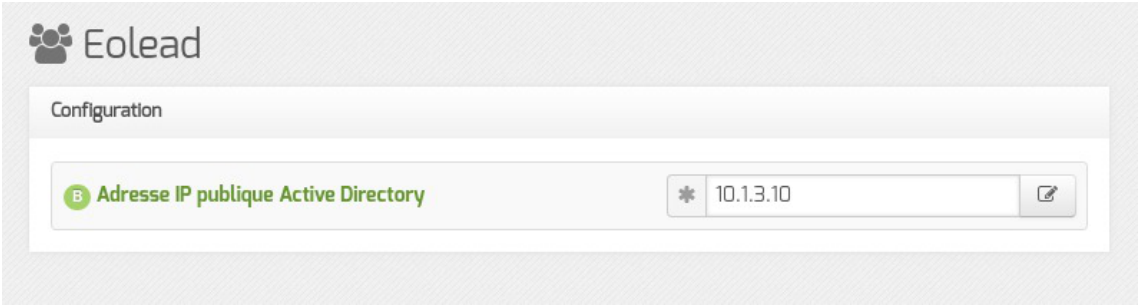
L'installation du paquet `horus-ad` sur un module Horus active automatiquement la fonctionnalité AD :

```
# apt-eole install horus-ad
```

Configuration du module Horus devenu HorusAD

Adresse du service Active Directory

Par rapport à un module standard, une seule nouvelle variable est à renseigner pour ajouter la fonctionnalité Active Directory :

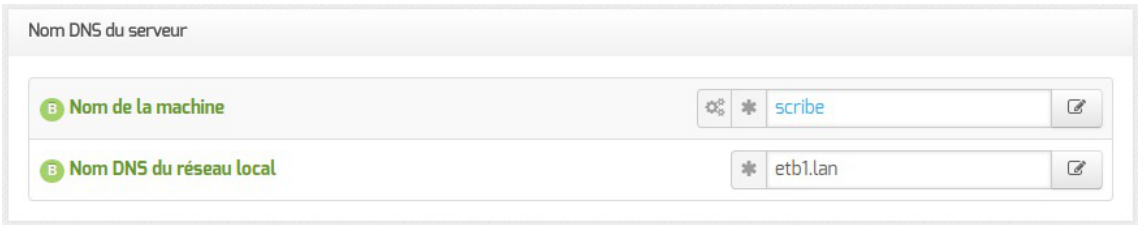


La valeur à saisir est une adresse IP disponible sur le réseau, elle permet d'exposer le service Active Directory.

Si un serveur DHCP[p.758] est utilisé, c'est cette adresse IP qu'il faut diffuser en tant que DNS pour les clients.

Choix du nom de domaine et configuration DNS

Par défaut le nom du domaine Active Directory (realm[p.776]) est le `Nom DNS du réseau local` paramétré dans l'onglet `Général`.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le choix de cette valeur est primordial pour la bonne intégration du serveur dans une infrastructure existante.



La mise en place d'un service Active Directory dans une infrastructure impose des contraintes fortes en terme de configuration DNS.

Si le domaine Active Directory est une sous-zone d'un domaine géré par un serveur DNS externe (le module Amon, par exemple), ce dernier doit lui déléguer la gestion de cette sous-zone.

Une fois instancié, le serveur d'origine utilise en tant que serveur DNS le serveur Active Directory qu'il héberge tandis que ce dernier se sert du premier DNS déclaré dans la variable `Adresse IP du serveur DNS` comme DNS de forward[p.759].

Le nom du serveur Active Directory qui est également celui du conteneur LXC est `addc`. Cette valeur n'est pas modifiable.

Instanciation

Une fois configuré, il faut instancier ou ré-instancier le serveur à l'aide de la commande `instance`.

Génération du conteneur addc

Lors de la première instance, le conteneur LXC, nommé `addc` est généré puis configuré. Cette opération dure plusieurs minutes.

```
run-parts: executing /usr/share/eole/preservice/05-eolead instance

Génération du conteneur addc
Checking cache download in /var/cache/lxc/xenial/rootfs-amd64 ...
Installing packages in template:
 apt-transport-https,ssh,vim,language-pack-en,language-pack-fr
Downloading ubuntu xenial minimal ...
I: Retrieving InRelease
I: Checking Release signature
I: Valid Release signature (key id 790BC7277767219C42C86F933B4FE6ACC0B21F32)
I: Retrieving Packages
I: Validating Packages
   [...]
```

Une fois le conteneur fonctionnel, l'initialisation du contrôleur de domaine débute.

Deux utilisateurs Active Directory sont créés, 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 :

```
Initialisation DC
Generation de la clef SSH pour les echanges entre DC
Création du mot de passe "Administrator" Active Directory :
Confirmation du mot de passe :
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `admin` : compte d'administration à privilégier pour la jonction des clients au domaine et les opérations courantes.

```
Creation utilisateur 'admin'
Création du mot de passe "admin" Active Directory :
Confirmation du mot de passe :
```



Le mot de passe de l'utilisateur *admin de l'Active Directory* est écrasé par celui de l'utilisateur *admin de l'annuaire Horus* lorsque ce dernier est modifié ou que la synchronisation des mots de passe est forcée.

Intégration au domaine et synchronisation de l'annuaire

Dans l'infrastructure HorusAD, le serveur Samba[p.777] du module Horus initial devient membre du nouveau domaine Active Directory.

Cette modification n'est pas entièrement automatisée, il est nécessaire de saisir à nouveau le mot de passe du compte `Administrator` créé précédemment.

```
run-parts: executing /usr/share/eole/posttemplate/05-eolead instance

Intégration au domaine Active Directory
Mot de passe de l'utilisateur Administrator pour le domaine ETB1.LAN :
Using short domain name -- ETB1
Joined 'HORUS' to dns domain 'etb1.lan'
Mise à jour du mot de passe dans les fichiers de configuration

Synchronisation ldap
   [...]
```

Une fois cette opération réalisée, la synchronisation initiale entre l'annuaire OpenLDAP du module Horus et l'annuaire Active Directory est exécutée.

Celle-ci est plus ou moins longue et verbeuse selon que l'annuaire du module Horus est déjà peuplé ou non.

La synchronisation des annuaires via LSC ne permet pas la synchronisation des mots de passe.

Celle-ci fait l'objet d'une procédure dédiée qui peut être exécutée à l'instance :

```
run-parts: executing /usr/share/eole/posttemplate/05-eolead-pwd instance
Voulez-vous (re)synchroniser les mots de passe des utilisateurs ? [oui/non]
[oui] :
Synchronisation en cours (1 mots de passe)...

```

Si l'annuaire contient beaucoup de comptes, cette opération peut durer plusieurs minutes.

Dans le cadre d'une nouvelle installation, seul le mot de passe du compte `admin` est synchronisé.

Trucs & astuces

La commande diagnose permet de connaître l'état du service :

```
*** Serveur de fichiers
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
2
3 Test du fichier de configuration :
4 .                     Syntaxe => Ok
5
6 Partages :
7 .           Partage (SMB/TCP) => Ok
8 .           Partage (NMB/UDP) => Ok
9 .            Connexions samba => 0
10
11 .             Ticket kerberos => Ok
12 .         Synchronisation LSC => Ok
```

Synchronisation

Forcer la synchronisation manuelle des comptes depuis le maître :

```
# /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 maître :

```
# 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)
```

Relancer le service samba-ad-dc

Le service samba-ad-dc est dans le conteneur addc, pour relancer le service :

```
# ssh addc "service samba-ad-dc restart"
```

Liste d'utilisateurs

Lister tous les utilisateurs depuis le maître :

```
# ssh addc "ldbsearch -H /var/lib/samba/private/sam.ldb -S
'(objectclass=user)' cn | grep ^cn:"
```

Attributs utilisateur

Chercher un utilisateur depuis le maître :

```
# ssh addc "ldbsearch -H /var/lib/samba/private/sam.ldb -S cn=p.nom"
```

Journaux

Les journaux de l'outil LSC sont disponibles dans :

- `/var/log/lsc/` pour les synchronisations manuelles ;
- `/var/log/rsyslog/local/lsc/` pour les opérations réalisées par le démon.

Les journaux du service Active Directory sont disponibles sur le maître dans le répertoire `/var/log/samba-ad-dc/`.

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.765].

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.770].

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.775].

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.752] 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.774] 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.763].

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.758] local et/ou d'un serveur PXE[p.775].

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.770] (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.771], 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.783]).

Le logiciel utilisé, Nginx[p.771], 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.778] Exim[p.761].

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.774] / IMAP[p.765].

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.779] : proxy cache ;
- e2guardian[p.759] : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM[p.771] ou Kerberos[p.766].

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.775].

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.767].

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.780].

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.

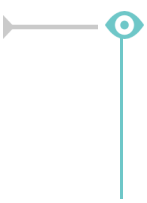
Conteneurs

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.753].

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.759] local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.754].

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.758].

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.775].

Logiciels et services

Le paquet `eole-ltsp-server` s'appuie sur les service NBD[p.770] et LDM[p.767].

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.777].

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.764].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync[p.757].

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.778].

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.776].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.779].

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.757] 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.774]** : permet de modifier un template[p.781] fourni par EOLE ;
- le **dictionnaire[p.758] 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.781] 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.781] 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.759] :
> 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.357]

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.

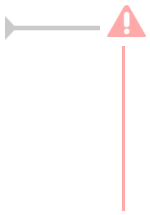
Les services à activer/désactiver se définissent dans le dictionnaire grâce à la balise **<service>.**

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.

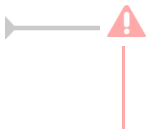
La balise service peut également être utilisée pour activer/désactiver des configurations de site web apache2 (commandes : `a2ensite` / `a2dissite`).

Comme pour les services système, l'activation d'un site peut être conditionnée par une `servicelist`.

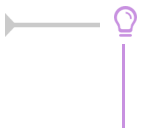
On peut ainsi gérer le lien symbolique suivant : `/etc/apache2/sites-enabled/monsite` avec :

```
<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>

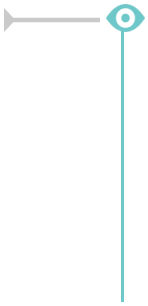
La balise **<host>** permet de déclarer des hôtes à ajouter dans le fichier `/etc/hosts` du maître et/ou des conteneurs.

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.



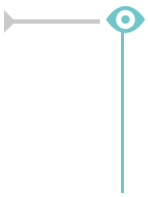
```
<containers>
    <container name="proxy" id='20'>
        <package>eole-proxy-pkg</package>
        <service>squid</service>
        <host hostlist='auth_smb' name='nom_serveur_smb' ip=
'ip_serveur_smb' instance_mode='when_container' crossed='False' comment=
"serveurs d'authentification SMB"/>
    </container>
</containers>
```

Montage d'une partition <disknod>

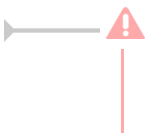
La balise **<disknod>** permet de le montage d'une partition du maître à l'intérieur d'un conteneur.
Par exemple, le montage de la partition `/home` dans le conteneur fichier.

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.780] 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`

```
1  <service_access service='genconfig'>
2      <port>7000</port>
3  </service_access>
4  <service_restriction service='genconfig'>
5      <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type=
   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
6      <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type=
   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
7      <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type=
   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
8      <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type=
   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
9      <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type=
   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
10 </service_restriction>
11
```

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 choisir une icône, il faut se rendre sur les pages ci-dessus et recopier le nom de l'icône. Pour la font Mfizz il faut enlever le préfixe `icon-`.



```
<family name='messagerie' mode='basic' icon='envelope'>
<variable name='system_mail_from' type='mail' description="Adresse électronique d'envoi pour le compte root"/>
</family>
```

Variable : <variable>

Une variable contient une description et, optionnellement, une valeur EOLE par défaut.

Les variables peuvent être à valeur unique ou multi-valuées.

Les balises **<variable>** sont incluses obligatoirement dans une balise **<family>**.

Les attributs de la balise *variable* sont les suivants :

- l'attribut **name** (obligatoire) est le nom de la variable ;
- l'attribut **type** (obligatoire) permet d'utiliser un type EOLE avec des vérifications automatiques (fonctions de vérifications associées a chaque type de variable) ;
- l'attribut **description** permet de définir le libellé à afficher dans l'interface de configuration du module ;
- l'attribut **multi** permet de spécifier qu'une variable pourra avoir plusieurs valeurs (par exemple pour un DNS, on aura plusieurs adresses IP de serveurs DNS) ;
- l'attribut **mode** permet de définir le mode d'affichage de la variable (*basic, normal* ou *expert*) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- si l'attribut **hidden** vaut *True*, la variable ne sera pas affichée dans l'interface de configuration (on peut par exemple souhaiter masquer des variables dont la valeur est calculée automatiquement) ;
- si l'attribut **disabled** vaut *True*, la variable sera déclarée comme désactivée.
- si l'attribut **mandatory** vaut *True*, la variable sera considérée comme obligatoire, cet attribut remplace l'ajout d'un *check obligatoire* au niveau des conditions :
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir une variable déjà définie dans un autre dictionnaire ;
- si l'attribut **exists** vaut *False*, cela permet de définir une variable si et seulement si elle n'a pas déjà été définie dans un autre dictionnaire.
- si l'attribut **remove_check** vaut *True* pour une variable redéfinie, alors toutes les validations (*check*) associées à cette variable sont réinitialisées ;
- si l'attribut **remove_condition** vaut *True* pour une variable redéfinie, alors toutes les conditions associées à cette variable sont réinitialisées (attention, **remove_condition** n'est disponible qu'à partir de la version **EOLE 2.5.2**) ;
- si l'attribut **auto_freeze** vaut *True*, la variable devient à verrouillage automatique. Sa valeur est verrouillée dès le premier enregistrement de la configuration. Dans l'interface de configuration du module, ces variables sont identifiées par la présence d'un cadenas. Ce dernier apparaît verrouillé une fois le serveur instancié ;
- si l'attribut **auto_save** vaut *True*, la variable devient à enregistrement obligatoire. Sa valeur est obligatoirement enregistrée dans le fichier de configuration et elle n'est donc pas automatiquement modifiée si sa valeur par défaut change au niveau des dictionnaires. On retrouve ainsi un fonctionnement équivalent à celui disponible sur EOLE 2.3.

Les principaux types de variables Creole sont les suivants :

- *number* : la valeur de la variable doit être du type "int". La fonction python `int(value)` ne doit pas retourner d'erreur ;
- *string* : la valeur de la variable doit être du type "unicode" ;
- *ip* : valeur de type IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *local_ip* : la même chose que IP, sauf que les adresses réservées et privées soulèvent un warning (voir *IPy* pour des informations sur les adresses réservées et privées) ;
- *netmask* : adresse de masque réseau. La valeur doit passer ce test : `IPy.IP('0.0.0.0/{0}'.format(value))` ;
- *network* : adresse réseau. La valeur doit passer ce test : `IPy.IP(value)` ;
- *broadcast* : adresse de broadcast. : La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *netbios* : alphanumérique autorisé sauf pour le 1er caractère qui doit forcement être du type alpha, minimum 2 et maximum 15 caractères ;
- *domain* :
  - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`

  ou

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

  - alphanumérique et '.' autorisé sauf pour le 1er caractère qui doit forcement être du type alpha. Le '.' est obligatoire. Minimum 2 et maximum 255 caractères ;
- *domain_strict* : nom DNS uniquement (adresse IP interdite) ;
- *unix_user* : nom d'utilisateur ou de groupe Unix ;
- *web_address* : adresse Internet. Doit débuter par `http://` ou `https://` ;
- *hostname* :
  - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`

  ou
  - alphanumérique autorisé sauf pour le 1er caractère qui doit forcement être du type alpha.Minimum 2 et maximum 63 caractères ;
- *hostname_strict* : nom d'hôte uniquement (adresse IP interdite) ;
- *mail* : adresse e-mail ;
- *port* : entier compris entre 1 et 65535 ;
- *filename* : tout chemin Unix (fichier ou répertoire) ;
- *oui/non* : seules valeurs possibles : "oui" et "non" ;
- *yes/no* : seules valeurs possibles : "yes" et "no" ;
- *on/off* : seules valeurs possibles : "on" et "off" ;
- *password* : la valeur de la variable est masquée dans l'interface une fois le champ validé. Elle est affichée en clair lorsque le champ est édité. Aucune contrainte n'est associée à ce type de variable.

Comportement avec redefine='True' et remove_check='False'

- si la nouvelle variable fournit une valeur par défaut, elle remplace l'ancienne ;
- si la nouvelle variable fournit un ou plusieurs des attributs suivants : *description*, *hidden*, *mandatory*, *auto_freeze*, *mode*, les valeurs des nouveaux attributs remplacent les anciennes ;
- les attributs *type* et *multi* ne sont pas modifiables ;
- si un nouveau *valid_enum* est défini dans les fonctions *checks*, il remplace l'ancien ;
- si de nouveaux *disabled_if(_not)_in* sont définis, ils remplacent les anciens ;
- les autres conditions et contraintes sont ajoutées à celles qui étaient déjà définies.

Valeur : <value>

A l'intérieur d'une balise **<variable>**, il est possible de définir une balise **<value>** permettant de spécifier la valeur par défaut de la variable.

Séparateurs : <separators> et <separator>

Les séparateurs permettent de définir des barres de séparation au sein d'une famille de variable dans l'interface de configuration.

Les séparateurs définis dans un dictionnaire sont placés dans la balise **<separators></separators>** dans la balise **<variables>**.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

A l'intérieur de la balise **<separators>** il faut spécifier autant de balises **<separator>** que de séparateurs souhaités.

Les attributs de la balise *separator* sont les suivants :

- l'attribut **name** (obligatoire) correspond au nom de la variable suivant le séparateur ;
- si l'attribut **never_hidden** vaut *True*, le séparateur sera affiché même si la variable associée est masquée.

Dans le cas où il n'y a aucune variable à afficher dans le bloc défini par le séparateur, celui-ci est forcément masqué.

Exemple

Variables, familles et séparateurs

```
<variables>
  <family name='services'>
    <variable name='activer_esu' type='oui/non' description="Utiliser le logiciel ESU" hidden='True'>
      <value>oui</value>
    </variable>
  </family>
  <family name='esu'>
    <variable name='esu_proxy' type='oui/non' description="Activer le proxy ESU">
      <value>non</value>
    </variable>
    <variable name='esu_proxy_server' type='domain' description='Adresse du proxy ESU' mandatory='True'/>
    <variable name='esu_proxy_port' type='port' description='Port du proxy ESU' mandatory='True'>
      <value>3128</value>
    </variable>
    <variable name='esu_proxy_bypass' type='string' description='Ne pas utiliser le proxy ESU pour' multi='True'>
      <value>127.0.0.1</value>
    </variable>
  </family>
  <separators>
    <separator name='esu_proxy'>Proxy ESU</separator>
  </separators>
</variables>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3.4. Comportement des variables

En plus des propriétés décrites explicitement dans les dictionnaires Creole, certaines variables se voient ajouter des contraintes ou des modifications de propriétés en fonction de certains paramètres.

Les variables possédant la propriété `auto_freeze='True'` sont obligatoirement affichées en mode basique lors de la saisie initiale, ceci afin d'attirer l'attention de l'utilisateur sur le fait qu'elles ne seront plus modifiables ultérieurement.
Une exception a été ajoutée à cette règle, si la propriété `expert='True'` est explicitement ajoutée sur la variable, celle-ci apparaîtra uniquement dans le mode expert.

Les variables obligatoires (`mandatory='True'`) ne possédant pas de valeur par défaut (calculée ou non) sont obligatoirement affichées en mode basique, puisque l'utilisateur devra forcément les renseigner.

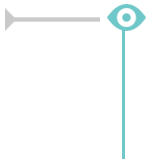
Les variables non obligatoires (`mandatory='False'`) possédant une valeur par défaut (balise `<value>`) deviennent obligatoires.

2.3.5. Mettre en place des contraintes

Des fonctions (contraintes) peuvent être utilisées pour grouper / tester / remplir / conditionner des variables.
L'ensemble des contraintes d'un dictionnaire se place à l'intérieur d'un nœud XML **<constraints></constraints>**.

Lien entre variables : <group>

Il est possible de lier des variables sous la forme d'une relation maître-esclave(s).
La variable maître doit obligatoirement être multi-valuée (`multi='True'`).
Elle se définit dans l'attribut **master**.
Les variables esclaves sont définies entre les balises **<slave>**.
Les variables esclaves deviennent automatiquement multi-valuées.



```
<group master='adresse_ip_eth0'>
    <slave>adresse_netmask_eth0</slave>
    <slave>adresse_network_eth0</slave>
</group>
```

Calcul automatique modifiable <fill> ou non <auto>

Le calcul automatique permet d'associer automatiquement (par le calcul) une valeur par défaut à une variable.
Cette valeur peut être :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- éditable par l'utilisateur : balise *<fill>* ;
- non éditable par l'utilisateur (exemple : l'IP d'un serveur en DHCP) : balise *<auto>*.



Contrairement aux versions précédentes si l'utilisateur a choisi de conserver la valeur par défaut d'une variable affectée par un *fill*, le calcul de la valeur sera réalisé à chaque fois, comme pour les variables *auto* sauf si la variable possède l'attribut `auto_save='True'`.



Les calculs *auto* ne sont pas compatibles avec les variables à verrouillage automatique (`auto_freeze`) ou à enregistrement obligatoire (`auto_save`).

L'attribut *name* correspond au nom de la fonction qui sera utilisée pour le calcul.

Les fonctions utilisées peuvent être :

- des fonctions natives de Tiramisu[p.781] ;
- 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>
```

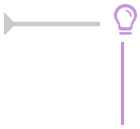
  Il est possible d'utiliser des *calc_multi_condition* avec des variables non déclarées ou désactivées mais uniquement si toutes les variables testent la même condition.

  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 :

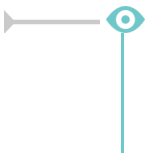
- des fonctions natives de Tiramisu[p.781] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

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.

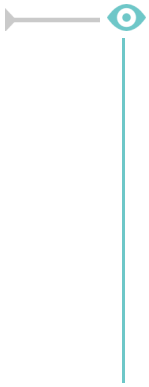
Il est possible de créer des boucles, des tests, de gérer les lignes optionnelles, de réaliser des inclusions répétées, ...

La déclaration de test : if

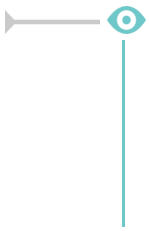
Syntaxe :

`%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
```



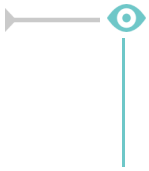
```
%if %%toto == 'yes' and ( %%titi != "" or %%tata not in ['a','b','c'] ) :
la condition a été validée
%end if
```

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 #`

Version : révision : Juin création : Février 2017 2018
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.761].

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.654]

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.766].



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.756] ;
- 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 :

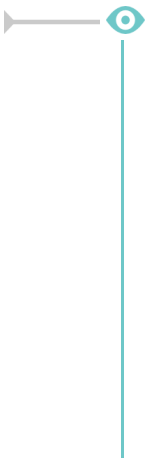
- d'instancier un seule template existant sur le module en utilisant la ou les destinations déclarées dans le dictionnaire :
  `# CreoleCat -t hostname`
- d'instancier un template existant sur le module en redirigeant le résultat dans un fichier spécifique :
  `# CreoleCat -t hostname -o /tmp/hostname.txt`
- 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.757].

- `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.756].

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.774] 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.782], 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.661]

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.661]

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

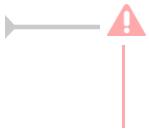


La commande `uname -r` permet de connaître le noyau en cours d'utilisation.

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.781].

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est cron[p.758] qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bareos[p.753] 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.784] (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.758] 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.780] 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.620]

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.768] (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.757]) 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.762]) :

- **<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) :

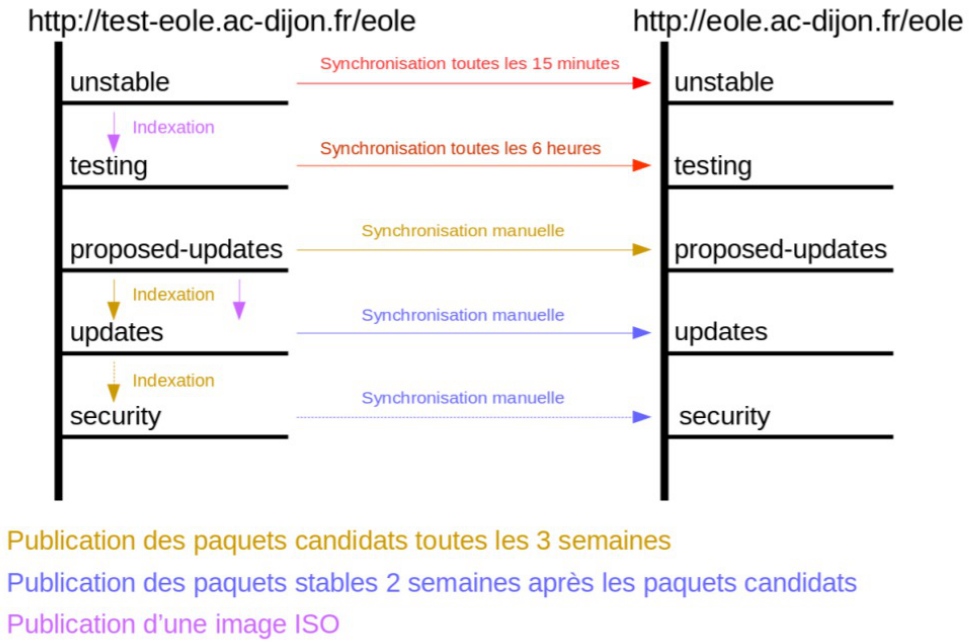
- **eole-2.6-unstable** : paquets de développement pouvant contenir des évolutions fonctionnelles, des corrections de sécurité ou de dysfonctionnement ;
- **eole-2.6-testing** : paquets candidats (correspondant aux images RC de la distribution) qui sont éligibles pour passer en version stable après validation ;
- **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.753] (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.764] 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.753] 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

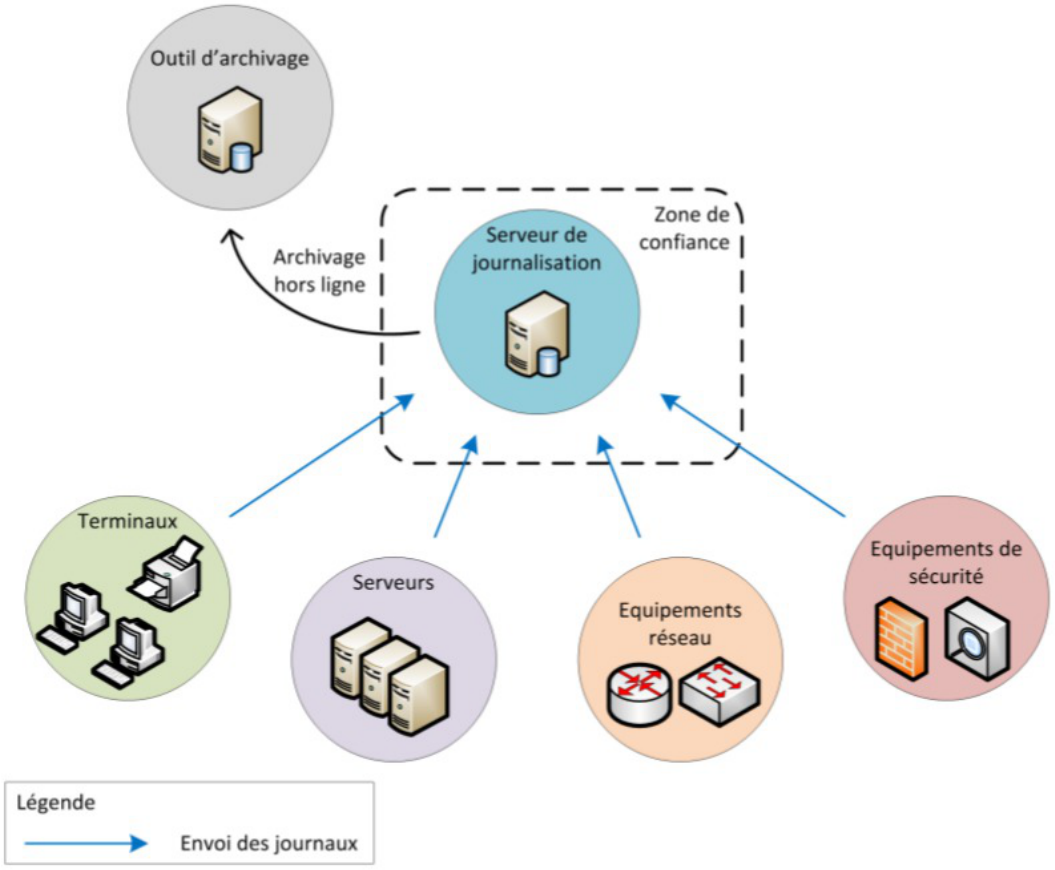
- l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux doit être prise

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

en compte dans le dimensionnement des équipements,

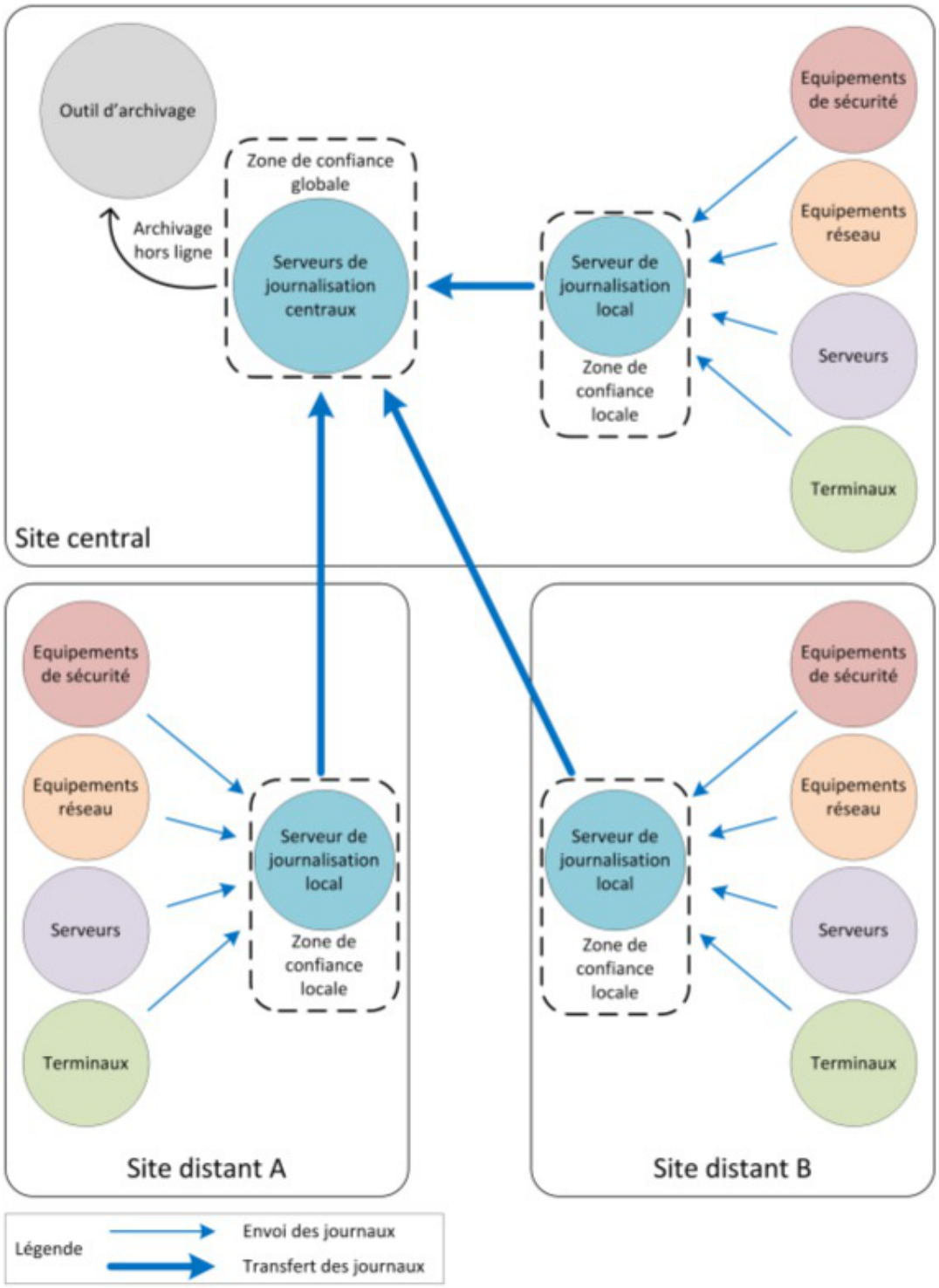
Recommandations d'architecture et de conception

- 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 Horus

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un service d'annuaire OpenLDAP.

L'installation d'`eole-annuaire` entraîne celle d'`eole-client-annuaire`.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

http://www.openldap.org/

Historique

L'annuaire LDAP est la brique centrale de plusieurs modules EOLE.

Grâce au paquet `eole-annuaire`, la configuration de base est identique sur les modules Horus, Scribe, AmonEcole, Zéphir, Seshat et Thot bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `annuaire (id=10)`.

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.2. eole-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 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>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

1.3. eole-bareos

Le paquet `eole-bareos` permet d'installer et de configurer la solution de sauvegarde Bareos[p.753].

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).

1.4. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

1.5. 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`).

1.6. eole-dhcp

Le paquet `eole-dhcp` permet la mise en place d'un serveur DHCP[p.758] local et/ou d'un serveur PXE[p.775].

Logiciels et services

Le paquet `eole-dhcp` s'appuie sur les services dhcp3-server et tftpd-hpa.

http://www.isc.org/software/dhcp

Historique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

1.7. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP[p.778] Exim[p.761].

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)`.

1.8. eole-fichier-primaire

Le paquet `eole-fichie-primaire` permet la mise en place d'un serveur de fichiers PDC[p.774] complet.

Logiciels et services

Le paquet `eole-fichie-primaire` permet de gérer les services suivants :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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`).

1.9. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de base de données Interbase[p.765].

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)`

1.10. eole-mysql

Le paquet `eole-mysql` permet la mise en place d'un serveur de base de données MySQL[p.770].

Logiciels et services

Le paquet `eole-mysql` s'appuie principalement sur le service mysql-server.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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)`.

1.11. 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).

1.12. eole-proftpd

Le paquet `eole-proftpd` permet la mise en place d'un serveur FTP[p.763].

Logiciels et services

Le paquet `eole-proftpd` permet de gérer le service proftpd (serveur FTP).

http://www.proftpd.org/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Historique

Les services fournis sont spécifiques aux modules Horus, Scribe et eSBL.

Conteneurs

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

1.13. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.
Le logiciel utilisé, Nginx[p.771], 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).

1.14. eole-web

Le paquet `eole-web` permet la mise en place d'un serveur web.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

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.

2. Ports utilisés sur le module Horus

Le module Horus propose de nombreux services.

Ce document donne la liste exhaustive des ports utilisés sur un module Horus 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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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)

Ports spécifiques au module Horus

- 21/tcp : ftp (ProFTPD)
- 67/udp : dhcp
- 69/udp : tftp
- 80/tcp : http (Apache2)
- 137/udp : nmbd
- 138/udp : nmbd
- 139/tcp : samba (netbios)
- 389/tcp : ldap (OpenLDAP)
- 443/tcp : https (Apache2)
- 445/tcp : samba (sans netbios)
- 631/tcp+udp : CUPS
- 636/tcp : ldaps (OpenLDAP sur le port SSL)
- 647/tcp : failover DHCP, port en écoute sur le serveur primaire et port d'émission pour le serveur secondaire

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 847/tcp : failover DHCP, port en émission sur le serveur primaire et port d'écoute pour le serveur secondaire
- 3050/tcp : Xinetd (Interbase)
- 3306/tcp : MySQL
- 7080/tcp : horus_frontend
- 7911/tcp : API OMAPI (configuration du DHCP)
- 9101/tcp : bareos-dir
- 9102/tcp : bareos-fd
- 9103/tcp : bareos-sd

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. L'annuaire LDAP du module Horus

L'annuaire LDAP[p.766] du module Horus est basé sur le logiciel OpenLDAP (version 2.4).

Il est la pièce maîtresse du module puisqu'il est utilisé par quasiment tous les logiciels intégrés sur Horus.

Il fournit les services suivants :

- authentification utilisateur ;
- comptes Samba ;
- définition des groupes et des partages.

Horus utilise l'annuaire LDAP pour stocker la liste des utilisateurs et des groupes ainsi que leurs paramètres. Cet annuaire est initialisé avec un utilisateur et plusieurs groupes spéciaux :

- l'utilisateur dédié à toutes les tâches d'administrations :
  - `admin` (membre du groupe `DomainAdmins`)
- les groupes dédiés à l'environnement Windows :
  - `DomainAdmins`
  - `DomainUsers`
  - `DomainComputers`
  - `PrintOperators`
- les groupes propres à Horus :
  - `minedu`
  - `applidos`

Le groupe `DomainAdmins` correspond au groupe `Administrateurs du domaine`. Les membres de ce groupe sont `Administrateur` des postes Windows et bénéficient d'un **accès en lecture/écriture sur l'ensemble des partages** du module Scribe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le groupe `DomainUsers` correspond au groupe `Utilisateurs du domaine`. Il s'agit des utilisateurs standards n'ayant pas de privilèges particuliers.

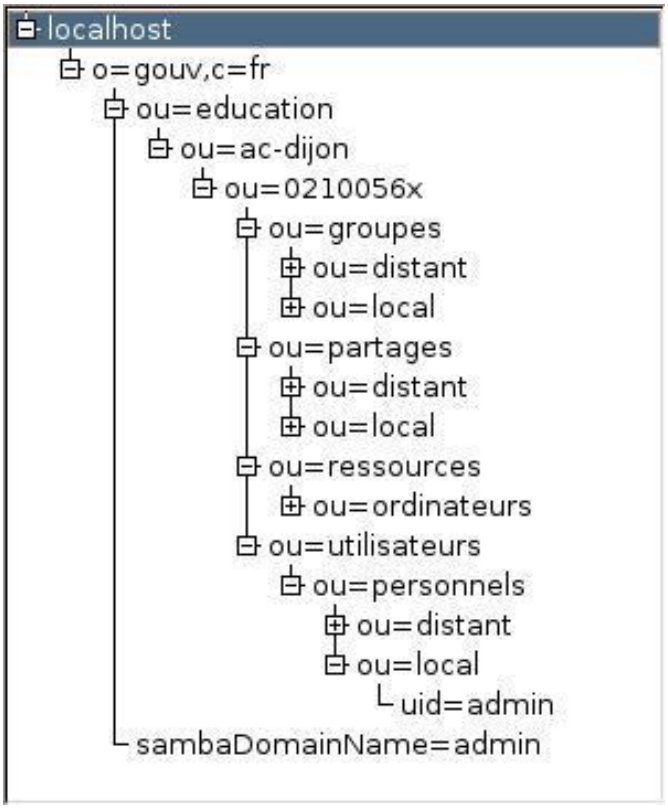
Le groupe `DomainComputers` est le groupe principal pour les stations intégrées au domaine.

Le groupe `PrintOperators` correspond au groupe `Administrateurs des imprimantes`.

Les groupes `minedu` et `applidos` sont des groupes propres à Horus permettant d'appliquer des méthodes de gestion spécifiques.

3.1. Arborescence de l'annuaire

L'arborescence LDAP (Lightweight Directory Access Protocol) du module Horus utilise le **nom de l'académie** et le **numéro de l'établissement** pour offrir à chaque établissement des branches personnalisées.



Arborescence de l'annuaire ldap d'Horus

3.2. Utilisateurs spéciaux

Le compte d'administration

L'administrateur LDAP[p.766] de l'application *(rootdn)* est l'utilisateur spécial :

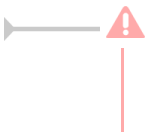
cn=admin,o=gouv,c=fr

Pour des raisons pratiques et de sécurité, le mot de passe de cet utilisateur est changé régulièrement (mise à jour et reconfiguration du module).

Il est possible de récupérer ce mot de passe "en clair" dans certains fichiers présents sur le système :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`/etc/smbldap-tools/smbldap_bind.conf`
ou de le modifier "manuellement" à l'aide du script `ldap_pwd.py` .



Ne pas confondre l'utilisateur `admin` de l'annuaire LDAP avec l'utilisateur `admin` du module Scribe ou Horus. Celui-ci est considéré dans l'annuaire comme étant un enseignant.

Le compte en lecture seule

Afin de répondre à certains besoins applicatifs, le compte en lecture seule `reader` a été ajouté :

cn=reader,o=gouv,c=fr

L'utilisation de ce compte par les applications leurs permettent d'accéder aux attributs LDAP protégés par des ACL[p.752]. Ces attributs ne sont pas accessibles par des requêtes anonymes et l'utilisation d'un compte en lecture seule permet de préserver la sécurité de l'annuaire.

Pour faciliter la mise en œuvre d'applications distantes, le mot de passe de cet utilisateur n'est jamais modifié après avoir été généré.

Le mot de passe de cet utilisateur est stocké dans le fichier `/root/.reader`



La validité du mot de passe de l'utilisateur `reader` peut être testée avec la commande suivante :

```
ldapsearch -x -D cn=reader,o=gouv,c=fr -w `cat /root/.reader` uid=admin uid
```

3.3. Entrée ordinateur du domaine

Lors de la jonction au domaine d'ordinateur (pour les versions supérieures ou égales à Windows 2000), un compte de machine est créé dans l'annuaire. Ces comptes sont stockés dans la branche :

```
ou=ordinateurs,ou=ressources,ou=numero_etab,ou=nom_academie,ou=education,o=(
```

Classes d'objet

Les ordinateurs héritent des classes d'objet suivantes :

- posixAccount (`nis.schema`)
- sambaSAMAccount (`samba.schema`)
- account (`cosine.schema`)

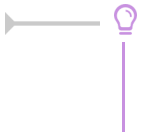
Attributs

Dans certains cas (formatage ou renouvellement d'une station), il peut être nécessaire de supprimer l'ordinateur de l'annuaire.

Les attributs spécifiques aux machines sont les suivants :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- uid : identifiant, c'est le nom de la machine suivi du caractère **$**
- cn : nom de la machine (généralement identique à l'uid)



Les entrées ordinateurs peuvent être obtenues à l'aide d'une requête LDAP anonyme : `ldapsearch -x uid=*$`

3.4. Entrée partage

Les partages de l'établissement sont placés dans la branche :

```
ou=local,ou=partages,ou=numero_etab,ou=nom_academie,ou=education,o=gouv,c=fr
```

Classes d'objet

Les partages héritent des classes d'objet suivantes :

- sambaFileShare (`eoleshare.schema`)

Attributs

Les attributs spécifiques aux partages sont les suivants :

- cn : chemin samba du partage (`smb://serveur_samba/partage`)
- sambaShareName : nom du partage
- sambaShareGroup : groupe associé au partage, par convention sur Scribe un partage est toujours associé au groupe du même nom
- sambaFilePath : chemin Unix du partage (`/home/workgroups/partage`)
- sambaShareURI : URI du partage (`\\serveur_samba\partage`)
- sambaShareModel : modèle de partage Samba à utiliser pour déclarer le partage
- sambaShareDrive : lettre de lecteur associée au partage (facultatif)
- sambaShareOptions : options spécifiques (exemple : *sticky bit* sur les partages Horus, facultatif)

3.5. Annuaire : diagnostic et résolution de problème

Exécuter le service en mode débogage

Les commandes suivantes permettent de relancer le service *slapd* en mode débogage :

```
# service slapd stop
# slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 256
```


L'option -d pour le débogage est suivie de la valeur de masquage 256 qui offre la verbosité nécessaire.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ré-indexer l'annuaire

Dans certaines situations, la ré-indexation de l'annuaire s'avère nécessaire.

Les commandes suivantes permettent de re-créer les fichiers d'index :

```
# service slapd stop
# su openldap -s /bin/bash -c "slapindex -f /etc/ldap/slapd.conf -v"
```

Sauvegarde et restauration de l'annuaire

Export automatique de l'annuaire

Sur les modules EOLE possédant un annuaire local, un export de l'annuaire est réalisé toutes les nuits dans le fichier `/home/backup/sauv_ldap.ldif`.

C'est le cas même si la sauvegarde Bareos n'est pas activée car c'est eole-schedule[p.760] qui gère l'export.

La programmation de l'export quotidien peut-être vérifiée à l'aide de la commande suivante :

```
# manage_schedule -l
```

Si l'export automatique est bien activé, les lignes suivantes apparaissent dans le résultat :

```
  * les tâches journalières se feront tous les jours à 01:14 (hors sauvegarde)
   - avant sauvegarde
    + Exportation de l'annuaire LDAP (annuaire)
```

Restauration de l'export quotidien

En cas de crash de l'annuaire OpenLDAP, restaurer l'annuaire tel qu'il était la nuit précédente peut permettre de gagner du temps sur la mise à disposition des services.

La restauration s'effectue à l'aide des commandes habituelles :

```
# service slapd stop
# rm -f /var/lib/ldap/[^D]*
# slapadd -f /etc/ldap/slapd.conf -l /home/backup/sauv_ldap.ldif
# chown -R openldap: /var/lib/ldap/
# service slapd start
```

Restauration de la dernière sauvegarde

Dans le cas où la sauvegarde Bareos est utilisée, il est possible de restaurer l'annuaire tel qu'il était lors de la dernière sauvegarde.

La restauration de l'annuaire depuis la sauvegarde s'effectue à l'aide de la commande :

```
# bareosrestore.py --ldap
```

Export manuel de l'annuaire

La commande suivante permet d'exporter le contenu de l'annuaire dans un fichier :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > annuaire.ldif
```

Voir aussi...

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Gestion des tâches planifiées eole-schedule [p.667]

Restauration partielle [p.481]

4. La gestion du SID

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 d'un module Scribe ou Horus, Samba[p.777] génère aléatoirement son propre SID.

Dans certains cas (migration, restauration), il est nécessaire de le modifier afin d'obtenir un fonctionnement correct avec d'anciennes données.

Tous les utilisateurs possèdent, en plus de leur identifiant Unix (uidNumber) et de leur identifiant de groupe principal (gidNumber), les équivalents Microsoft, appelés sambaSID et sambaPrimaryGroupSID.

Lors de l'intégration d'une station au domaine (à partir de Windows 2000), un compte de station est créé avec des identifiants uniques.

Toutes ces informations sont stockées dans l'annuaire LDAP[p.766] du module.

Calcul du SID pour les groupes

- gidNumber : gid numérique Unix traditionnel

10001 pour le groupe professeurs

- sambaSID : SID suivi d'une valeur obtenue par le calcul suivant : `2 x gidNumber + 1001`

S-1-5-21-nnn-nnn-nnn-21003 pour le groupe professeur

Calcul du SID pour les utilisateurs et les comptes de stations

- uidNumber : UID numérique Unix traditionnel

11327 pour l'utilisateur test

- sambaSID : SID suivi d'une valeur obtenue par le calcul suivant : `2 x uidNumber + 1000`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



S-1-5-21-nnn-nnn-nnn-23654 pour l'utilisateur test

- sambaPrimaryGroupSID : sambaSID du groupe principal de l'utilisateur



S-1-5-21-nnn-nnn-nnn-21005 pour un élève

S-1-5-21-nnn-nnn-nnn-515 pour une station (groupe spécial *domainComputers*)

Quelques commandes

- Obtenir le SID du serveur

```
# net getlocalsid
SID for domain SCRIBE is: S-1-5-21-1282421234-3914496513-4208907870
```

- Vérifier la valeur du SID stocké dans l'annuaire LDAP

```
# ldapsearch -x sambaDomainName=* | grep sambaSID
sambaSID: S-1-5-21-1282421234-3914496513-4208907870
```

- Valider le SID (enregistrement samba)

```
# net rpc getsid
Storing SID S-1-5-21-1282421234-3914496513-4208907870 for Domain DOMACA in
secrets.tdb
```

- Forcer la valeur du SID (restauration du SID de l'ancien serveur)

```
# net setlocalsid S-1-5-21-nnn-nnn-nnn
```


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.783] 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` :

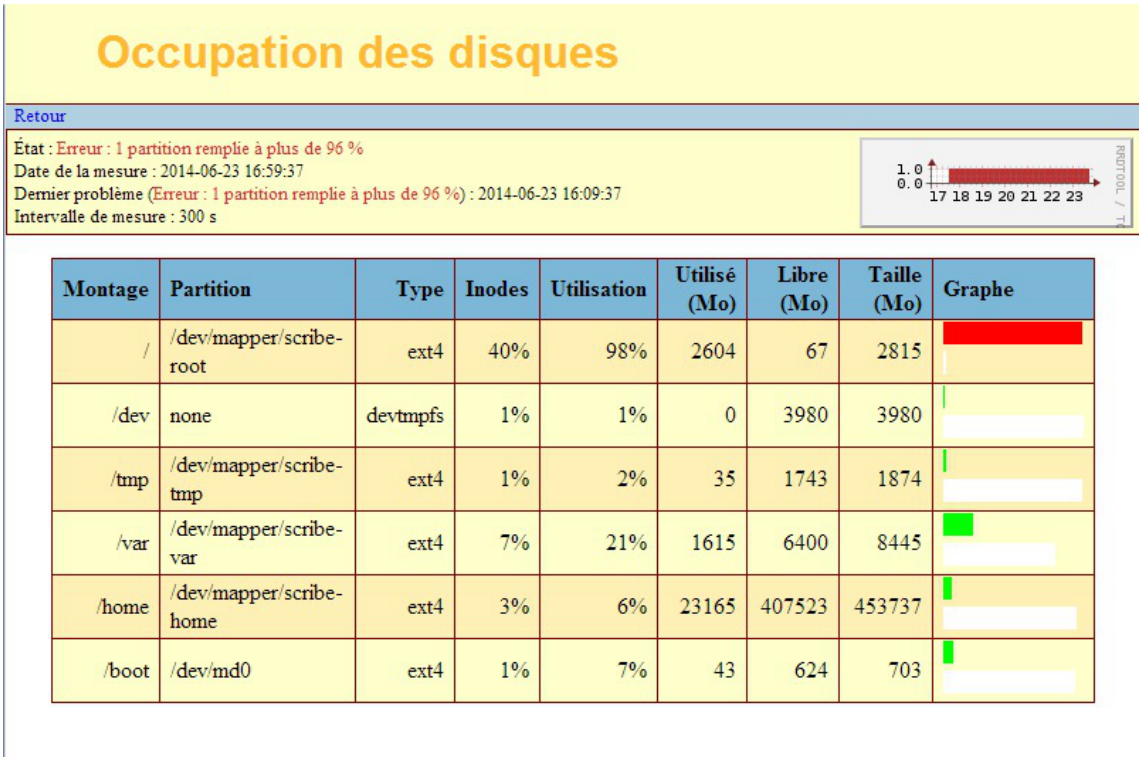
```
# mount /var/home
```



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

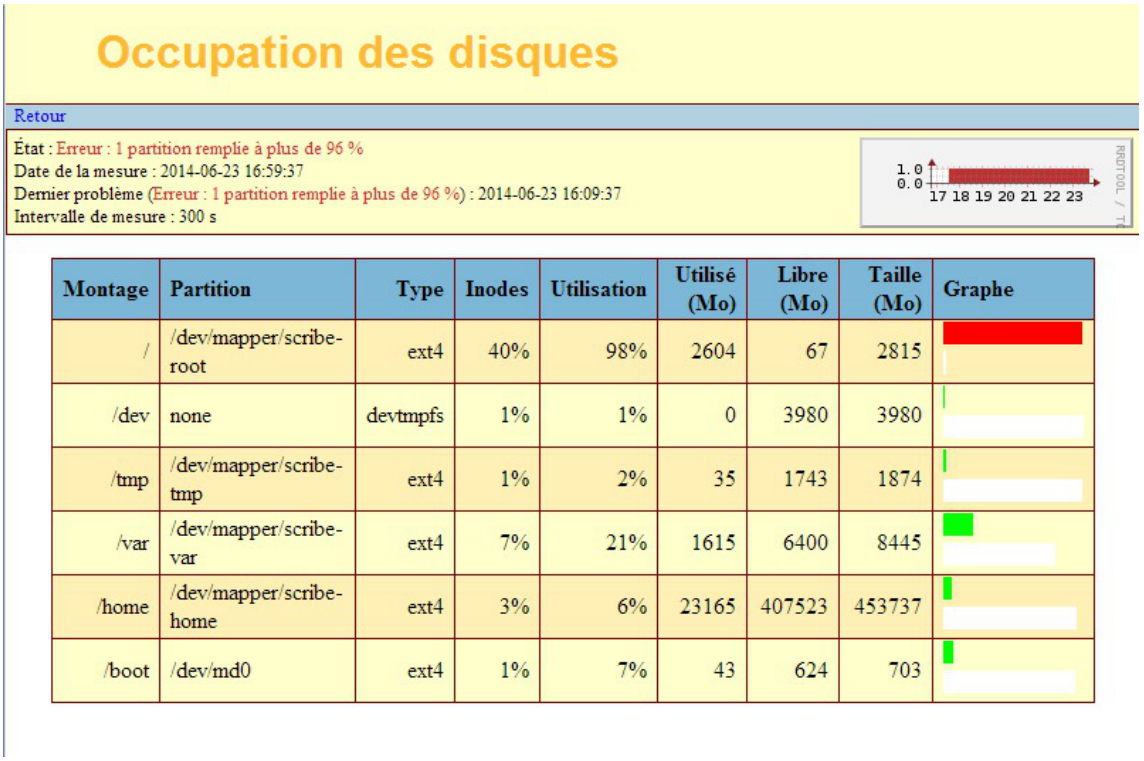
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	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

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. 768]).

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. 768]).

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.

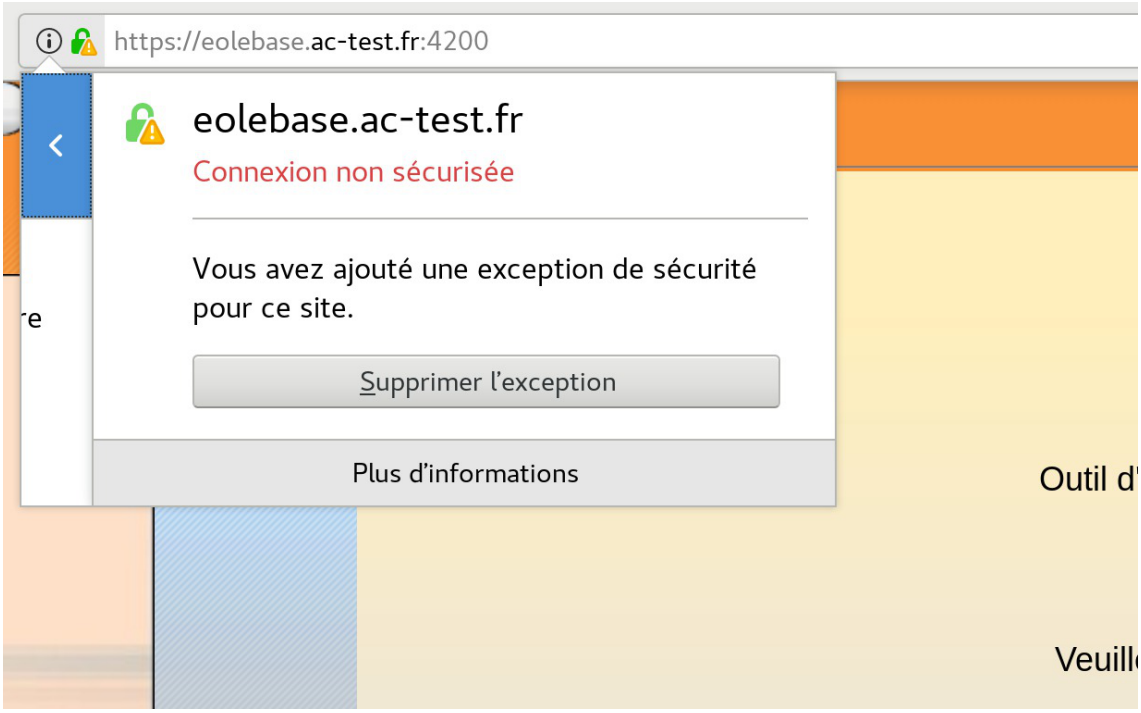
Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

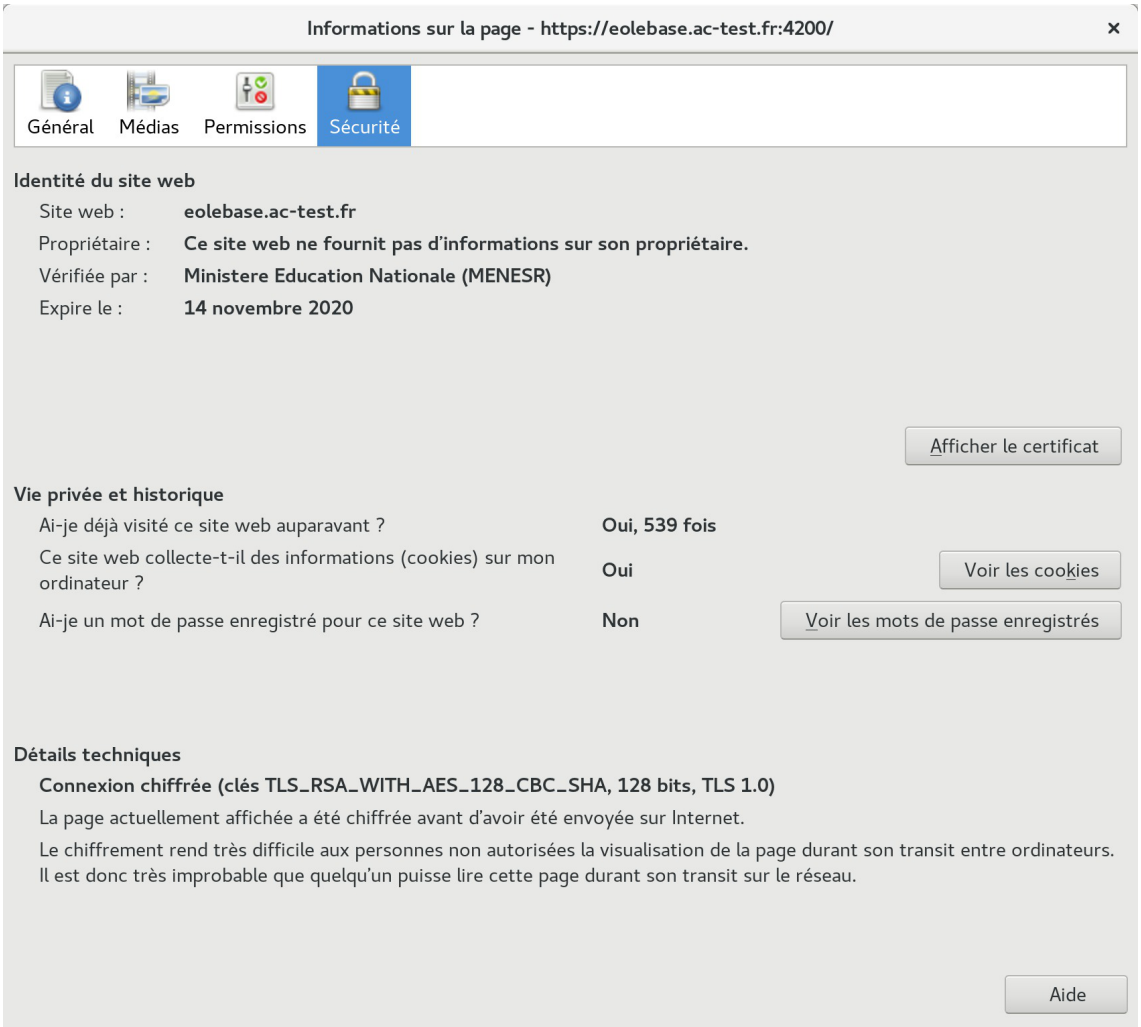


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



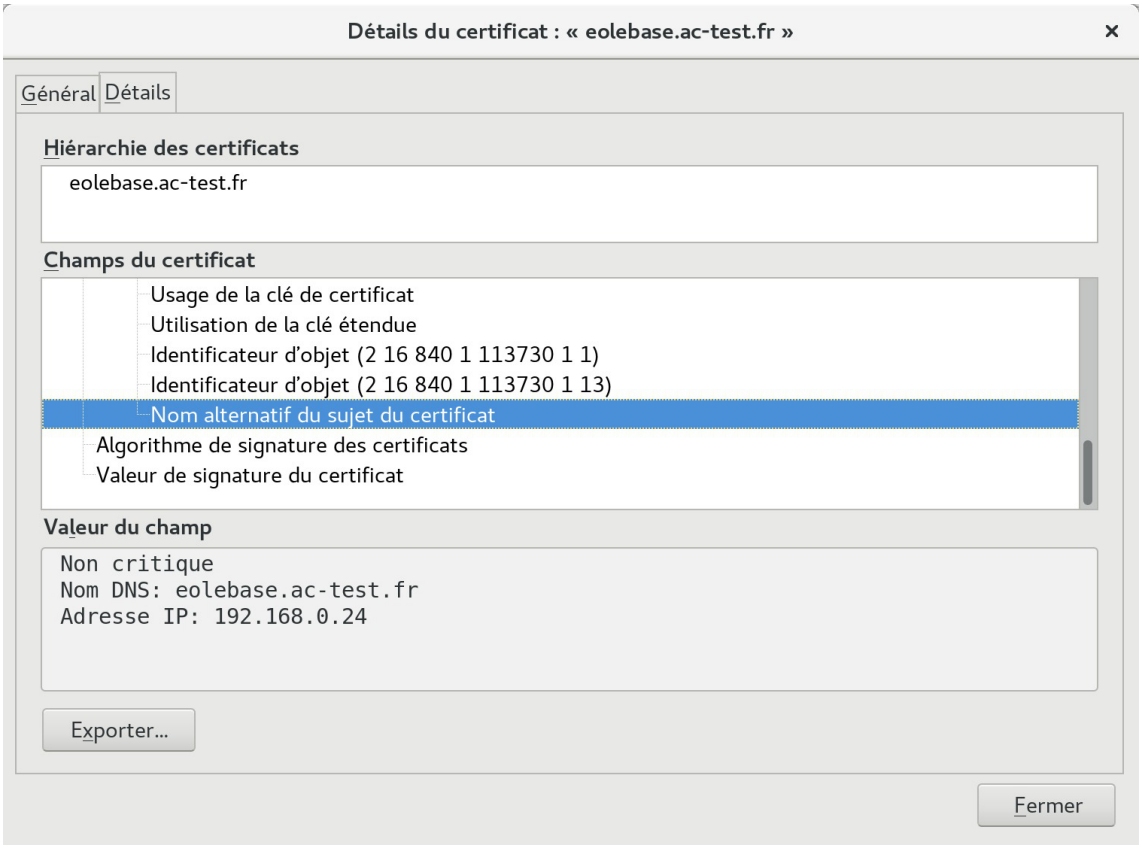
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- 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.781] 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.764].



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 Horus

Modifier le mot de passe d'un utilisateur en ligne de commande

Le mot de passe d'un utilisateur LDAP peut être modifié en ligne de commande avec la commande `smbldap-passwd`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



```
# smbldap-passwd <user>
Changing UNIX and samba passwords for <user>
New password:
Retype new password:
#
```

Session Windows, configuration non appliquée et messages d'erreurs

L'utilisateur ouvre une session, la configuration ESU n'est pas appliquée et l'utilisateur obtient des erreurs.



Après un démarrage du poste, lorsque Windows 10 affiche l'invite d'ouverture de session, il est possible que le service Scribe n'ait pas fini de démarrer.

Avant de démarrer une session il faut bien attendre que Windows 10 ait fini de démarrer.

Il est possible de démarrer les stations à l'avance le matin (comme pour WPKG) avec WOL[p. 783] avec par exemple le logiciel ecoStations.

Session Windows, erreur : Aucun serveur d'accès n'est actuellement disponible...

Les utilisateurs ne peuvent pas se connecter sur un poste Windows 10 intégré au domaine et le message d'erreur `Aucun serveur d'accès n'est actuellement disponible pour traiter la demande d'ouverture de session s'affiche`.



La station Windows 10 a été intégrée manuellement sans exécuter les commandes, utilisez le script `Win10.bat` en tant qu'Administrateur à l'aide d'un clic droit sur `Win10.bat` → Exécuter en tant qu'Administrateur.

Session Windows, erreur : Une tentative d'ouverture de session a eu lieu...

Lors de la tentative d'ouverture de session d'une machine équipée de Windows 10, raccordée au domaine, le message suivant s'affiche :

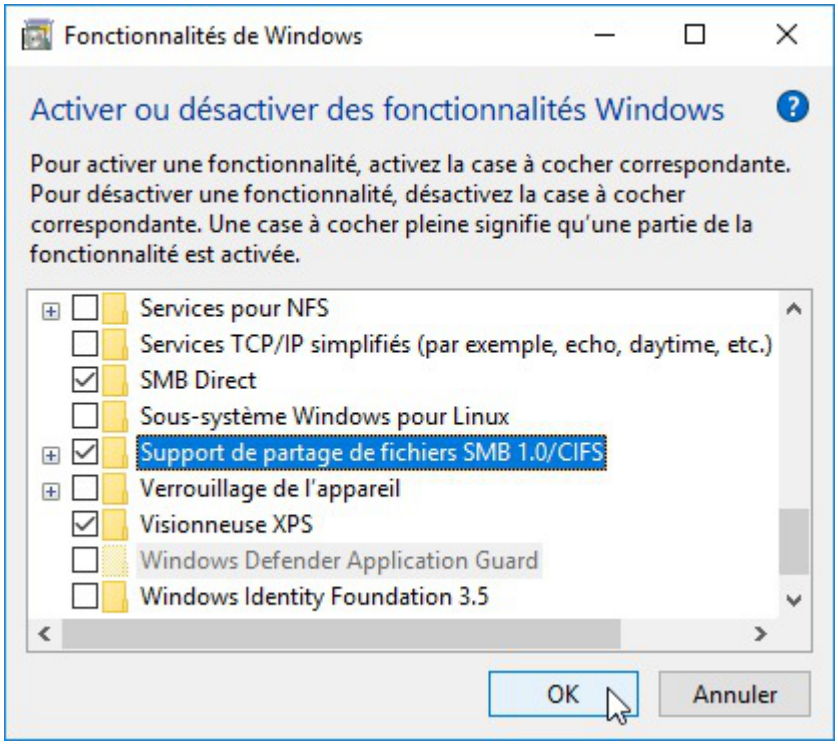
`Une tentative d'ouverture de session a eu lieu alors que le service d'ouverture de session réseau n'avait pas démarré.`

La version de Windows est supérieure ou égale à Windows 10 1709.



Il faut activer le support le `Support de partage de fichiers SMB 1.0/CIFS` dans la gestion des fonctionnalités de Windows.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

Comment effectuer un changement de nom de domaine académique

Le changement du nom de domaine académique entraîne un dysfonctionnement de l'annuaire LDAP car la construction de l'annuaire utilise cette valeur et n'a lieu qu'une fois au moment de l'instance.

Pour connaître le nom de domaine utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep -E 'dn: ou=[^,]+,ou=education'
```

Le nom utilisé ici est `ac-test` :

```
dn: ou=ac-test,ou=education,o=gouv,c=fr
```

Le nom de domaine `Nom de domaine académique` se change dans l'interface de configuration du module dans l'onglet `Général`.

Le suffixe peut être changé dans le même onglet à la ligne `Suffixe du nom de domaine académique`.

Pour connaître la valeur de ces variables en ligne de commande :

```
# CreoleGet nom_academie
ac-test
# CreoleGet suffixe_domaine_academique
fr
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La solution consiste à extraire l'annuaire, à faire la modification souhaitée dans tous le `.ldif`, puis à injecter l'annuaire modifié.

Extraire l'annuaire :

Arrêt du service

```
# service slapd stop
```

Extraction vers `~root/full-ldap-old.ldif` :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > ~root/full-ldap-old.ldif
```

Remplacer toutes les occurrences de **ou=ac-test** par **ou=ac-dijon** et toutes les occurrences de **ou : ac-test** par **ou : ac-dijon** avec la commande :

```
# sed -e 's/ou=ac-test,/ou=ac-dijon,/g' -e 's/ou: ac-test,/ou=ac-dijon,/g' ~root/full-ldap-old.ldif > ~root/full-ldap-fixed.ldif
```

Vérifier l'absence (hors messagerie -i) de la chaîne **ac-test** dans le nouveau fichier :

```
# grep 'ac-test' ~root/full-ldap-fixed.ldif
```

Injection du nouvel annuaire avec les commandes suivantes :

- Supprimer les anciens fichiers d'annuaire, sauf le fichier `/var/lib/ldap/DB_CONFIG`

  ```
  # rm -f /var/lib/ldap/[^D]*
  ```

- Injecter l'annuaire corrigé

  ```
  # slapadd -f /etc/ldap/slapd.conf -l ~root/full-ldap-fixed.ldif
   -######### 47.59% eta 04s elapsed 03s spd 307.1 k/s
  Closing DB...
  ```

- Corriger le propriétaire des fichiers de la base de données

  ```
  # chown -R openldap: /var/lib/ldap/
  ```

- Redémarrer l'annuaire

  ```
  # service slapd start
  ```

Vérifier le bon fonctionnement du service avec la commande `diagnose`.

Comment effectuer un changement de nom de domaine de messagerie

Le nom de domaine de la messagerie pour les listes de discussions avant changement :

```
# ll $(CreoleGet container_path_mail)/var/lib/sympa/expl/
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
total 12 drwxrwx--x 3 sympa sympa 4096 janv. 28 01:26 ./ drwxrwx--x 8 sympa sympa 4096 janv. 15 20:11 ../
drwxr-xr-x 53 sympa sympa 4096 févr. 2 01:57 i-etb1.ac-test.fr/
```

La valeur du nom de domaine de la messagerie est ici `etb1.ac-test.fr` :

```
root@scribe:~# CreoleGet domaine_messagerie_etab
etb1.ac-test.fr
```



Pour changer le nom de domaine de la messagerie il est possible d'utiliser le script `/usr/share/eole/backend/migre-domaine-messagerie.sh` :

```
# /usr/share/eole/backend/migre-domaine-messagerie.sh etb1.ac-test.fr etb1.ac-dijon.fr
Migrer de etb1.ac-test.fr vers etb1.ac-dijon.fr [oui/non] [non] : oui
# Sauvegarde de l'annuaire dans /root/annuaire-20160202.ldif...
Stop System V service slapd [ OK ]
# Modification de l'annuaire...
"#################### 100.00% eta none elapsed 06s spd 326.7 k/s
Closing DB...
Start System V service slapd [ OK ]
# Migration des configurations sympa...
# Migration des alias Exim4...
Migration terminée : modifiez la variable "Nom de domaine de la messagerie"
puis lancez la commande *reconfigure*
```



Comme indiqué il faut changer le `Nom de domaine de la messagerie` dans l'onglet `Messagerie` de l'interface de configuration du module.

Il est également possible de le faire en ligne de commande avec `CreoleSet` :

```
# CreoleSet domaine_messagerie_etab etb1.ac-dijon.fr
```

Pour vérifier la valeur de la variable :

```
# CreoleGet domaine_messagerie_etab
etb1.ac-dijon.fr
```



Le changement du nom de domaine de la messagerie nécessite une reconfiguration du serveur avec la commande `reconfigure` .

Le nom de domaine de la messagerie pour les listes de discussions est devenu `i-etb1.ac-dijon.fr` :

```
# ll $(CreoleGet container_path_mail)/var/lib/sympa/expl/
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
total 12 drwxrwx--x 3 sympa sympa 4096 févr. 2 15:49 ./ drwxrwx--x 8 sympa sympa 4096 janv. 15 20:11 ../ drwxr-xr-x 53 sympa sympa 4096 févr. 2 01:57 i-etb1.ac-dijon.fr/
```

Comment effectuer un changement de nom du serveur de fichier

Le changement du nom du contrôleur de domaine et/ou du nom du domaine Samba entraîne un dysfonctionnement de l'annuaire LDAP car la construction de l'annuaire utilise cette valeur et n'a lieu qu'une fois au moment de l'instance.

Pour connaître le nom du domaine Samba utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep "^sambaDomainName"
```

Le nom utilisé ici est `dompedago` :

```
sambaDomainName: dompedago
```

Pour connaître le nom du contrôleur de domaine utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep -m1 'sambaShareURI'
```

Le nom utilisé ici est `scribe` :

```
sambaShareURI: \\scribe\icones$
```

Le nom du contrôleur de domaine et le nom du domaine Samba sont configurés dans l'interface de configuration du module dans l'onglet `Samba`.

Pour connaître la valeur de ces variables en ligne de commande :

```
# CreoleGet smb_netbios_name
scribe
# CreoleGet smb_workgroup
dompedago
```

La solution consiste à extraire l'annuaire, à faire la modification souhaitée dans tous le `.ldif`, puis à injecter l'annuaire modifié.

Extraire l'annuaire après arrêt du service :

Arrêt du service

```
# service slapd stop
```

Extraction vers `~root/full-ldap-old.ldif` :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > ~root/full-ldap-old.ldif
```

Remplacer toutes les occurrences de **scribe** par **nomnetbios** avec la commande :

```
# sed -e 's/\\\\scribe\\/\\\\nomnetbios\\/g'
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
~root/full-ldap-old.ldif > ~root/full-ldap-partiallyprefixed.ldif
#       sed       -e       's/\/\/scribe\//\/\/nomnetbios\//g'
~root/full-ldap-partiallyprefixed.ldif                          >
~root/full-ldap-prefixed.ldif
```

Remplacer toutes les occurrences de **dompedago** par **nomworkgroup** avec la commande :

```
# sed -e 's/=dompedago,/=nomworkgroup,/g' -e 's/sambaDomainName:
dompedago/sambaDomainName:                  nomworkgroup/g'
~root/full-ldap-prefixed.ldif > ~root/full-ldap-fixed.ldif
```

Vérifier l'absence (hors messagerie -i) de la chaîne **ac-test** dans le nouveau fichier :

```
# grep 'scribe' ~root/full-ldap-prefixed.ldif
```

Injection du nouvel annuaire avec les commandes suivantes :

- Supprimer les anciens fichiers d'annuaire, sauf le fichier `/var/lib/ldap/DB_CONFIG`

  ```
  # rm -f /var/lib/ldap/[^D]*
  ```

- Injecter l'annuaire corrigé

  ```
  # slapadd -f /etc/ldap/slapd.conf -l ~root/full-ldap-prefixed.ldif
   -######### 47.59% eta 04s elapsed 03s spd 307.1 k/s
  Closing DB...
  ```

- Corriger le propriétaire des fichiers de la base de données

  ```
  # chown -R openldap: /var/lib/ldap/
  ```

- Redémarrer l'annuaire

  ```
  # service slapd start
  ```

Vider le cache de Samba :

```
# net cache flush
```

Si cela ne suffit pas il faut supprimer les fichiers `/var/lib/samba/wins.dat` et `/var/cache/samba/browse.dat` :

```
# service samba stop
# rm -f /var/lib/samba/wins.dat /var/cache/samba/browse.dat
# service samba start
```

Vérifier le bon fonctionnement du service avec la commande `diagnose`.

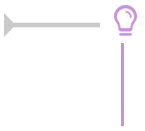
Comment effectuer un changement de l'identifiant de l'établissement (UAI)

L'identifiant de l'établissement est une valeur verrouillée dans l'interface de configuration une fois le

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

serveur instancié.

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` ;
- procéder à une reconfiguration du serveur à l'aide de la commande `reconfigure`.

Le changement de l'identifiant de l'établissement (UAI) entraîne un dysfonctionnement de l'annuaire LDAP car la construction de l'annuaire utilise cette valeur et n'a lieu qu'une fois au moment de l'instance.

Pour connaître l'identifiant utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep "cn=edu"
```

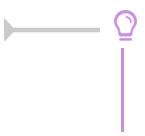
L'UAI utilisé ici est `0000000A` :

```
dn: cn=edu,ou=local,ou=groupes,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
```

L'UAI est configuré dans l'interface de configuration du module dans l'onglet `Général`.

Pour connaître la valeur de cette variable en ligne de commande :

```
# CreoleGet numero_etab
0000000A
```



La solution consiste à extraire l'annuaire, à faire la modification souhaitée dans tous le `.ldif`, puis à injecter l'annuaire modifié.



Extraire l'annuaire après arrêt du service :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Arrêt du service

```
# service slapd stop
```

Extraction vers `~root/full-ldap-old.ldif` :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > ~root/full-ldap-old.ldif
```



Remplacer toutes les occurrences de **0000000A** par **0000000B** avec la commande :

```
# sed -e 's/ou=0000000A/ou=0000000B/g' -e 's/ou: 0000000A/ou: 0000000B/g' ~root/full-ldap-old.ldif > ~root/full-ldap-prefixed.ldif
```



Vérifier l'absence de la chaîne **0000000A** dans le nouveau fichier :

```
# grep '0000000A' ~root/full-ldap-prefixed.ldif
```

Injection du nouvel annuaire avec les commandes suivantes :

- Supprimer les anciens fichiers d'annuaire, sauf le fichier `/var/lib/ldap/DB_CONFIG`

  ```
  # rm -f /var/lib/ldap/[^D]*
  ```

- Injecter l'annuaire corrigé

  ```
  # slapadd -f /etc/ldap/slapd.conf -l ~root/full-ldap-prefixed.ldif
   -######### 47.59% eta 04s elapsed 03s spd 307.1 k/s
  Closing DB...
  ```

- Corriger le propriétaire des fichiers de la base de données

  ```
  # chown -R openldap: /var/lib/ldap/
  ```

- Redémarrer l'annuaire

  ```
  # service slapd start
  ```

Procéder à la reconfiguration du serveur pour la prise en compte du changement de la valeur de l'identifiant dans l'interface de configuration du module.



Vérifier le bon fonctionnement du service avec la commande `diagnose`.

Impossible de trouver ClientScribe & ClientHorus

La commande `apt-eole install client-scribe` renvoie le message "le paquet n'existe pas".



ClientScribe & ClientHorus étaient une expérimentation de client lourd pour GNU Linux sur la version EOLE 2.2 mais qu'elle n'a pas été poursuivie.

Les paquets `client-scribe` et `client-horus` n'existent plus.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Erreur MySQL : Access denied for user 'debian-sys-maint'@'localhost'

Suite à une restauration ou à une migration il est possible de rencontrer l'erreur suivante :

`ERROR 1045 (28000): Access denied for user 'debian-sys-maint'@'localhost' (using password: YES)`

Il faut remettre à jour le mot de passe de l'utilisateur MySQL "debian-sys-maint"

En mode non conteneur il faut :

- récupérer le nouveau mot de passe MySQL :

  `# grep password /etc/mysql/debian.cnf`

- Sur une première console, lancer MySQL en mode safe :

  `# mysqld_safe --skip-grant-tables`

- Sur une seconde console, se connecter à la base :

  `# mysql -u root mysql`

- mettre à jour le mot de passe :

  `UPDATE user SET authentication_string=PASSWORD('MOT_DE_PASSE_RECUPERE_AVEC_GREP') WHERE User='debian-sys-maint' ;`

  `FLUSH PRIVILEGES ;`

- quitter la console :

  `\quit` ou Ctrl + d

- relancer MySQL :

  `# killall mysqld`

  attendre quelques secondes

  `# service mysql start`

En mode conteneur il faut :

- se connecter au conteneur bdd :

  `# ssh bdd`

- récupérer le nouveau mot de passe MySQL :

  `# grep password /etc/mysql/debian.cnf`

- se connecter à la console MySQL :

  `# mysqld_safe --skip-grant-tables & mysql -u root mysql`

- mettre à jour le mot de passe :

  `UPDATE user SET authentication_string=PASSWORD('MOT_DE_PASSE_RECUPERE_AVEC_GREP') WHERE User='debian-sys-maint' ;`

  `FLUSH PRIVILEGES ;`

- quitter la console :

  `\quit` ou Ctrl + d

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- relancer MySQL :
  `# killall mysqld`
  attendre quelques secondes
  `# service mysql start`
- quitter le conteneur :
  `# exit` ou Ctrl + d

Erreur MySQL : Too many connections

Le nombre de connexions clientes maximum simultanées à la base de données MySQL est atteint.

Augmenter le paramètre mysql_max_connexions

Dans l'interface de configuration du module, en mode expert, aller dans l'onglet `Mysql` et adapter le `Nombre maximum de connexions simultanées` aux usages constatés.

Lancer la commande `reconfigure` pour appliquer le nouveau réglage.

3. Questions fréquentes propres à la sauvegarde

La sauvegarde programmée est en échec

Relancer les services

Il faut en premier lieu enlever le verrou :

```
# bareosconfig.py --unlock
```

Si tout n'est pas passé au vert dans l'EAD, il faut relancer les services :

```
# service bareos-dir stop
# service bareos-sd stop
# service bareos-fd stop
# service bareos-dir start
# service bareos-sd start
# service bareos-fd start
```

Modification de la configuration de Bareos non prise en compte

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.

Afin de prendre en compte la nouvelle valeur, il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et ré-initialiser la base de données Bareos.

Ré-initialisation de la base Bareos

```
# bareosregen.sh
Le catalogue Bareos a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non]
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
[non] : oui
```

Réinitialisation de la sauvegarde

Pour réinitialiser la sauvegarde il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et surtout il faut ré-initialiser la base de données de Bareos.

Ré-initialisation de la base Bareos

```
# bareosregen.sh
Le catalogue Bareos a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non]
[non] : oui
```

Supprimer le verrou de sauvegarde

Il faut utiliser la commande suivante :

```
# bareosconfig.py --unlock
```

Paramètres de la commande bareosconfig.py

Pour afficher la liste des paramètres de la commande `bareosconfig.py` :

```
# bareosconfig.py --help
```

Problème de droit sur le point de montage des sauvegardes

Il peut survenir un problème de droit sur le point de montage des sauvegardes dans les cas où la configuration du support choisie est `Configuration manuelle du support` ou sur `Disque USB local`.

```
# bareosmount.py --mount
Échec du montage : point de montage : OK
montage : OK
permissions : Erreur
```

Appliquer les bons droits sur le point de montage

Tester la configuration du support et rendre l'utilisateur *bareos* et le groupe *tape* propriétaires du point de montage

```
# bareosmount.py -t -o
 Test OK
```

Monter le support

```
# bareosmount.py --mount
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
Montage OK
```

Démontage du support

```
# bareosmount.py --umount
Démontage OK
```

Comment restaurer avec l'outil bconsole

Comment restaurer avec `bconsole`, dans le cas où la sauvegarde complète s'effectue le week-end puis des incrémentales en semaine ?

Pour faire une restauration partielle, il n'est pas nécessaire de passer par la restauration complète.

bconsole reconstruit l'arborescence et prend les fichiers dans le jeux de sauvegarde adéquat.

Arrêter une sauvegarde en cours

Dans certains cas (saturation du support de sauvegarde,...), il peut arriver qu'une sauvegarde reste bloquée.

Dans ce cas, il faut utiliser l'instruction `cancel` de la console Bareos : `bconsole`.

Voici un aperçu des manipulations à réaliser :

```
# bconsole
(pour lancer la console de bareos)
*status dir
(pour voir les jobs en cours)
JobId Level Name Status
======================================================================
23 Full Complet.2010-09-03 23.00.00 02 is waiting for a mount request
24 Full BackupCatalog.2010-09-03 23.00.00 03 is waiting execution
*cancel JobId=23
(pour annuler le job en question)
*quit
```

Tester le support de sauvegarde

Pour tester le support de sauvegarde USB local ou SMB, il est possible d'utiliser le script `bareosmount.py`.

```
1 root@scribe:~# bareosmount.py -t
2 Test de montage OK
3 root@scribe:~#
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
root@scribe:~# bareosmount.py -t
Problème de montage (1 essais restants)
ERREUR : périphérique /dev/sda1 non reconnu
Problème de montage (0 essais restants)
ERREUR : périphérique /dev/sda1 non reconnu
Échec du test de montage :
point de montage : Erreur
permissions : Erreur
montage : Erreur
root@scribe:~#
```

```
root@scribe:~# bareosmount.py -t
Problème de montage (1 essais restants)
[Errno 32] mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

Problème de montage (0 essais restants)
[Errno 32] mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

Échec du test de montage :
point de montage : Erreur
permissions : Erreur
montage : Erreur
root@scribe:~#
```

Options de montage du support de sauvegarde

Le fichier `/etc/eole/bareos.conf` permet de personnaliser les options de montage du support de stockage de la sauvegarde. L'intérêt est que ce fichier ne sera pas écrasé lors de la prochaine mise à jour.

Le fichier `/etc/eole/bareos.conf` a une syntaxe du type fichier INI[p.765] : clé = valeur.

Il existe trois variables paramétrables `DISTANT_LOGIN_MOUNT`, `DISTANT_MOUNT` et `USB_MOUNT` :

- la ligne de commande permettant de monter un support distant avec authentification, la valeur par défaut de `DISTANT_LOGIN_MOUNT` est :

  `/bin/mount -t cifs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev //{4}/{5} {6}`

- la ligne de commande permettant de monter un support distant sans authentification, la valeur par défaut de `DISTANT_MOUNT` est :

  `/bin/mount -t cifs -o password={0},ip={1},uid={2},noexec,nosuid,nodev //{3}/{4} {5}`

- la ligne de commande permettant de monter un support USB :

  Par défaut la valeur de la variable USB_MOUNT est :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `/bin/mount {0} {1} -o noexec,nosuid,nodev,uid={2},umask=0077` pour les systèmes VFAT et NTFS
- `/bin/mount {0} {1} -o noexec,nosuid,nodev` pour le reste.



L'EAD et la commande `bareosmount.py -t` retourne des erreurs.

Le montage à la main donne des erreurs :

```
# mount -t cifs //<adresseServeur>/sauvhorus /mnt/sauvegardes/ -ousername=sauvegarde,password=***
mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
# mount -t smbfs //<adresseServeur>/sauvhorus /mnt/sauvegardes/ -ousername=sauvegarde,password=***
mount error(13): Permission denied
Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
```

Il faut ajouter le paramètre `sec=ntlm` aux commandes :

```
# mount -t cifs //<adresseServeur>/sauvhorus /mnt/sauvegardes/ -ousername=sauvegarde,password=***,sec=ntlm
# mount -t smbfs //<adresseServeur>/sauvhorus /mnt/sauvegardes/ -ousername=sauvegarde,password=***,sec=ntlm
```

Il faut créé le fichier `/etc/eole/bareos.conf` et mettre le contenu suivant :

```
DISTANT_LOGIN_MOUNT='/bin/mount -t cifs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev,sec=nt
//{4}/{5} {6}'
```

Impossible de changer le type de base de données du catalogue

Suite à la migration du module vers 2.5 le type de base de données est SQLite et il est impossible de le changer pour profiter du logiciel web bareos-webui.



Réimporter le fichier config.eol

Pour obtenir la possibilité de changer la valeur du type de base de données, il faut, dans l'interface de configuration du module, exporter puis importer le fichier `config.eol`, changer la valeur à à MySQL, enregistrer et ensuite régénérer le catalogue.

Pour réinitialiser la sauvegarde il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et surtout il faut ré-initialiser la base de données de Bareos.



Ré-initialisation de la base Bareos

```
# bareosregen.sh
Le catalogue Bareos a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non]
[non] : oui
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La contrepartie est de perdre toutes les sauvegardes enregistrées dans l'ancien type de base de données.

Le service bareos-dir ne démarre plus

Suite à une migration le type de base de données du catalogue s'est positionné sur SQLite par défaut.

Les erreurs affichées dans les journaux montrent des requêtes infructueuses :

```
Oct  7 13:17:16 srv-scribe bareos-dir: bareos-dir JobId 0: Fatal error: Query failed: SELECT VersionId FROM Version: ERR=no such table: Version
Oct  7 13:17:16 srv-scribe bareos-dir: bareos-dir JobId 0: Fatal error: Impossible d'ouvrir le catalogue « MyCatalog », sur la base de données « bareos ».
Oct  7 13:17:16 srv-scribe bareos-dir: bareos-dir JobId 0: Fatal error: Query failed: SELECT VersionId FROM Version: ERR=no such table: Version
Oct  7 13:17:16 srv-scribe bareos-dir: bareos-dir ERROR TERMINATION#012Merci de corriger le fichier de configuration : /etc/bareos/bareos-dir.conf
```

Après vérification la base de données est vide :

```
# echo .dump | sqlite3 /var/lib/bareos/bareos.db
[...]
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
COMMIT
[...]
```

Procéder à la restauration du catalogue

Il faut restaurer le catalogue à l'aide de la commande `bareosrestore.py --catalog <nomCatalogue>`.

```
root@scribe:~# bareosrestore.py --catalog scribe-dir
Restauration du catalogue
Le fichier config.eol a été restauré avec le nom /root/zephir-restore.eol
Pour que ce fichier soit pris en compte, il faut le déplacer : mv /root/zephir-restore.eol /etc/eole/config.eol

## Régénération du catalogue Bareos##
Stop System V service bareos-dir
[  OK  ]
Stop System V service areos-sd
[  OK  ]
Dropping sqlite3 database
Drop of bareos database succeeded.
Creating sqlite3 database
Creating of bareos database succeeded.
Régénération du catalogue terminée
Suppression des anciens rapports d'état
Start System V service bareos-dir
[  OK  ]
Start System V service bareos-sd
[  OK  ]
root@scribe:~#
```

Utiliser un label pour identifier le périphérique de sauvegarde

Lorsque une clé USB est connectée en même temps que le périphérique de sauvegarde le numéro du

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

périphérique dans `/dev` change. Le numéro du périphérique n'est pas fiable.



Une astuce consiste à utiliser un label pour identifier de façon plus certaine le périphérique utilisé.

Pour donner un label au périphérique :

```
# tune2fs -L Sauvegardes /dev/sdX
```

Pour configurer le support de sauvegarde sur le périphérique USB :

```
# bareosconfig.py -s usb --usb_path=/dev/disk/by-label/Sauvegardes
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Glossaire

.REG *= abréviation de registry*	Un fichier portant l'extension .REG est un fichier contenant des instructions permettant d'apporter des modifications locales à la base de registre.
AAF *= Annuaire Académique Fédérateur*	L'annuaire fédérateur est un dispositif technique qui sert à alimenter l'annuaire LDAP d'un rectorat avec les autres annuaires académiques qui existent au sein de l'Éducation nationale et qui sont directement utilisés par les applications du ministère et des collectivités.
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 Zéphir	Les agents Zéphir sont des sondes qui génèrent divers statistiques et rapports sur les modules EOLE. Sur un module, elles sont consultables en HTTP sur le port 8090. Elles sont également accessibles via la page d'accueil de l'interface d'administration EAD. Si le module est enregistré sur un serveur Zéphir, ces données sont remontées à intervalles réguliers et sont susceptibles de générer des alertes centralisées dans l'interface web Zéphir.
	L'agrégation de liens (niveau 2) est une technique utilisée dans les

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Agrégation de liens Ethernet *= Bonding*	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.
ARENA *= Accès aux Ressources de l'Éducation Nationale et Académiques*	Les portails d'applications ARENA vous donnent accès aux applications en ligne du ministère de l'Éducation nationale et de l'Académie.
Autorité de Certification *= CA : Certification Authority*	AC est l'acronyme de Autorité de Certification. Une autorité de certification est une société ou un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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/
CAS *= Central Authentication Service*	CAS est un système d'authentification unique créé par l'université de Yale : on s'authentifie sur un site Web, et on est alors authentifié sur tous les sites Web qui utilisent le même serveur CAS. Il évite de s'authentifier à chaque fois qu'on accède à une application en mettant en place un système de ticket.
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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	• détecter les vulnérabilités des systèmes, au travers notamment d'une veille technologique ; • piloter la résolution des incidents, si besoin avec le réseau mondial des CERT ; • aider à la mise en place de moyens permettant de se prémunir contre de futurs incidents ; • organiser la mise en place d'un réseau de confiance. Source : https://www.cert.ssi.gouv.fr/
CETIAD *= Centre d'Études et de Traitements Informatiques de l'Académie de Dijon*	DSI de l'académie de Dijon en charge l'informatisation des services académiques et des établissements des 1er et 2nd degré nommée ainsi jusqu'au déménagement du service de la rue Berbisey à la rue du Général Delaborde dans les nouveaux locaux du rectorat de l'académie de Dijon en novembre 2012.
Classe de caractères	Une classe de caractères définit un ensemble de caractères ayant un sens commun : • caractères alphabétiques ; • caractères non-alphabétiques ; • les caractères numériques ; • les caractères alphanumériques ; • les caractères grecs.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	nommage des cartes réseau sous GNU / Linux. Cette convention a été implémentée au travers du module kernel biosdevname par la société Dell. Le schéma de nommage de biosdevname respecte les conventions suivantes : • em[1−N] pour les cartes physiques embarquées, le numéro correspond à l'emplacement interne de la carte sur la carte mère (numéro renvoyé par la commande `lspci`) ; • p<numeroEmplacement>p<numeroEmplacementPhysique> pour les cartes PCI, le numéro de l'emplacement physique commençant à 1 ; • un suffixe _vf est ajouté au matériel NPAR et SR-IOV, le numéro dépend du nombre de partitions ou des fonctions de virtualisation utilisées et sur quel port ; • d'autres conventions comme les suffixes vlan et alias sont inchangées et reste applicables. Source : http://en.wikipedia.org/wiki/Consistent_Network_Device_Naming systemd/udev utilisent leur propre schéma de nommage similaire à biosdevname. Les principales différences sont supportées nativement par udev : • carte embarquée et numéro interne de l'emplacement de la carte (numéro renvoyé par la commande `lspci`) (exemple: eno1) ; • carte PCI Express et numéro interne de l'emplacement de la carte (exemple: ens1) ; • carte et localisation du connecteur au niveau du matériel (exemple: enp2s0) ; • carte avec l'adresse MAC (exemple: enx78e7d1ea46da) ; • pour les cartes nommées nativement dans le kernel (exemple: eth0).
Conteneur	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
Contrôleur de domaine NT	Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire. Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	hiérarchique dans une entreprise. Par exemple, le domaine "ADMINISTRATIF" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service administratif, et les comptes utilisateur qui sont autorisés à s'y connecter. Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données. Cette base de données est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003), appelés Contrôleurs de Domaine.
Corosync Cluster Engine *= Corosync*	Corosync Cluster Engine est un moteur libre de cluster. C'est un système de communication avec des fonctionnalités supplémentaires pour la mise en œuvre de la haute disponibilité dans les applications. Le projet fournit quatre fonctionnalités principales : • un groupe restreint de processus avec une garantie de synchronisation virtuelle afin de créer des machines à états répliquées ; • un simple gestionnaire de disponibilité qui redémarre les processus d'application lorsqu'ils ont échoués ; • une configuration et des statistiques stockées en base de données dans la mémoire vive permet de définir, de récupérer et de recevoir des notifications concernant les changements d'état ; • un système de notification qui se déclenche lorsque un quorum est atteint ou perdu. Sources : https://fr.wikipedia.org/wiki/Corosync_Cluster_Engine et http://clusterlabs.org/
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.
CreoleService	`CreoleService` est un nouvel outil qui vient remplacer avantageusement la fonction *Service()* de `FonctionsEoleNg`. Pour l'utiliser : `CreoleService apache2 reload` S'il existe le même service dans plusieurs conteneurs il est possible de spécifier le conteneur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Exemple : `CreoleService -c fichier smbd restart`
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.
CUPS *= Common Unix Printing System*	CUPS est un système modulaire d'impression informatique qui permet à l'ordinateur sur lequel il est installé de fonctionner en tant que serveur d'impression. Un serveur d'impression est capable d'accepter des tâches d'impression d'autres ordinateurs (les clients) et de les répartir sur les imprimantes qui sont paramétrées. CUPS met à disposition une interface de gestion accessible avec un navigateur web.
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 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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	(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). 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`.
EPLE *= Établissement Public Local d'Enseignement*	En France, un établissement public local d'enseignement (EPLE) est un établissement scolaire d'enseignement secondaire (ou, exceptionnellement, primaire) : • collège • lycée d'enseignement général et technologique (LGT) • lycée professionnel (LP) • établissement régional d'enseignement adapté (EREA)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	• école régionale du premier degré (ERPD)
ERA *= Éditeur de Règles pour le module Amon*	ERA est une application graphique de génération et de gestion de règles de sécurité adaptée au module pare-feu Amon. À partir du fichier XML de description du pare-feu, un script de règles iptables pour Netfilter est généré de manière à implémenter ces règles sur le module pare-feu Amon. La génération directe de règles iptables est également possible, permettant d'utiliser ERA pour d'autres types de serveurs sous GNU/Linux.
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
ESU *= Environnements Sécurisés des Utilisateurs*	Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques. ESU propose de nombreuses fonctions : • limitation des accès aux paramètres de Windows (panneau de configuration...) ; • définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ; • configuration des imprimantes partagées sur les postes ; • configuration des navigateurs (Internet Explorer et Mozilla Firefox) ; • éditeur de règles permettant de rajouter autant de règles que vous le souhaitez.
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/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.
Fichiers métadata	Les fichier métadata sont des fichiers au format XML contenant les informations nécessaires à la définition des entités partenaires en vue d'échange de message SAML. Ces fichiers contiennent la plupart du temps : • le nom de l'entité ; • les différentes urls sur lesquelles envoyer les différentes requêtes et réponse au format SAML; • la description des certificats utilisés pour signer ses messages; • des informations sur les attributs nécessaires pour identifier les utilisateurs ; • .... La description complète du format de ces fichiers et des éléments possibles est disponible sur le site du consortium OASIS.
Flask	Flask est un framework d'application web léger écrit en Python et basé sur le toolkit Werkzeug (une librairie Python WSGI) et sur le moteur de template Jinja2. Flask est appelé microframework parce qu'il garde un cœur simple, mais extensible. Il n'y a aucune couche d'abstraction de données, pas de formulaire de validation ou tout autre composant que des bibliothèques tierces ne traitent déjà. Cependant, Flask supporte les extensions, ce qui permet d'ajouter des fonctionnalités si elles sont mises en œuvre dans Flask lui-même. Il existe des extensions pour utiliser les objets relationnels, valider des formulaires, le téléchargement, diverses technologies d'authentification ouvertes, et plus encore. Flask est sous licence BSD. http://flask.pocoo.org/
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/
FranceConnect	FranceConnect est un dispositif permettant de garantir l'identité d'un utilisateur en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée. Ce dispositif est un bien commun mis à la disposition de toutes les autorités administratives. Il est mis en œuvre

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	par la DINSIC, dépendante du SGMAP2, un service du premier ministre. Certains acteurs du secteur privé peuvent aussi en bénéficier s'ils contribuent à l'action publique (banques et assurances par exemple). Source : http://fr.wikipedia.org/wiki/FranceConnect
FTP *= File Transfert Protocol*	File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers. La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS. FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande). FTP, qui appartient à la couche application du modèle OSI et du modèle ARPA, utilise une connexion TCP. Par convention, deux ports sont attribués (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990. Ce protocole peut fonctionner avec IPv4 et IPv6. (Source : http://fr.wikipedia.org/wiki/File_Transfer_Protocol)
Gaspacho	Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil. Pour le moment il n'existe que la version GNU/Linux du client 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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
GTK *= The GIMP Toolkit*	GTK est un ensemble de bibliothèques logicielles, c'est-à-dire un ensemble de fonctions permettant de réaliser des interfaces graphiques. Cette bibliothèque a été développée originellement pour les besoins du logiciel de traitement d'images GIMP. GTK est maintenant utilisé dans de nombreux projets, dont les environnements de bureau GNOME, Xfce, Lxde et ROX. Source Wikipédia : http://fr.wikipedia.org/wiki/GTK+
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	inaccessible.
Image ISO *= Image disque*	Une image ISO est une archive proposant la copie conforme d'un disque optique ou magnétique. L'opération de gravure de l'image ISO consiste à recopier cette structure sur un disque optique.
IMAP *= Internet Message Access Protocol*	IMAP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Mais contrairement au protocole POP, il permet de laisser les messages sur le serveur, ce qui présente un gros avantage pour consulter sa messagerie depuis plusieurs postes équipés de clients lourds.
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
instance *= instanciation, instancier*	Instancier un serveur correspond à la troisième étape de mise ne œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande `instance` .
InterBase	InterBase est un moteur de base de données. Il a été choisi par le ministère de l'Éducation nationale pour supporter les bases de données utilisées par les logiciels nationaux (comme GFC et SELENE, par exemple). Source Wikipédia : http://fr.wikipedia.org/wiki/InterBase
iptables	iptables est un logiciel libre grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu dans l'espace noyau composé par des modules Netfilter. Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.
IPv6 *= Internet Protocol version 6*	L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4. Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
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
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)
Keycloak	Keycloak est un outil libre et moderne de gestion d'identité et des accès (IAM).
LDAP	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Lightweight Directory Access Protocol	les systèmes d'annuaires.
LDM *= LTSP Display Manager*	LDM est le gestionnaire d'affichage spécialement écrit pour LTSP.
LemonLDAP *= LemonLDAP::NG*	LemonLDAP::NG est une infrastructure d'authentification unique distribuée (SSO – Single Sign On) avec gestion centralisée des droits. Il se présente sous la forme d'une suite logicielle libre reposant sur le serveur web Apache. Source : http://www.starxpert.fr/lemon-ldap/
Let's Encrypt *= LE*	Let's Encrypt est une autorité de certification qui fournit des certificats gratuits X.509 pour le protocole cryptographique TLS au moyen d'un processus automatisé destiné à se passer du processus complexe actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation des sites internet. Source Wikipédia : https://fr.wikipedia.org/wiki/Let's_Encrypt
libvirt	libvirt est une bibliothèque, une API, un daemon et des outils en logiciel libre de gestion de la virtualisation. Elle est notamment utilisée par KVM, Xen, VMware ESX, QEMU et d'autres solutions de virtualisation. Elle est notamment utilisée par la couche d'orchestration des hyperviseurs. Source : http://fr.wikipedia.org/wiki/Libvirt
Licence CeCILL	Acronyme pour CEa Cnrs Inria Logiciel Libre. C'est une licence libre de droit français compatible avec la licence GNU GPL.
Linux *= Kernel Linux*	Le noyau Linux est un noyau de système d'exploitation de type Unix. Le noyau Linux est un logiciel libre développé initialement par Linus Torvalds. Il a officiellement vu le jour en 1991. Formellement, « Linux » est le nom du seul noyau, mais dans les faits, on appelle souvent « Linux » l'ensemble du système d'exploitation, aussi appelé « GNU/Linux », voire l'ensemble d'une distribution Linux.
LTS *= Long Term Support*	Certaines versions d'Ubuntu sont estampillées LTS. Ces versions, publiées tous les deux ans au mois d'avril, sont soutenues pour une durée prolongée de 60 mois (5 ans). Le label LTS : • la récupération des paquets de Debian se fait de manière plus conservatrice, synchronisée depuis Debian testing plutôt que Debian unstable ; • la stabilisation de la distribution commence tôt dans le cycle de développement en limitant le nombre de nouveautés. L'équipe d'Ubuntu fait une sélection entre les paquets qui doivent être inclus dans une distribution maintenue sur une durée d'au plus

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	qui dispose de ses propres processus et de son propre réseau (isolés du système physique hôte).
man in the middle *= homme du milieu*	L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. Source Wikipédia : http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
MD5 *= Message Digest 5*	L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. Il a été inventé par Ronald Rivest en 1991. Source : https://fr.wikipedia.org/wiki/MD5
MEEM *= Ministère de l'Environnement, de l'Énergie et de la Mer*	Le ministère de l'Environnement, de l'Énergie et de la Mer est l'administration française chargée de préparer et mettre en œuvre la politique du Gouvernement dans les domaines du développement durable, de l'environnement et des technologies vertes, de la transition énergétique et de l'énergie, du climat, de la prévention des risques naturels et technologiques, de la sécurité industrielle, des transports et de leurs infrastructures, de l'équipement et de la mer. Il est dirigé par le ministre de l'Environnement, de l'Énergie et de la Mer, membre du gouvernement français. Né de la fusion, en 2007, du Ministère de l'Environnement et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer il a depuis changé plusieurs fois de nom et de compétences : • Ministère de l'Écologie, du Développement et de l'Aménagement durables (2007-2010) Le ministère de l'Écologie, du Développement et de l'Aménagement durables (MEDAD) naît ainsi de la fusion du Ministère de l'Écologie et du Développement durable et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer. Il intègre également l'énergie, qui relevait alors du ministère de l'économie. • Ministère de l'Écologie, du Développement durable, des Transports et du Logement (2010-2012) Le ministère devient le Ministère de l'Écologie, du Développement durable, des Transports et du Logement (MEDDTL) et perd au passage ses compétences sur l'énergie, exception faite des énergies renouvelables. • Ministère de l'Écologie, du Développement durable et de l'énergie (2012-2016)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Le Ministère de l'Écologie, du Développement durable et de l'énergie (MEDDE) assemble des fonctions historiquement séparées dans différents ministères : l'écologie (ministère de l'écologie et du Développement durable) et l'énergie (auparavant rattachée au ministère de l'industrie). • Ministère de l'Environnement, de l'Énergie et de la Mer (depuis 2016) Le ministère devient Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM) et est chargée des relations internationales sur le climat. Source Wikipédia : http://fr.wikipedia.org/wiki/Minist%C3%A8re_de_l'Environnement,_de_l http://fr.wikipedia.org/wiki/Liste_des_ministres_fran%C3%A7ais_des_T
MTU *= 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
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	principalement entre systèmes UNIX. Des implémentations existent pour Macintosh et Microsoft Windows. NFS est compatible avec IPv6 sur la plupart des systèmes.
Nginx *= Engine-x*	Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions. Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.
NSCD *= Name Service Caching Daemon*	NSCD met en cache les requêtes faites à la libc auprès des services de nom. Si la récupération des données NSS est relativement coûteuse, NSCD peut accélérer de façon importante des accès consécutifs aux mêmes données et améliorer les performances globales du système.
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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

OAuth	OAuth est un protocole libre qui permet d'autoriser un site web, un logiciel ou une application (dit « consommateur ») à utiliser l'API sécurisée d'un autre site web (dit « fournisseur ») pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification, mais un protocole de "délégation d'autorisation". Source Wikipédia : http://fr.wikipedia.org/wiki/OAuth
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.
OpenID	OpenID est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID. Le modèle se base sur des liens de confiance préalablement établis entre les fournisseurs de services et les fournisseurs d'identité (OpenID providers). Il permet aussi d'éviter de remplir à chaque fois un nouveau formulaire en réutilisant les informations déjà disponibles. Ce système permet à un utilisateur d'utiliser un mécanisme d'authentification forte.
OpenID Connect *= OIDC*	OpenID Connect est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID Connect. Cette couche d'identification simple est basée sur le protocole OAuth 2.0. Ce standard est géré par la fondation OpenID. Plusieurs entreprises utilisent OpenID Connect tel Google, Microsoft, Ping Identity, Deutsche Telekom, salesforce.com, Trustelem. L'état Français l'utilise également dans son dispositif d'authentification et d'identification universel FranceConnect. Source Wikipédia : http://fr.wikipedia.org/wiki/OpenID_Connect
OpenNebula	OpenNebula est un projet libre et européen qui fournit un ensemble de fonctionnalités permettant de gérer un nuage informatique. OpenNebula organise le fonctionnement d'un ensemble de serveurs physiques, fournissant des ressources à des machines virtuelles. Il orchestre et gère le cycle de vie de toutes ces machines virtuelles.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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
OTP *= One-time password*	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisé par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir. Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	POP3. C'est cette dernière qui a cours actuellement.
POSIX	POSIX est le nom d'une famille de standards définie depuis 1988 par l'Institute of Electrical and Electronics Engineers. Ces standards ont émergé d'un projet de standardisation des API des logiciels destinés à fonctionner sur des variantes du système d'exploitation UNIX.
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.
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.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ramsese *= Répertoire académique et ministériel sur les établissements du système éducatif*	Une base Ramsese est le fichier de gestion des établissements secondaires d'une académie : EPLE (établissements publics locaux d'enseignements) et EREA (établissements régionaux d'enseignements adaptés) publics et privés. Il contient toutes les informations concernant chaque établissement, notamment sa localisation, son code. Caractéristiques techniques : • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
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.
Redis *= REmote DIctionary Server*	Le nom Redis vient de l'anglais REmote DIctionary Server qui peut être traduit par « serveur de dictionnaire distant » et qui est un jeu de mot avec le mot Redistribute. Redis est un système de gestion de base de données clef-valeur scalable, très hautes performances, écrit avec le langage de programmation C ANSI et distribué sous licence BSD. Il fait partie de la mouvance NoSQL et vise à fournir les performances les plus élevées possibles. Source Wikipédia : http://fr.wikipedia.org/wiki/Redis
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.
Restauration	La restauration c'est la réutilisation de données sauvegardées. C'est

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	l'opération inverse de la sauvegarde.
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 *= 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.
SAML *= Security assertion markup language*	SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.
SAN *= Storage Area Network*	Un SAN, un réseau de stockage est un réseau spécialisé permettant de mutualiser des ressources de stockage. Un réseau de stockage se différencie des autres systèmes de stockage tels que le NAS (Network attached storage) par un accès bas niveau aux disques. Pour simplifier, le trafic sur un SAN est très similaire aux principes utilisés pour l'utilisation des disques internes (ATA, SCSI). C'est une mutualisation des ressources de stockage. Source Wikipédia : https://fr.wikipedia.org/wiki/R%C3%A9seau_de_stockage_SAN
Sauvegarde *= Backup*	La sauvegarde est l'opération qui consiste à dupliquer dans un lieu sûr les données contenues dans un système informatique.
Scannedonly	Scannedonly est composé d'un module VFS (Virtual File System) Samba et d'un service d'exploration qui garantissent que seuls les fichiers qui ont été scannés pour les virus sont visibles et accessibles

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	à l'utilisateur final. http://olivier.sessink.nl/scannedonly/
SecurID	SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID
SGMAP *= Secrétariat Général pour la Modernisation de l'Action Publique*	Le secrétariat général pour la modernisation de l'action publique est une administration française placée sous l'autorité du Premier ministre et rattachée au secrétaire général du Gouvernement. http://www.modernisation.gouv.fr/
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. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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.
StartTLS	Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas, par exemple des protocoles de mails IMAP et SMTP ou LDAP.
strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/
SubjectAltName	OpenSSL respecte la norme X. 509v3 qui permet d'étendre la demande de certificat à l'usage qui en sera fait du dit certificat.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Subject Alternative Name, nom alternatif du sujet du certificat, SAN	Plusieurs extensions sont disponibles dont l'extension Subject Alternative Name. Cette extension permet d'inclure diverses valeurs littérales dans le fichier de configuration : • un email (une adresse de courrier électronique) ; • un URI (un indicateur de ressource uniforme) ; • un DNS (un nom de domaine DNS) ; • un RID (un ID enregistré: OBJECT IDENTIFIER) ; • une adresse IP ; • un dirName (un nom distinctif) ; • ou un otherName (un autre nom distinctif).
Sunstone	Sunstone est une interface graphique permettant de gérer OpenNebula. C'est une application Web qui permet de gérer et d'administrer les machines virtuelles et tout ce qui s'y rapporte. Depuis la version 2.7.2, l'accès à l'interface Sunstone s'effectue en https via un navigateur web : `https://<adresseServeur>`
systemd *= system daemon*	systemd est un système d'initialisation et un daemon qui a été spécifiquement conçu pour le noyau Linux comme alternative à System V. Il a pour but d'offrir un meilleur cadre pour la gestion des dépendances entre services, de permettre le chargement en parallèle des services au démarrage, et de réduire les appels aux scripts shell. Le projet a été lancé par Lennart Poettering en 2010 et publié sous licence GNU LGPL version 2.1. https://fr.wikipedia.org/wiki/Systemd
TCP *= Transmission Control Protocol*	TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport qui travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.
TCP Wrapper *= tcpd*	TCP Wrapper est une technique, propre à Unix, permettant de contrôler les accès à un service (ou démon) suivant la source. Il se configure grâce au deux fichiers /etc/hosts.allow et /etc/hosts.deny. Tous les démons ne supportent pas la technique TCP Wrapper.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
Twisted	Twisted est un framework d'application réseau écrit en Python et sous licence MIT. Twisted supporte TCP, UDP, SSL/TLS, multicast, Unix domain sockets, un grand nombre de protocoles dont HTTP, NNTP, IMAP, SSH, IRC, FTP, et beaucoup d'autres. Twisted se base sur un paradigme événementiel, ce qui signifie que les utilisateurs écrivent de courtes fonctions de rappel (callbacks) qui sont appelées par le framework. http://twistedmatrix.com
UAC *= User Account Control*	UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7. UAC est aussi connu sous ses dénominations précédentes durant le développement de Windows Vista, à savoir UAP (User Account Protection) et LUP (Least User Privilege). Ce mécanisme permet d'exécuter par défaut les programmes avec des droits restreints, évitant ainsi que des applications puissent tourner avec des droits administratifs, qui permettraient de modifier la sécurité du système d'exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

UAC *= User Account Control*	UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7. UAC est aussi connu sous ses dénominations précédentes durant le développement de Windows Vista, à savoir UAP (User Account Protection) et LUP (Least User Privilege). Ce mécanisme permet d'exécuter par défaut les programmes avec des droits restreints, évitant ainsi que des applications puissent tourner avec des droits administratifs, qui permettraient de modifier la sécurité du système d'exploitation.
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
UNC *= Universal Naming Convention ou Uniform Naming Convention*	UNC est une convention sur une manière de définir l'adresse d'une ressource sur un réseau. Plutôt que de spécifier une lettre de lecteur et un chemin d'accès (par exemple, `D:\lecteur`), on utilise la syntaxe suivante `\\serveur\partage\répertoire\nomFichier`
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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
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.
Wake on Lan *= WoL*	Wake on Lan est un standard des réseaux Ethernet qui permet à un ordinateur éteint d'être démarré à distance. Source Wikipédia : http://fr.wikipedia.org/wiki/Wake-on-LAN
WINS *= Windows Internet Name Service*	WINS est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.
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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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 : • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. Source : http://fr.wikipedia.org/wiki/Xml
XML-RPC *= XML Remote procedure call*	XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau. XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et avec n'importe quel langage de programmation. Le serveur est lui même sur n'importe quel système et est programmé dans n'importe quel langage. Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage. Source : http://fr.wikipedia.org/wiki/XML-RPC
XMPP *= Extensible Messaging and Presence Protocol*	XMPP peut être traduit par « Protocole extensible de présence et de messagerie »), et est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données. XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la Voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	XMPP est constitué d'un protocole TCP/IP basé sur une architecture client-serveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML). XMPP est en développement constant et ouvert au sein de l'IETF.
YAML *= YAML Ain't Markup Language*	YAML est un format de représentation de données par sérialisation Unicode. Il reprend des concepts d'autres langages comme XML, ou encore du format de message électronique. Son objet est de représenter des informations plus élaborées que le simple CSV en gardant cependant une lisibilité presque comparable, et bien plus grande en tout cas que du XML. Symfony 2, Drupal 8 et phpMyAdmin, entre autres, l'utilisent pour leurs formats d'entrée et de sortie. Source Wikipédia : http://fr.wikipedia.org/wiki/YAML
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)