Installation et mise en œuvre du module AmonEcole

EOLE 2.5.2



création : Mai 2015 Version : révision : Avril 2018 Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

EOLE 2.5.2

Version : révision : Avril 2018

Date : création : Mai 2015

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 - Introduction au module AmonEcole 11
1. Qu'est ce que le module AmonEcole ? 11
2. À qui s'adresse ce module ? 13
3. Les services AmonEcole 13
4. Structure des conteneurs 14
4.1. Les conteneurs du module AmonEcole 15
4.2. Les flux réseaux entre conteneurs du module AmonEcole 15
5. Pré-requis 16
6. Les différences entre les versions 2.4 et 2.5 16
7. Errata 2.5.n 20
Chapitre 2 - Fonctionnement du module AmonEcole 22
Chapitre 3 - Installation du module AmonEcole 24
Chapitre 4 - Configuration du module AmonEcole 26
1. Configuration en mode basique 26
1.1. Onglet Général 27
1.2. Onglet Services 29
1.3. Onglet Firewall 30
1.4. Onglet Interface-0 31
1.5. Onglet Interface-1 33
1.6. Onglet Directeur bareos 35
1.7. Onglet Dhcp : Configuration du serveur DHCP 35
1.8. Onglet Samba : Configuration du contrôleur de domaine 37
1.9. Onglet Applications web : Configuration des applications web 39
1.10. Onglet Messagerie 39
2. Configuration en mode normal 41
2.1. Onglet Général 42
2.2. Onglet Services 45
2.3. Onglet Firewall 46
2.4. Onglet Interface-0 47
2.5. Onglet Interface-1 51
2.6. Onglet Interface-n 55
2.7. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité 60
2.8. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs 64
2.9. Onglet Clamav : Configuration de l'anti-virus 65
2.10. Onglet Directeur bareos 66
2.11. Onglet Stockage bareos 69
2.12. Onglet Annuaire 69
2.13. Onglet Dhcp : Configuration du serveur DHCP 70
2.14. Onglet Esu : Configuration du proxy ESU 72
2.15. Onglet Samba : Configuration du contrôleur de domaine 73
2.16. Onglet Onduleur 76
2.17. Onglet Rvp : Mettre en place le réseau virtuel privé 82
2.18. Onglet Applications web : Configuration des applications web 84
2.19. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 87
2.20. Onglet Messagerie 91
2.21. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS 93
2.22. Onglet Proxy authentifié : 5 méthodes d'authentification 95

2.23. Onglets Proxy authentifié 2 : Double authentification 100
2.24. Onglet Exceptions proxy 100
2.25. Onglet Reverse proxy : Configuration du proxy inverse 102
2.26. Onglet Freeradius : Configuration de l'authentification Radius 105
3. Configuration en mode expert 109
3.1. Onglet Général 111
3.2. Onglet Services 114
3.3. Onglet Firewall 115
3.4. Onglet Système 117
3.5. Onglet Sshd : Gestion SSH avancée 119
3.6. Onglet Logs : Gestion des logs centralisés 119
3.7. Onglet Interface-0 121
3.8. Onglet Interface-1 127
3.9. Onglet Interface-n 133
3.10. Onglet Réseau avancé 139
3.11. Onglet Certificats ssl : gestion des certificats SSL 143
3.12. Onglet Apt-cacher 145
3.13. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité 145
3.14. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs 149
3.15. Onglet Clamav : Configuration de l'anti-virus 150
3.16. Onglet Directeur bareos 153
3.17. Onglet Stockage bareos 156
3.18. Onglet Annuaire 157
3.19. Onglet Dhcp : Configuration du serveur DHCP 158
3.20. Onglet Tftp : Configuration d'un serveur PXE/TFTP 161
3.21. Onglet Esu : Configuration du proxy ESU 161
3.22. Onglet Samba : Configuration du contrôleur de domaine 163
3.23. Onglet Nscd 171
3.24. Onglet Onduleur 172
3.25. Onglet Rvp : Mettre en place le réseau virtuel privé 178
3.26. Onglet Applications web : Configuration des applications web 183
3.27. Onglet Apache : Configuration avancée du serveur web 185
3.28. Onglet Envole : Espace Numérique Personnel pour l'Éducation 188
3.29. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 189
3.30. Onglet Zones-dns : Configuration du DNS 196
3.31. Onglet Ead-web : EAD et proxy inverse 198
3.32. Onglet Mysql : Configuration du serveur MySQL 199
3.33. Onglet Messagerie 199
3.34. Onglet Openldap : Configuration du serveur LDAP local 206
3.35. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS 207
3.36. Onglet Filtrage web : Configuration du filtrage web 209
3.37. Onglet Squid : Configuration du proxy 214
3.38. Onglet Proxy authentifié : 5 méthodes d'authentification 219
3.39. Onglets Squid2 et Proxy authentifié 2 : Double authentification 224
3.40. Onglet Exceptions proxy 225
3.41. Onglet Cups : Configuration du serveur d'impression 227
3.42. Onglet Proxy parent : Chaînage du proxy 229
3.43. Onglet Reverse proxy : Configuration du proxy inverse 231
3.44. Onglet Proftpd : Configuration du serveur FTP 235
3.45. Onglet Freeradius : Configuration de l'authentification Radius 238
3.46. Onglet Eoleflask 242
3.47. Onglet Ent : Configuration de l'ENT 243
4. Configuration DNS pour chaque interface 244
5. Configurer la découverte automatique du proxy avec WPAD 247

6. Configuration du mode multi-établissement 252
7. Authentification unique avec EoleSSO 253
7.1. Présentation du produit EoleSSO 253
7.2. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 255
7.3. Protocoles supportés 262
7.3.1. Compatibilité CAS 262
7.3.2. Compatibilité SAML2 263
7.3.3. Compatibilité RSA Securid 264
7.3.4. Compatibilité OpenID Connnect 265
7.4. Gestion des attributs des utilisateurs 271
7.4.1. Ajout d'attributs calculés 271
7.4.2. Filtrage des données par application 274
7.4.3. Définition de filtres d'attributs 276
7.5. Fédération avec une entité partenaire 277
7.5.1. Déclaration d'un serveur parent 277
7.5.2. Fédération SAML : Gestion des Associations 278
7.5.3. Fédération SAML : Gestion des méta-données 283
7.5.4. Fédération SAML : Accès aux ressources 283
7.5.5. Gestion des sources d'authentification multiples 286
7.6. Personnalisation de la mire SSO 289
7.7. Configuration d'EoleSSO en mode cluster 291
7.8. Répartition de charge EoleSSO en mode cluster 294
7.9. Compléments de configuration EoleSSO 308
7.9.1. Résumé des fichiers et liens 308
7.9.2. Astuces d'exploitation 310
7.9.3. Exemple de Fédération avec RSA/FIM 311
7.9.4. Fédération entre 2 serveurs EoleSSO 312
7.9.5. Mise en place de l'authentification OTP 313
7.9.6. Application de redirection : Eole-dispatcher 315
7.9.7. Configuration du fournisseur d'identité France Connect 320
7.9.8. Configuration du fournisseur d'identité Google (Google APIs). 322
8. Activation et configuration de Bareos 323
9. Configuration du module Eclair avec un module AmonEcole 328
10. Gestion des bases de données avec EoleDB 330
Chapitre 5 - Instanciation du module 338
Chapitre 6 - Administration du module AmonEcole 339
1. Les rôles sur le module AmonEcole 339
2. Fonctionnalités de l'EAD propres au module AmonEcole 343
2.1. Les rôles sur le module AmonEcole 343
2.2. Groupes et utilisateurs 348
2.2.1. Groupes 348
2.2.2. Utilisateurs 358
2.2.3. Lettres de lecteur 365
2.2.4. Gestion fine des groupes et des utilisateurs : ACL 366
2.2.5. Visualisation des quotas disque dans l'EAD 367
2.2.6. Étendre les droits d'un personnel administratif avec les droits d'un enseignant 369
2.3. Importation de comptes 371
2.3.1. Préparation des fichiers nécessaires à l'importation 371
2.3.2. Importation par l'EAD 375
2.3.3. Importation en mode console 383
2.3.4. Informations complémentaires 384

2.4. Distribution de documents dans l'EAD 385
2.4.1. Distribuer des documents 386
2.4.2. Ramasser des documents 387
2.4.3. Rendre des documents 388
2.4.4. Supprimer les données 388
2.5. Observation des virus 389
2.6. Gestion des machines 390
2.7. Gestion des connexions dans l'EAD 391
2.8. Réservation d'adresse IP dans l'EAD 395
2.9. Directives optionnelles ERA depuis l'EAD 396
2.10. Exceptions sur la source ou la destination 396
2.11. Filtrage web 398
2.11.1. Filtrage par utilisateur 399
2.11.2. Filtrage par machine ou par groupe de machine 399
2.11.3. Interdire l'accès à un sous-réseau depuis une interface 405
2.11.4. Interdire ou restreindre l'activité d'un sous-réseau 407
2.11.5. Bases de filtres optionnels 409
2.11.6. Filtrage syntaxique 411
2.11.7. Interdire et autoriser des domaines 412
2.11.8. Interdire des extensions et des types MIME 414
2.11.9. Politique liste blanche 416
2.12. Observatoire des navigations 417
2.13. Outil d'analyse de logs LightSquid 418
3. Les clients GNU/Linux 421
3.1. Principe du client GNU / Linux 421
3.2. Configuration des comptes utilisateurs sur le serveur 424
3.3. Authentification LDAP depuis le client GNU / Linux 426
3.4. Problèmes d'authentification rencontrés et solutions 430
3.5. Partages avec NFS 432
3.6. Partages avec Samba 434
3.7. Intégration dans un environnement graphique 437
3.8. Installation de Gaspacho 439
3.9. Scripts d'intégration pour GNU / Linux 440
3.9.1. Paramétrage des clients GNU/Linux 443
3.10. Liens vers des contributions externes 446
4. Les clients Windows 447
4.1. Installation et configuration des clients Windows 447
4.1.1. Principe 447
4.1.2. Configuration réseau 447
4.1.3. Intégration et installation du client Scribe automatique 448
4.1.4. Intégration et installation du client Scribe manuelle 458
4.1.5. Mise à jour du client Scribe 475
4.1.6. Désinstallation du client Scribe 476
4.2. Administration des clients Windows 477
4.2.1. L'ouverture de session 478
4.2.2. Les profils utilisateurs 480
4.2.3. Gestion des configurations clientes avec ESU 487
4.2.4. L'application Gestion-postes 495
4.2.5. Administration avancée des clients Scribe 504
4.2.6. ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés 514
4.2.7. Gestion des quotas disque 516
4.3. Résolution des problèmes du client 522

4.3.1. Problèmes à l'inscription au domaine 522
4.3.2. Problèmes avec le Client Scribe 522
4.3.3. Problèmes Controle-vnc 524
4.3.4. Problèmes de droits sur les répertoires partagés 524
4.4. Déploiement d'applications pour Windows avec WPKG 524
4.4.1. Installation et configuration 525
4.4.2. Les packages WPKG 529
4.4.3. Journalisation des actions WPKG 533
4.4.4. WPKG scripts de pre et post installation 536
4.4.5. WPKG logiciels avec traitement particulier 540
4.4.6. Quelques références 540
5. Les clients FTP 541
6. Les clients Jabber 544
6.1. Mise en place du serveur jabber 544
6.2. Configuration d'un client 545
6.3. Jappix : client web Jabber 546
7. Administration des listes de diffusion 548
7.1. Présentation 548
7.2. L'interface web 549
7.3. Les listes créées automatiquement 549
7.4. Création manuelle de listes 552
7.5. Architecture du gestionnaire de liste de diffusion 553
7.6. Architecture messagerie académique 554
7.7. Résoudre des dysfonctionnements liés aux listes de diffusion 555
8. Synchronisation depuis l'Annuaire Académique Fédérateur - AAF 556
9. Outils à destination des enseignants 560
9.1. EOP : application web à destination des enseignants 560
9.1.1. Présentation 560
9.1.2. Distribution de documents 563
9.1.3. Gestion des documents 568
9.1.4. Observation et/ou contrôle à distance 571
9.1.5. Bloquer Internet / Masquer les partages (Mode devoir) 571
9.1.6. Changement de mot de passe par lot 573
9.1.7. Délégation de droits 574
9.1.8. Documentation technique 575
9.2. L'application Gestion-postes 576
9.2.1. Observation / Diffusion du poste 577
9.2.2. Bloquer Internet / Masquer les partages (Mode devoir) 580
9.2.3. Distribution de devoirs 582
9.3. Distribution de documents dans l'EAD 586
9.3.1. Distribuer des documents 587
9.3.2. Ramasser des documents 588
9.3.3. Rendre des documents 589
9.3.4. Supprimer les données 589
10. Les sauvegardes 590
10.1. Généralités sur la sauvegarde 590
10.1.1. Sauvegarde totale 591
10.1.2. Sauvegarde incrémentale 591
10.1.3. Sauvegarde différentielle 591
10.1.4. Des outils de sauvegarde 591
10.2. La sauvegarde EOLE 592

10.2.1. Le vocabulaire Bareos 593
10.2.2. Architecture de Bareos 595
10.2.3. Configuration des sauvegardes 596
10.2.4. Programmation des sauvegardes 608
10.3. La restauration des sauvegardes EOLE 610
10.3.1. Restauration complète 610
10.3.2. Restauration partielle 613
10.4. Ajouter des données à sauvegarder 617
10.5. Réinitialisation de la sauvegarde 618
10.6. bareos-webui : outil d'administration pour Bareos 619
10.7. Diagnostic, rapport et résolution de problème 622
10.7.1. Outils de diagnostic et rapport 622
10.7.2. Base de donnée sqlite de Bareos irrécupérable 624
10.8. Annexes 627
10.8.1. Autres outils d'administration pour Bareos 627
10.8.2. Quelques références 628
10.8.3. Un répertoire partagé Windows 7 comme support de sauvegarde 629
10.8.4. Un répertoire partagé Windows XP comme support de sauvegarde 632
11. Les imprimantes 636
11.1. L'interface simplifiée 636
11.2. L'interface de gestion CUPS 637
11.2.1. Création de l'imprimante 637
11.2.2. Choix du pilote 641
11.2.3. Quotas d'impression 646
11.3. Gestion des imprimantes sous Windows 646
11.4. Questions fréquentes 647
12. Les applications web sur le module AmonEcole 647
12.1. L'authentification unique avec EoleSSO 648
12.2. Espace Numérique Personnel pour l'Éducation avec Envole 649
12.2.1. Installation et paramétrage 652
12.2.2. Accès au portail 656
12.2.3. Administration 661
12.2.4. Personnalisations visuelles 696
12.3. Applications pré-installées 701
12.3.1. phpMyAdmin : gestionnaire de base de données MySQL 701
12.3.2. Pydio : gestionnaire de fichiers 703
12.3.3. Roundcube : interface pour le courrier électronique 705
12.3.4. EOP : outils à destination des enseignants 708
12.3.5. EOE : outils à destination des élèves 711
12.4. Applications pré-packagées 712
12.4.1. Ajaxplorer : gestionnaire de fichiers 712
12.4.2. Balad((O)) : partager ses enregistrements 714
12.4.3. Bergamote : indexation et recherche de fichier 716
12.4.4. Calendrier : gestion des événements 717
12.4.5. CDC : carnet de correspondance 719
12.4.6. Cdt : cahier de texte numérique 721
12.4.7. Dokuwiki : rédaction à plusieurs 724
12.4.8. ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés 727
12.4.9. eConnect : centralisation et mise à disposition de ressource en ligne 729
12.4.10. Envole : Espace Numérique Personnel pour l'Éducation 731
12.4.11. ePortail : portail d'entreprise 733

12.4.12. EtherCalc : tableur collaboratif 734
12.4.13. EtherPad : écriture collaborative 736
12.4.14. Feng Office : plateforme collaborative 738
12.4.15. FluxBB : forum de discussions 740
12.4.16. Gepi : gestion des notes, des absences, et des cahiers de texte 742
12.4.17. GRR : gestion de réservation de salles et de matériels 746
12.4.18. ICONITO : Espace Numérique de Travail pour le 1er degré 749
12.4.19. Gestion des quotas disque 750
12.4.20. Jappix : client web Jabber 755
12.4.21. LimeSurvey : sondage et enquête statistique 757
12.4.22. Mahara : portfolio électronique 759
12.4.23. mindmaps : conception de cartes cognitives 760
12.4.24. Moodle : plate-forme d'apprentissage en ligne 762
12.4.25. OpenSondage : planification de rendez-vous et mini-sondage 765
12.4.26. ownCloud : stockage et partage de fichiers 766
12.4.27. Piwigo : gestionnaire de galerie photo 767
12.4.28. Piwik : outil statistique 769
12.4.29. SACoche : évaluation et suivi d'acquisitions de compétences 771
12.4.30. SAP : administration du réseau social d'Envole 772
12.4.31. SPIP Eva : gestion de contenu 774
12.4.32. Taskfreak : gestionnaire de projet 776
12.4.33. Webcalendar : agendas partagés 778
12.4.34. WordPress : système de gestion de contenu 780
12.5. Prise en charge d'applications supplémentaires 783
12.5.1. Téléchargement et mise en place 784
12.5.2. Configuration Apache 785
12.5.3. Configuration MySQL 787
12.5.4. Configuration du logiciel 787
13. Gestion des tunnels : RVP 788
14. Résoudre des dysfonctionnements liés au MTU 790
Chapitre 7 - Paramétrage des postes client 792
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine 792
2. Configurer la découverte automatique du proxy avec WPAD 793
3. Proxy non configuré dans le navigateur : redirection ou page d'information 798
4. Synthèse des paramètres proxy à utiliser pour les postes client 802
Chapitre 8 - Compléments techniques 804
1. Les services utilisés sur le module AmonEcole 804
1.1. eole-annuaire 804
1.2. eole-antivirus 804
1.3. eole-apt-cacher-ng 806
1.4. eole-bareos 806
1.5. eole-client-annuaire 807
1.6. eole-courier 807
1.7. eole-cups 808
1.8. eole-db 808
1.9. eole-dhcp 809
1.10. eole-dns 809
1.11. eole-exim 810
1.12. eole-fichier-primaire 810
1.13. eole-mysql 811
1.14. eole-nut 811
1.15. eole-proftpd 812

1.16. eole-proxy 812
1.17. eole-radius 813
1.18. eole-reverseproxy 814
1.19. eole-spamassassin 814
1.20. eole-sympa 815
1.21. eole-web 815
1.22. eole-wpad 816
2. Ports utilisés sur le module AmonEcole 816
3. Les flux réseaux entre conteneurs du module AmonEcole 819
4. L'annuaire LDAP du module Scribe 820
4.1. Arborescence de l'annuaire 821
4.2. Utilisateurs spéciaux 821
4.3. Entrée groupe 822
4.4. Entrée élève 823
4.5. Entrée enseignant 825
4.6. Entrée personnel administratif 827
4.7. Entrée responsable légal 829
4.8. Entrée compte invité 831
4.9. Entrée ordinateur du domaine 832
4.10. Entrée partage 832
4.11. Annuaire : diagnostic et résolution de problème 833
5. Exportation des fichiers depuis SIECLE et STS 834
6. Le gestionnaire de listes électroniques Sympa 836
6.1. Architecture du gestionnaire de liste de diffusion 836
6.2. Résoudre des dysfonctionnements liés aux listes de diffusion 837
7. Architecture messagerie académique 838
8. La gestion du SID 839
9. Présentation des répertoires partagés du module Scribe 840
9.1. Partages sous Windows 841
9.2. Partages dans Pydio 841
9.3. Partages dans le navigateur web 844
9.4. Partages via un client FTP 845
10. Schéma de fonctionnement du client Scribe 846
Chapitre 9 - Questions fréquentes 847
1. Questions fréquentes communes aux modules 847
2. Questions fréquentes propres au module Amon 862
3. Questions fréquentes propres au module Scribe 864
4. Questions fréquentes propres à la sauvegarde 874
5. Questions fréquentes propres à Envole 878
Glossaire 882

Chapitre 1
Introduction au module AmonEcole

Le module AmonEcole est un pare-feu pédagogique facile à installer et à utiliser.

Il est l'association du module Amon et du module Scribe.

Ce module intègre donc les fonctionnalités des 2 modules :

- il vous permet de partager votre sortie Internet en toute sécurité, et de créer un intranet fédérateur au sein de votre établissement ou de n'importe quel réseau local (entreprise, association, domestique, ...) ;
- il intègre un serveur de fichiers et d'impression, un système de messagerie articulé autour d'un annuaire performant, des services web et une gestion avancée des utilisateurs et des postes clients.

1. Qu'est ce que le module AmonEcole ?

AmonEcole est un module qui intègre les fonctionnalités du module **Amon** (pare-feu) et les fonctionnalités du module **Scribe** (serveur pédagogique).

Grâce à LXC toutes les services seront installées sur une seule machine mais séparées 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 fichier, 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.

Ce module permet de partager en toute sécurité un accès Internet entre les sous-réseaux d'un réseau local.

Installé sur un serveur dédié, équipé de deux, trois, quatre ou cinq interfaces réseau, il permet d'organiser au mieux l'architecture réseau d'un établissement.

Des modèles de règles de pare-feu sont disponibles pour chaque architecture.

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, ERA[p.889], est à votre disposition pour effectuer ce travail.

Il est également possible de créer un réseau privé virtuel (VPN) entre l'établissement (une structure administrative) et un concentrateur académique (par exemple le module Sphynx). Ce réseau virtuel privé permet de sécuriser les flux sensibles au travers d'Internet.

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES[p.882].

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

Le module fournit un contrôleur de domaine doté de fonctions évoluées. Il optimise la gestion de votre parc de stations clientes.

Le module dispose d'un annuaire qui référence élèves, parents, personnels, enseignants et administratifs et propose de nombreuses fonctionnalités.

Principales fonctionnalités

Service réseau :

- routage ;
- authentification des utilisateurs ;
- filtrage IP ;
- filtrage de site amélioré (listes noires et contenu) ;
- réseau virtuel privé ;
- suivi détaillé de la navigation web ;
- mises à jour automatiques ;
- journalisation des fichiers logs ;
- détection d'intrusions ;
- service de cache web ;
- administration simplifiée ;
- statistiques sur l'état du système ;
- statistiques d'utilisation.

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL[p.882] ;
- quotas disque ;
- partage d'imprimantes ;
- gestion des comptes utilisateur et des accès ;
- exécution d'applications utilisateur ;
- gestion des devoirs élève.

Serveur de messagerie articulé autour d'un annuaire performant :

- l'annuaire est initialisé à partir d'importations de comptes (SCONET[p.901], ONDE[p.884], AAF[p.882], CSV[p.887],...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- la messagerie gère deux domaines distincts (l'Internet et l'intranet académique) ;
- utilisation au choix d'une interface web multilingue ou d'un client de messagerie (standards IMAP et POP) ;
- un service de listes de diffusion ;
- un service de messagerie instantanée (standard XMPP[p.906]) ;
- une sécurité anti-spam, un anti-virus, une gestion de quotas (taille des boites aux lettres), ...

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

Serveur web :

- une authentification centralisée ;
- un portail ;
- de nombreuses applications.

Gestion avancée des utilisateurs et des postes client :

- 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 ;
- effectuer des actions distantes sur les stations (fermer la session, éteindre ou redémarrer un ou plusieurs postes) ;
- surveiller la détection de virus par le serveur ;
- surveiller et éventuellement purger les files d'attente des imprimantes connectées au serveur (locales ou distantes).



Ce module est fourni exclusivement en mode conteneur.

2. À qui s'adresse ce module ?

Le module AmonEcole permet d'avoir un pare-feu Amon et un serveur pédagogique Scribe.

Cela permet aux établissements d'avoir différents services sur une même machine physique au lieu de multiplier le nombre de serveurs.

Cela fait du module AmonEcole un candidat idéal aussi bien pour les petites structures que pour les grandes.

3. Les services AmonEcole

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

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

Services communs à tous les modules

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

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

- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Le module pare-feu pédagogique **AmonEcole** reprend les services des modules Amon et Scribe.

Services spécifiques au module Amon

- *Bind* : implémentation la plus répandue du DNS (résolution des noms de machine en adresse IP) ;
- *iptables* : filtrage d'adresses IP ;
- *Squid* : proxy cache qui permet d'accélérer les connexions Internet ;
- *e2guardian* : outil de filtrage syntaxique des adresses web ;
- *LightSquid* : générateur de statistiques pour le proxy Squid ;
- *Strongswan* : version libre d'IPSec. Permet la création de réseaux virtuels privés ;
- *NginX* : proxy inverse ;
- *FreeRADIUS* : service d'authentification réseau ;
- *ERA* : outil de génération de règles iptables.

Services spécifiques au module Scribe

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *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.882] ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de base de données ;
- *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 le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;
- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

4. Structure des conteneurs

Le module AmonEcole reprend les fonctionnalités du module Scribe et du module Amon en les distribuant dans 4 conteneurs.

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

4.1. Les conteneurs du module AmonEcole

Le module AmonEcole reprend les fonctionnalités du module Scribe et du module Amon en les distribuant dans 4 conteneurs.

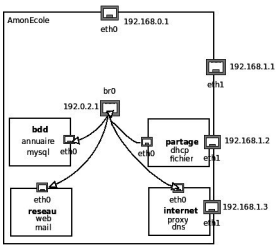
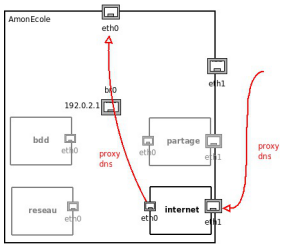


Schéma des conteneurs du module AmonEcole, exemple d'adresses IP proposées par défaut

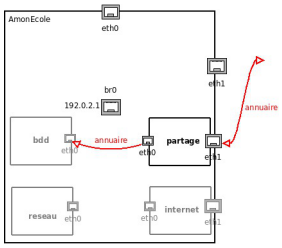
Deux conteneurs ont une adresse IP sur le réseau eth1 :

- le conteneur avec le proxy et le DNS ;
- le conteneur avec le serveur DHCP et le partage de fichiers.

4.2. Les flux réseaux entre conteneurs du module AmonEcole

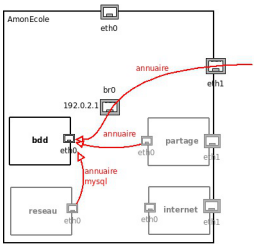


Le conteneur "internet"



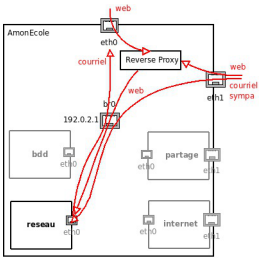
Le conteneur "partage"

Les deux autres conteneurs ne sont accessibles que par le réseau interne.



Le conteneur "bdd"

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



Le conteneur "réseau"

5. Pré-requis

Ce module fonctionne relativement bien sur des petits serveurs.

Les CPU doivent être de préférence en 64 bits.

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

Le modèle de filtrage est un modèle 2 zones qui nécessite deux cartes réseau.

La taille du disque dur est dépendante du nombre d'utilisateurs.

Les partitions à privilégier sont le `/home` et le `/var`.

Exemple d'usage du module AmonEcole dans une école du 1er degré. Il y a environ 200 comptes utilisateurs, 18 postes clients et 16 connectés en moyenne. Cette machine est équipée d'un processeur Intel avec 8Go de RAM et 2 disques dur de 2To.

6. Les différences entre les versions 2.4 et 2.5

La version 2.5 du module AmonEcole n'est disponible qu'à partir de la version 2.5.1 d'EOLE.

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

Noyau

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

Mise à jour

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

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

Passage à une nouvelle version

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

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

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

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

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

Commandes

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

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

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

Interface de configuration du module

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

- Flask[p.890] ;
- Backbone.js[p.883] et Marionette[p.893] ;
- Tiramisu[p.903].

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

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

Règles pare-feu

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

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

Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu[p.903].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML[p.905] Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

Mode conteneur

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

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

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

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

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

Changement dans le PATH des commandes

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

Répertoire d'installation du logiciel Nginx

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

Suppression de la base matériels

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

Logiciel de sauvegarde

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

La sauvegarde

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

2.5.1

Filtrage avec e2guardian

Le module Amon intègre le logiciel libre e2guardian[p.888]. Le logiciel DansGuardian a été complètement abandonné sur le module. Le nombre maximum de processus disponibles pour traiter les nouvelles connexions peut être modifié jusqu'à 8192.

WPAD

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Paquet dédié pour le service WPAD d'EOLE

Un paquet nommé `eole-wpad` est nouvellement dédié pour gérer la découverte automatique du proxy par les navigateurs.

ClamAV

À partir de la version 2.5.1, l'antivirus temps réel ClamAV est activé par défaut et utilisé pour le FTP et la messagerie mais est désactivé sur les partages Samba.

Optimisation du client Scribe

Le client Scribe a été optimisé, il utilise désormais la base de données MySQL locale pour stocker ses

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

informations.

L'ancien fichier `/usr/share/eole/controlevnc/machines.db` n'est plus du tout utilisé. Les informations sur les stations gérées par le client Scribe peuvent être obtenues en utilisant le script `/usr/share/eole/controlevnc/manage_stations.py`.

Gestion des ACLs depuis l'EAD

L'EAD permet depuis cette version d'appliquer :

- des droits par défaut pour un répertoire donné ;
- les modifications des droits de façon récursive.

Activation du proxy ESU dans les modèles par défaut

Maintenant, il est possible de configurer l'activation du proxy ESU dans les modèles par défaut. Ces modèles ne sont modifiés qu'à la première instance.

Choix du type de partitionnement à l'installation

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

2.5.2

Mot de passe au 1er redémarrage après installation

Une fois le système redémarré, comme indiqué par le prompt, vous pouvez ouvrir une session en console, mais aussi par SSH, avec l'utilisateur **root** et le **mot de passe aléatoire** qui est **affiché**.

Gestion des ACLs depuis l'EAD

La gestion des droits s'applique désormais aux fichiers et répertoires cachés.

Liste des machines

Dans l'EAD, il était possible de lister des machines du réseau local selon certains critères (Maîtres explorateurs, Contrôleur de domaine, Toutes les stations). Ces options ont été supprimées suite à l'arrêt du support de Windows XP.

JoinEOLE

JoinEOLE est un utilitaire de jonction au domaine Samba.

Il remplace les deux outils anciennement utilisés que forment le couple Prepawin et IntegrDom.

EOP

Des changements fonctionnels ont été réalisés sur l'application EOP. La date de distribution est maintenant conservée dans l'historique. La valeur maximale de téléversement peut être ajustée. Enfin, une délégation de droits a été ajoutée. Cette version d'EOP est compatible avec les navigateurs modernes ou avec une version d'Internet Explorer 9 et supérieure.

AAF

Les adresses électroniques des responsables ainsi que leurs numéros de téléphone mobile sont désormais disponibles dans les exports AAF. Les adresses postales sont également multi-lignes. Ces nouveautés sont prises en charge par la procédure EOLE d'importation AAF.

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

Samba

Deux nouvelles variables expertes permettent de forcer le niveau de protocole maximum supporté par le serveur et d'annoncer le service Spoolss comme architecture x64.

Gestion des bases de données EoleDB

EoleDB est un nouvel outil qui permet de gérer les bases de données sur un module EOLE. Avec un seul fichier de configuration il permet de gérer nativement plusieurs types de bases de donnée (MySQL, PostgreSQL, SQLite, ...). Il prend en charge l'externalisation, la génération et la mise à jour des bases de données.

Envole 5

Envole est un outil qui permet de mettre en place un Espace Numérique Personnel pour l'Éducation. C'est un portail qui rassemble un ensemble conséquent d'applications web.

Sur EOLE 2.5.2, ce sont les paquets correspondants à la version n°5 d'Envole qui sont mis à disposition.

2.5.2.1

Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI[p.904].

7. Errata 2.5.n

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

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



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



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

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

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

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

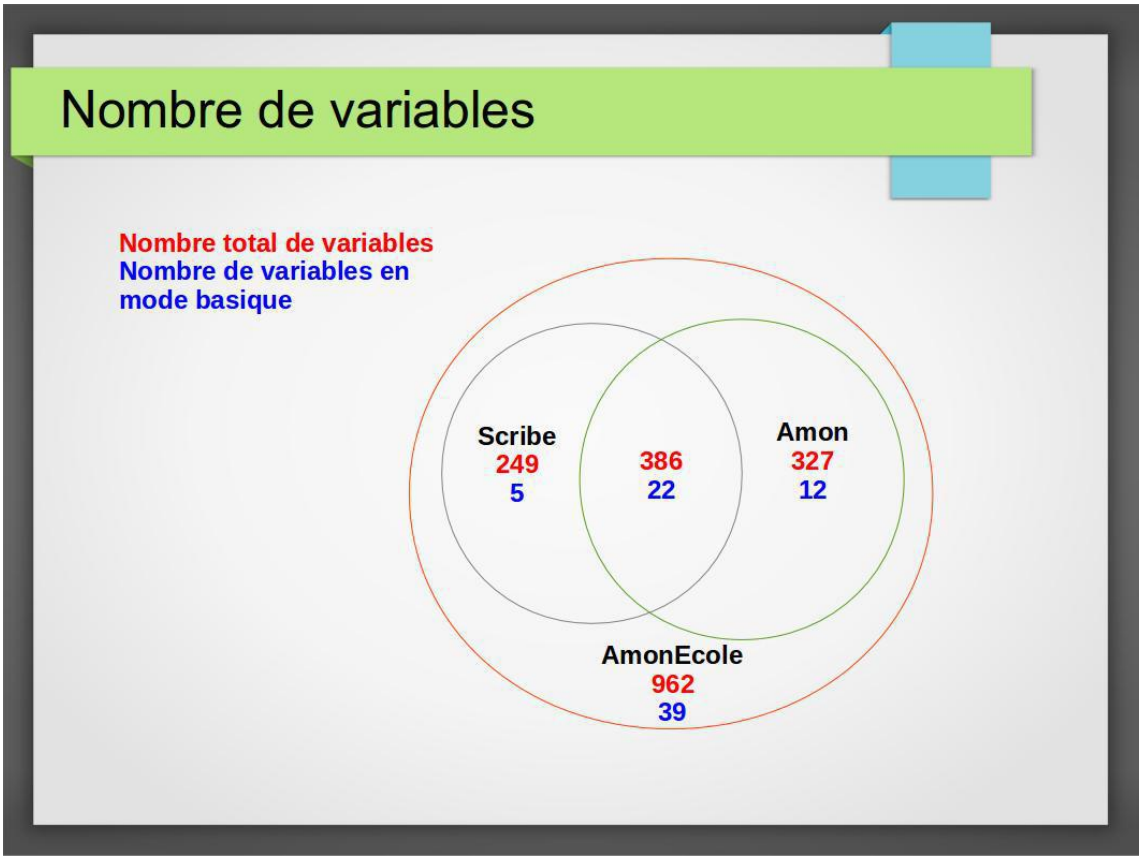
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 2
Fonctionnement du module AmonEcole

Le module AmonEcole a été imaginé pour les écoles et a vocation à être hébergé en établissement.

Basés sur la technologie LXC[p.893], les conteneurs permettent d'isoler les services avec une seule instance du noyau.

Ainsi, le module AmonEcole intègre les fonctionnalités des module **Amon** (pare-feu) et **Scribe** (serveur pédagogique) de manière cohérente avec une répartition des différents services.



Variables de configuration utilisées par le module AmonEcole

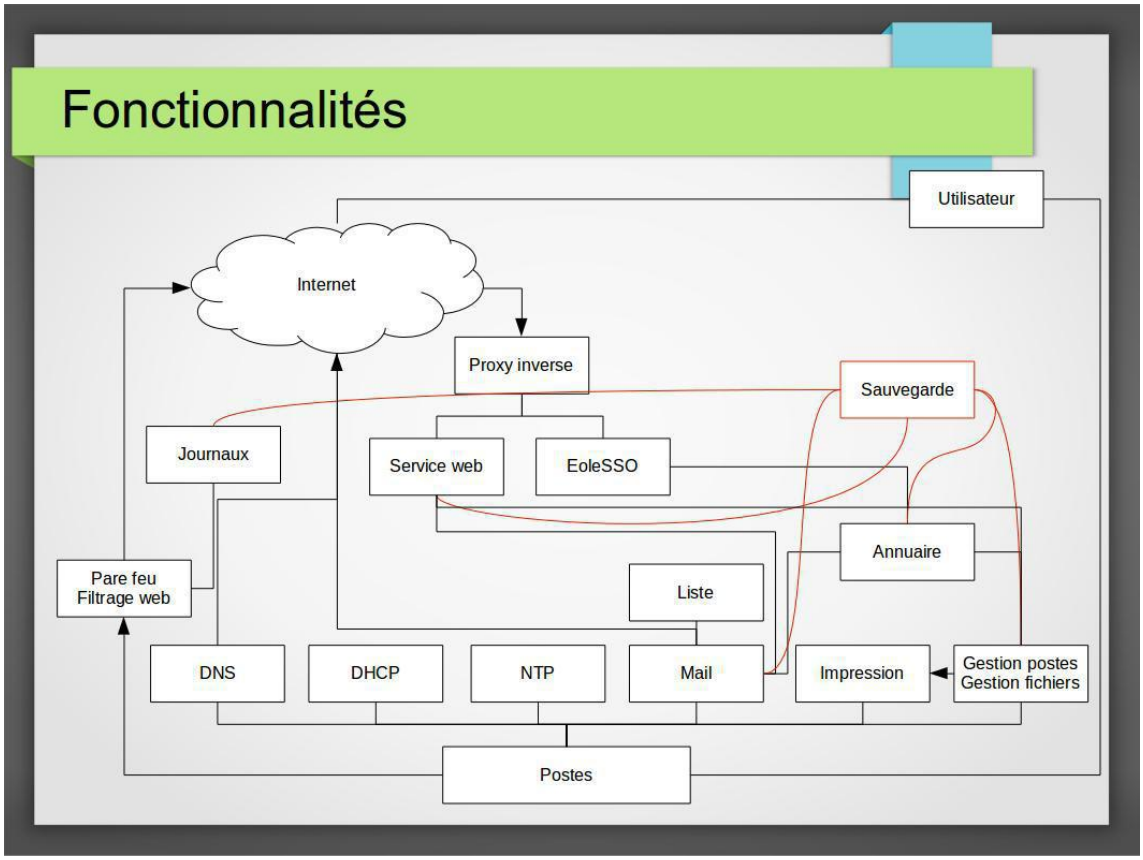
La configuration est centralisée, environ 400 variables sont communes aux modules Amon et Scribe. L'utilisation d'AmonEcole permet de s'affranchir d'une saisie redondante d'informations avec pour effet une meilleure cohérence de la configuration et une absence d'erreur de saisie.

L'intérêt est également d'avoir un seul module à surveiller et à administrer.

L'administration des conteneurs se fait depuis le maître au travers de SSH[p.902].

Les fonctionnalités offertes sont celles du module Scribe et du module Amon cumulées.

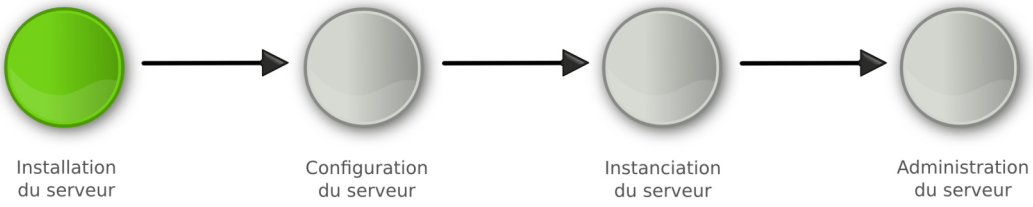
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Chapitre 3
Installation du module AmonEcole

La première des quatre phases



Installation

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

- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.891] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (https://pcll.ac-dijon.fr/eole/). Tous les modules installables depuis cette unique image ISO.

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

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

Après l'installation du module AmonEcole, il est nécessaire de procéder à l'installation des conteneurs. La mise à jour n'est pas obligatoire mais fortement recommandée.

Mise à jour

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

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

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

Installation des conteneurs

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

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.

> Comme sur la version 2.4 il n'est plus possible, sur un module en version 2.5.x, 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`.

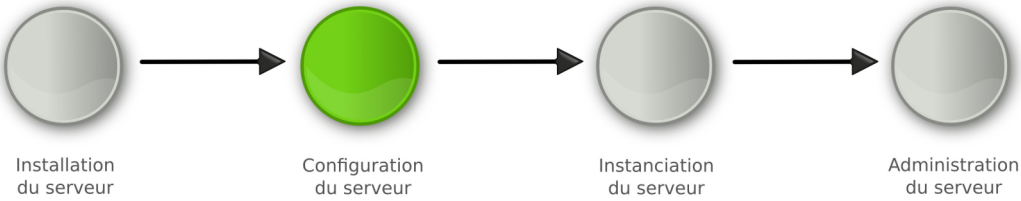
L'option `-l` permet de choisir le niveau des messages (info, warning,error ou critical).

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.

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

Chapitre 4
Configuration du module AmonEcole



Configuration

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

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

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

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

  Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid[p.902], e2guardian[p.888], etc.

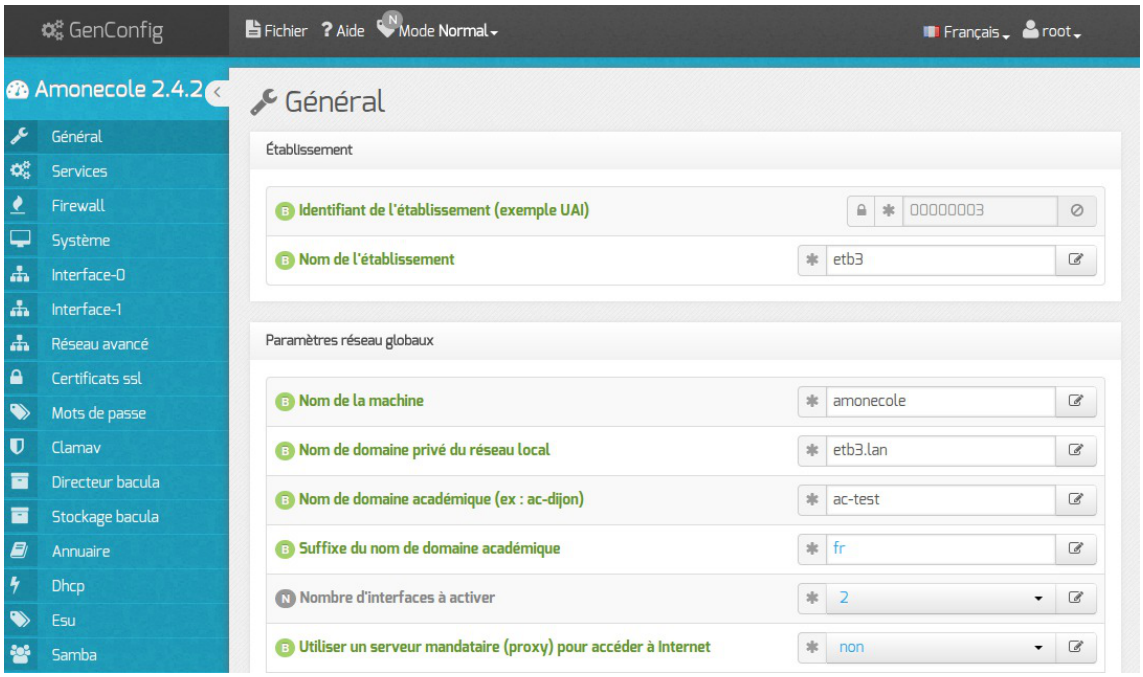
1. Configuration en mode basique

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

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Directeur bareos` ;
- `Dhcp` * ;
- `Samba` ;
- `Applications web` ;
- `Messagerie`.

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

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

Dans les onglets `Général` et `Firewall`, deux options sont à renseigner avec la plus grande attention : le `Nombre d'interfaces à activer` et le `Modèle de filtrage`.

En effet, ces options vont orienter l'architecture de vos réseaux internes ainsi qu'une partie importante de la politique de sécurité qui sera mise en place.

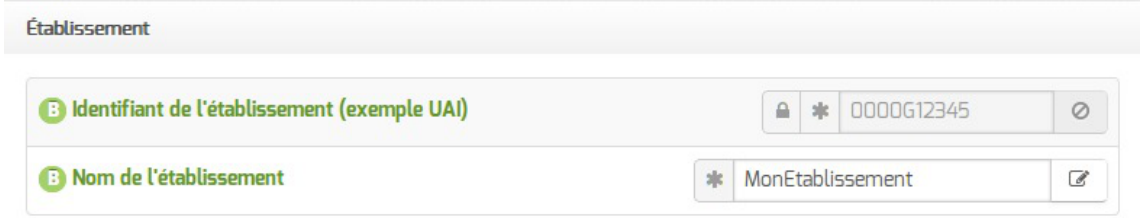
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.

1.1. Onglet Général

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

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

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

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

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

Sur les modules fournissant un annuaire LDAP[p.892] local, ces variables sont utilisées pour créer l'arborescence.



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

Paramètres réseau globaux



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

Cette information est découpée en plusieurs champs :

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

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

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

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

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

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

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



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

Nombre d'interfaces

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

Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

Proxy

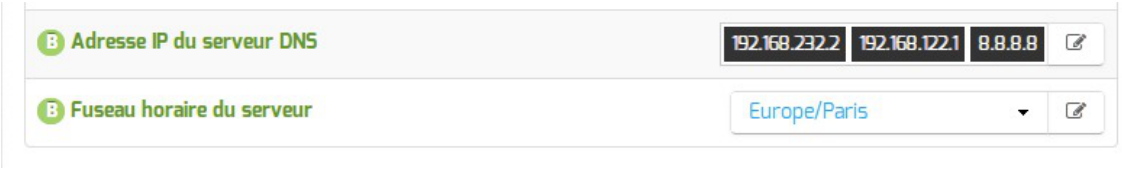
Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.



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

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

DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.887].

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

Voir aussi...

> Onglet Interface-n

1.2. Onglet Services

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

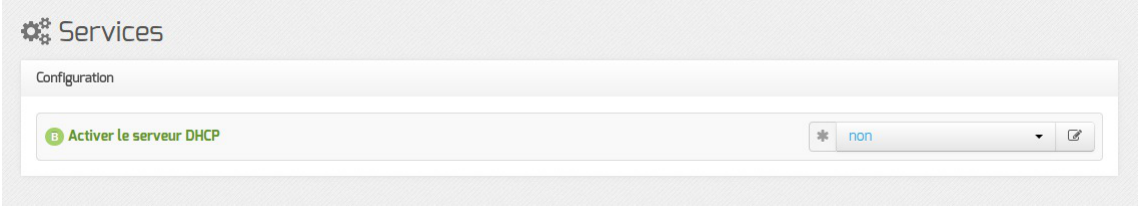
Suivant le module installé et le mode utilisé pour la configuration la liste des services activables ou désactivables est très différente.



Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un

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

onglet de configuration propre au service.

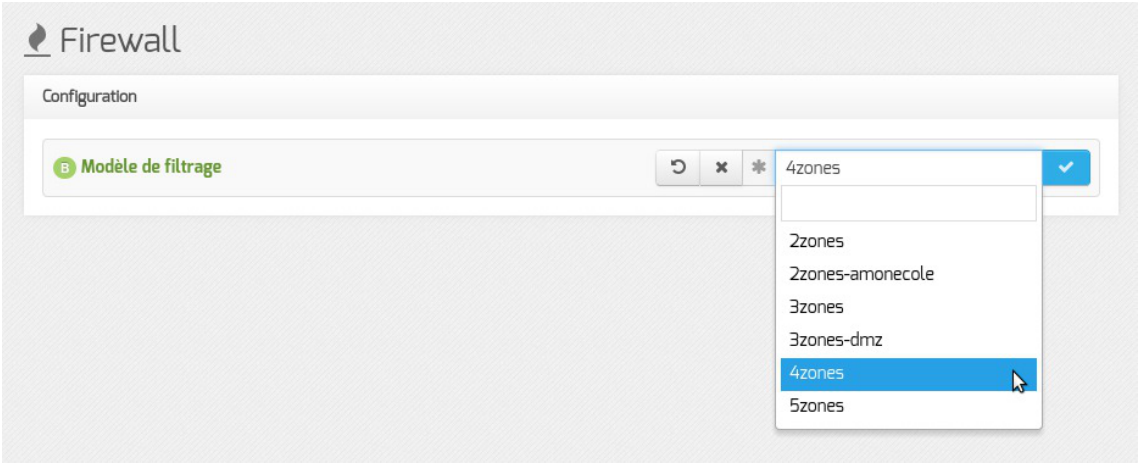


En mode basique seul le service DHCP est activable.

1.3. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.



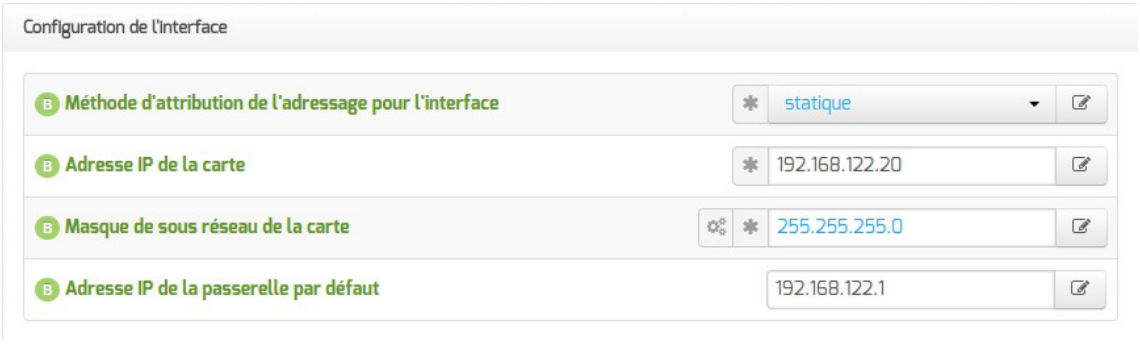
Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

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

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

1.4. Onglet Interface-0

Configuration de l'interface



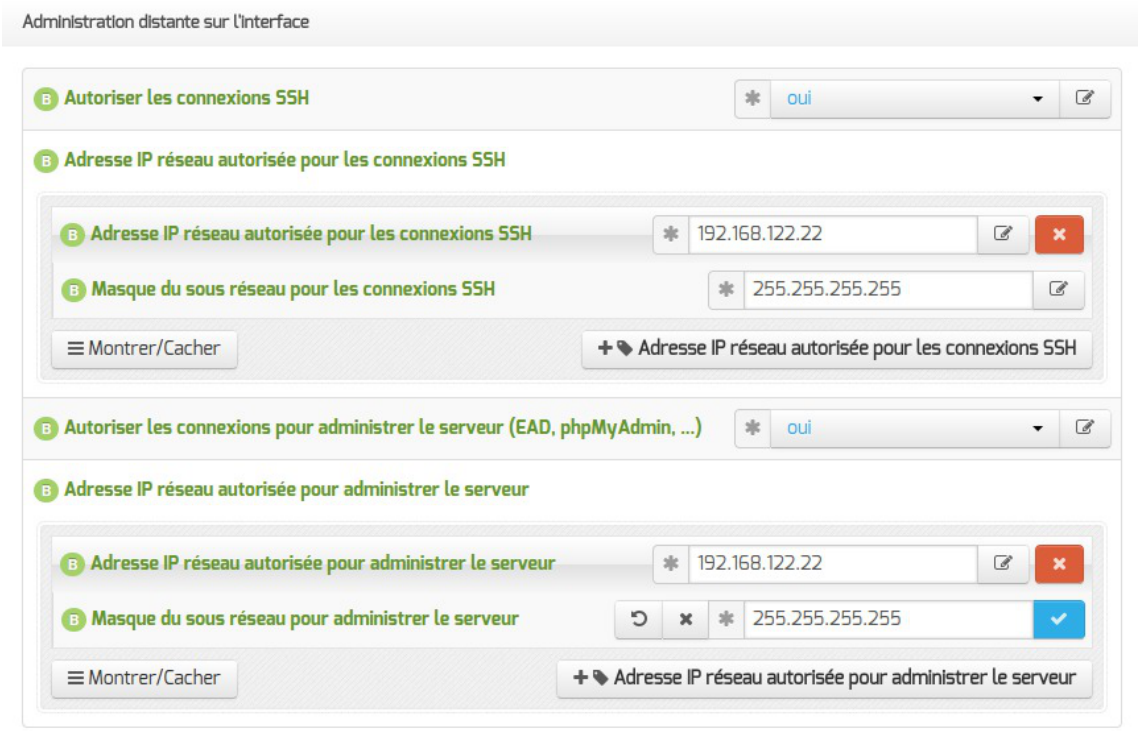
Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.887] et PPPoE[p.898].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

Administration à distance

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

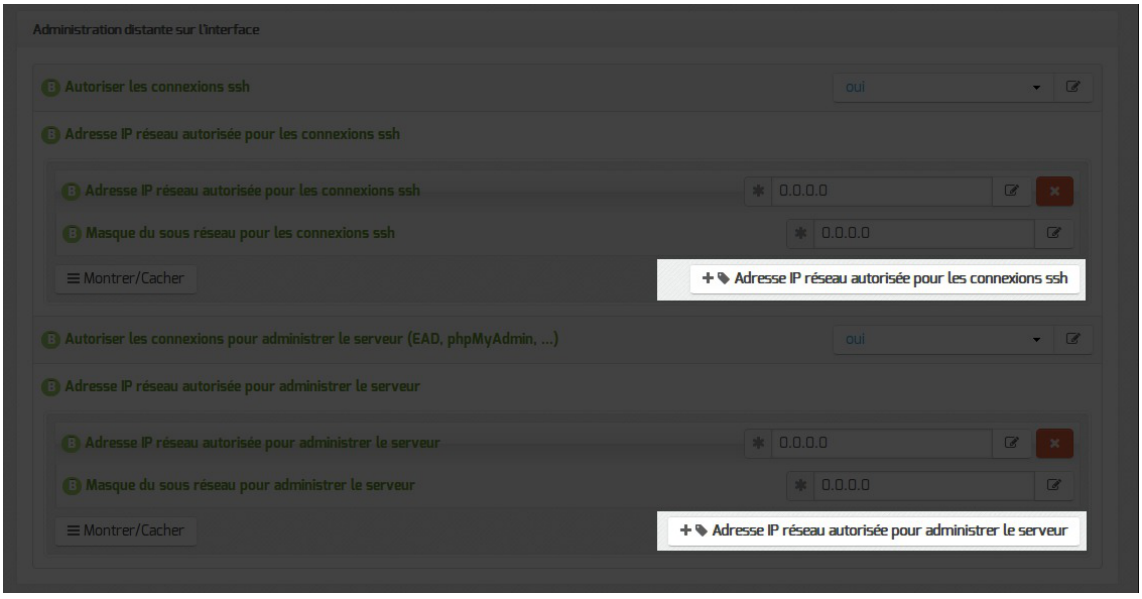


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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.

1.5. Onglet Interface-1

Nombre d'interfaces

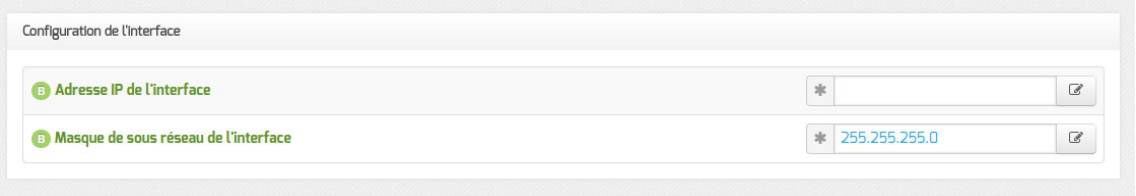
Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

Configuration de l'interface

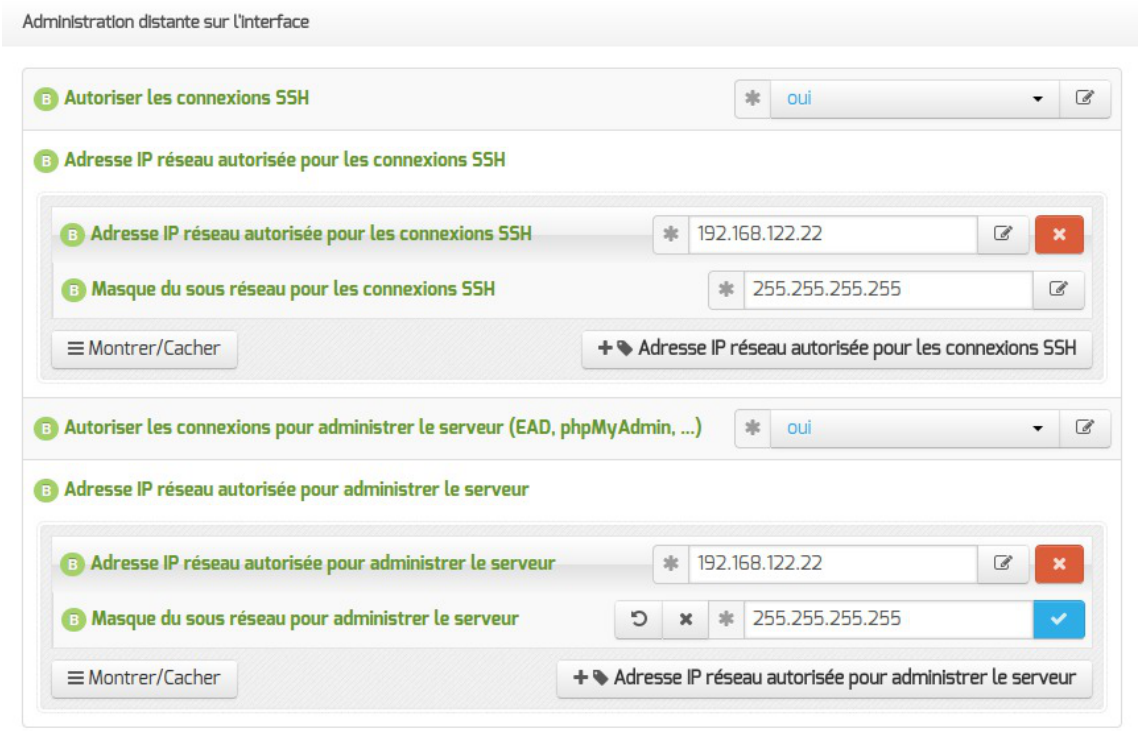


Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau.

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

Administration à distance

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

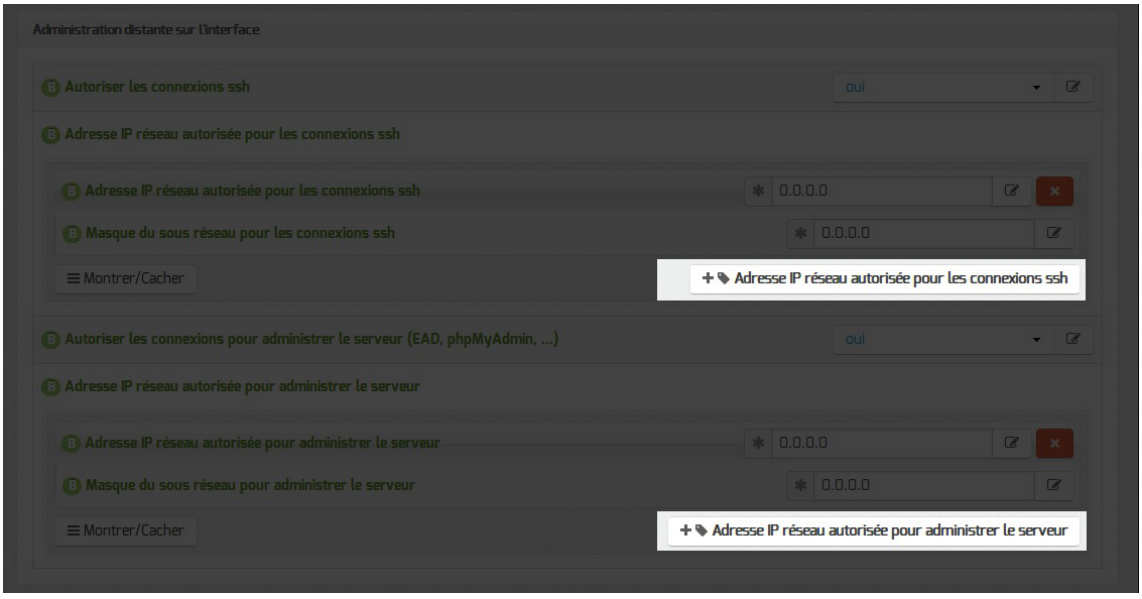


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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

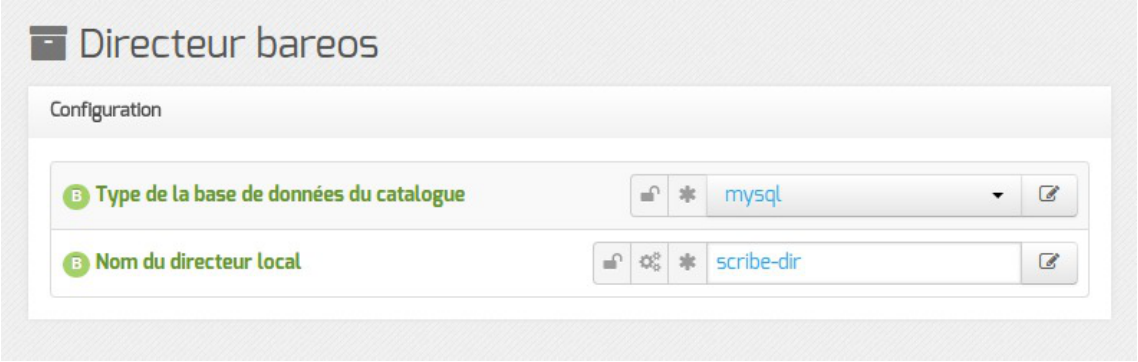
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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.

1.6. 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.

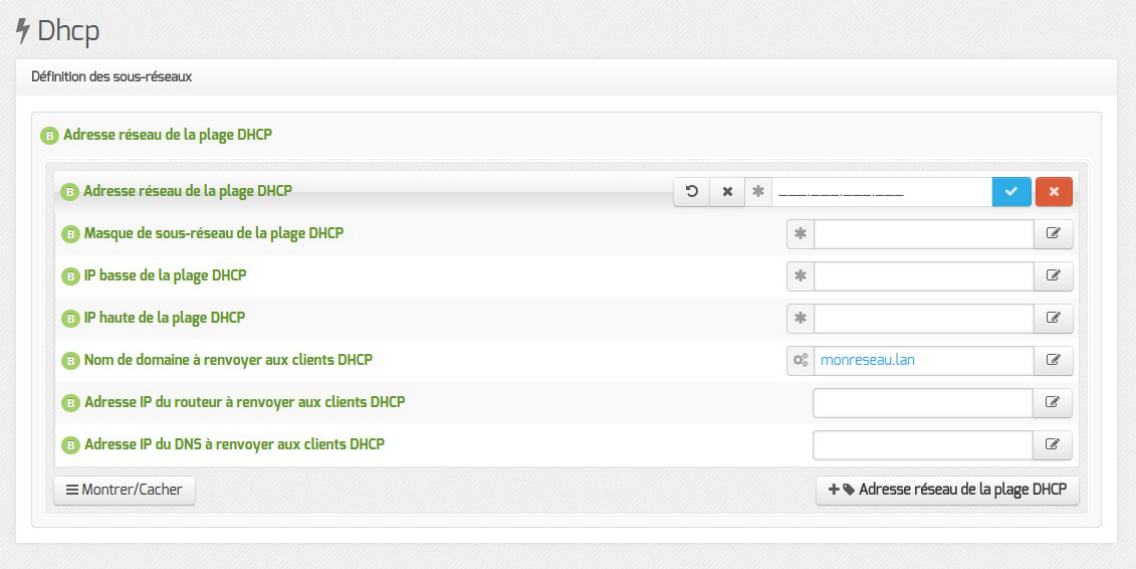
À l'enregistrement du fichier de configuration il ne sera plus possible de modifier le nom du directeur, en effet cette variable est utilisée dans les noms des fichiers de sauvegarde.

1.7. Onglet Dhcp : Configuration du serveur DHCP

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

L'onglet `Dhcp` apparaît uniquement s'il est activé.

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

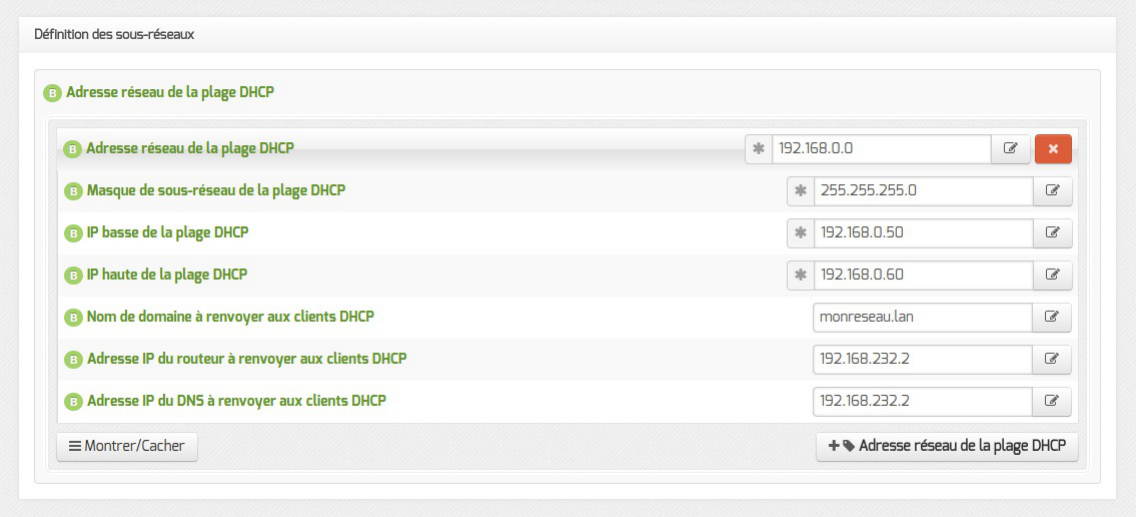


Sur les modules Scribe et Horus (mode une carte), les adresses servies doivent généralement être dans le même réseau que celui de l'Interface-0 (eth0).

Sur le module AmonEcole et ses dérivés, les adresses servies sont celles sur réseau interne (interface `eth1`).

Si le serveur est installé en DMZ, on pourra renseigner des adresses du réseau administratif/pédagogique mais dans ce cas, il faudra activer le relayage du DHCP sur le pare-feu.

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.

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

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

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.889] 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 préférable d'utiliser le module comme relais DNS[p.887], 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.

1.8. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.898]) 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.

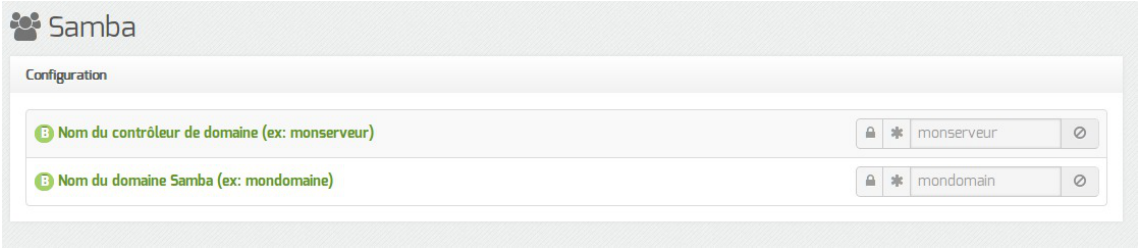
Sur le module Scribe, un professeur aura globalement plus de droits qu'un élève. Il a également à sa disposition des outils lui permettant d'interagir avec les élèves (observation, blocage, distribution de documents, etc.).

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

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



Configuration Samba

Le champ `Nom du contrôleur de domaine` (nom d'ordinateur NetBIOS[p.894]) 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 (*) ;
- 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

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

Fichiers invisibles sur les partages

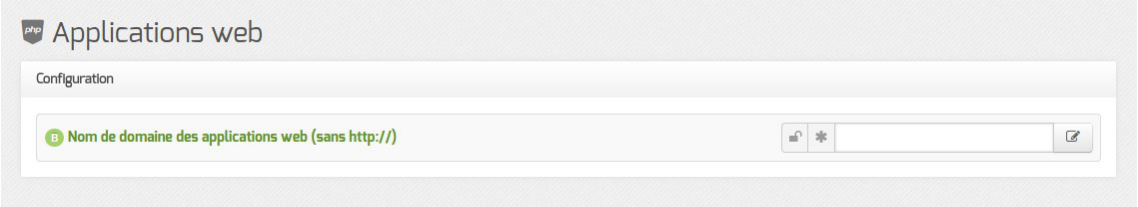
Tous les noms de fichiers commençant par un point sont invisibles dans les partages Windows.

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`) ;
- .scanned:* : si l'anti-virus temps réel est activé, les fichier `.scanned:*` générés par Scannedonly[p.901] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

1.9. Onglet Applications web : Configuration des applications web

L'onglet `Applications web` est disponible par défaut sur le module Scribe. Il est désactivable en passant `Activer le serveur web Apache` à `non`, dans l'onglet `Services`.



L'onglet `Applications web` permet de régler les paramètres essentiels du serveur web Apache.

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

Bien que l'utilisation de l'adresse IP de la carte eth0 soit possible pour une utilisation des applications sur le réseau local du module, il est fortement recommandé d'utiliser un nom de domaine.

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

1.10. Onglet Messagerie

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

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

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

Serveur d'envoi/réception

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.

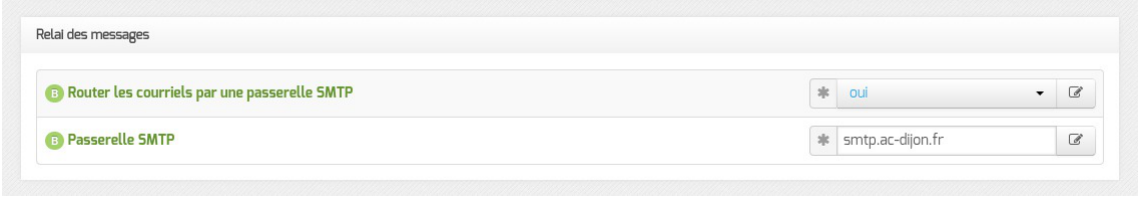


Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

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)

2. Configuration en mode normal

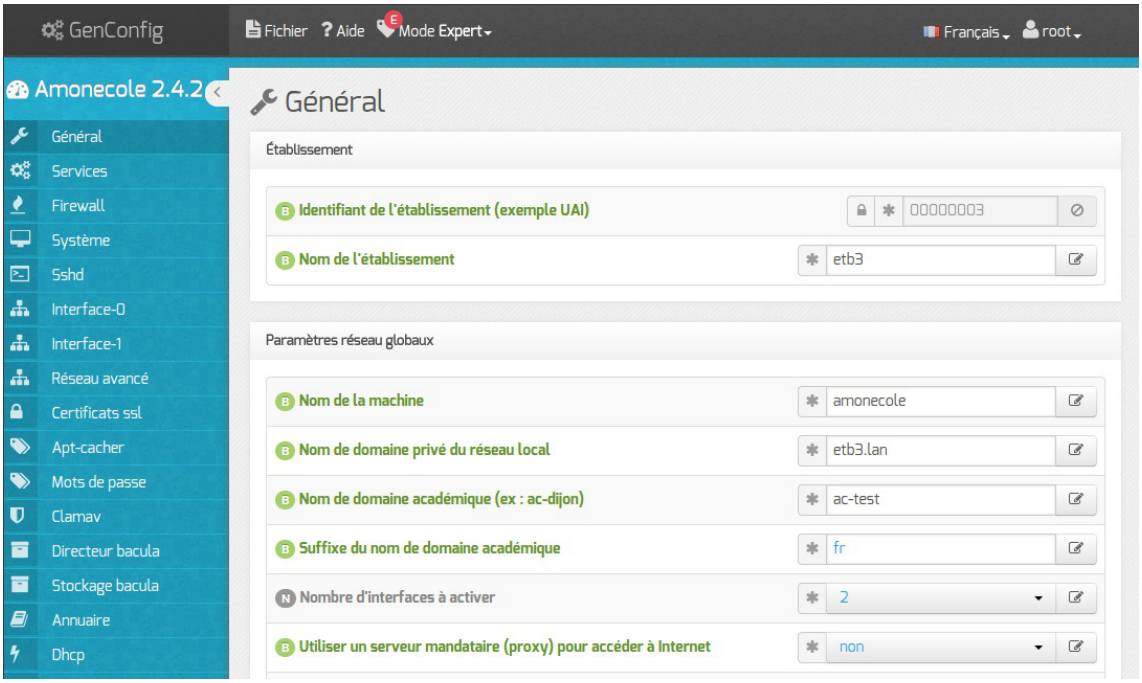
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode normal de l'interface de configuration du module.

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

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Agrégation` * ;
- `Mots de passe` ;
- `Clamav` ;
- `Directeur bareos` ;
- `Stockage bareos` ;
- `Annuaire` ;
- `Dhcp` * ;
- `Esu` ;
- `Samba` ;
- `Onduleur` * ;
- `Rvp` * ;
- `Applications web` ;
- `Eole sso` ;
- `Messagerie` ;
- `Authentification` ;
- `Proxy authentifié` ;
- `Proxy authentifié 2` ** ;
- `Exceptions proxy` ;
- `Reverse proxy` * ;
- `Freeradius` *.

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.

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

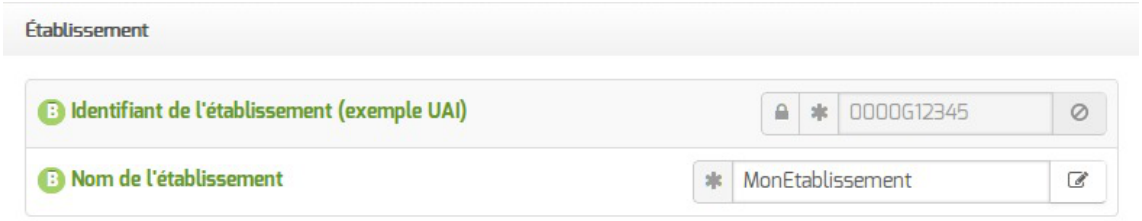


Vue générale de l'interface de configuration du module

2.1. Onglet Général

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

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

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

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

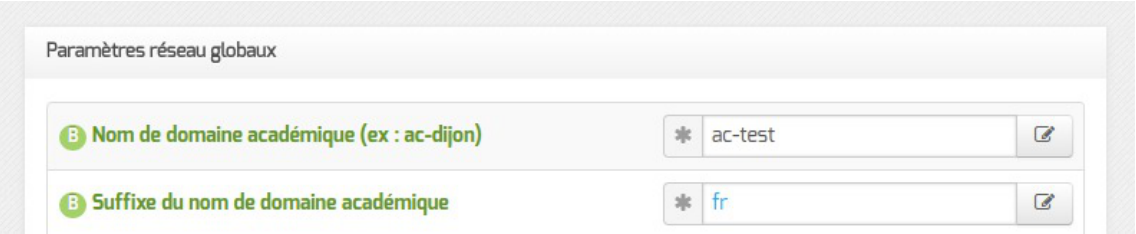
Sur les modules fournissant un annuaire LDAP[p.892] local, ces variables sont utilisées pour créer l'arborescence.



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

Paramètres réseau globaux

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



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

Cette information est découpée en plusieurs champs :

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

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

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

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

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

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

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

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

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

Proxy

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



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

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

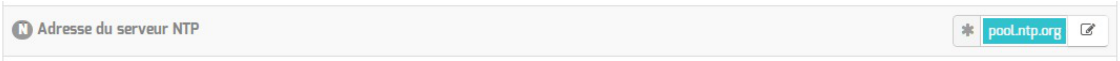
DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.887].

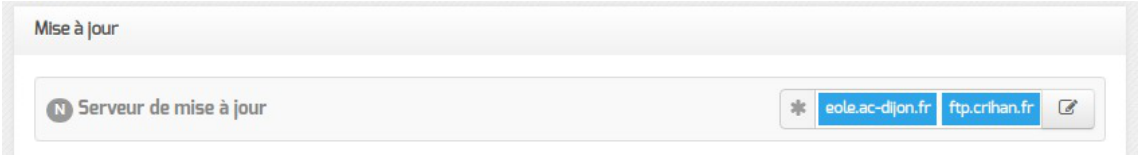
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.895]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour



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

Voir aussi...

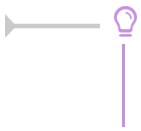
- Onglet Interface-n
- Les différents types de mises à jour

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

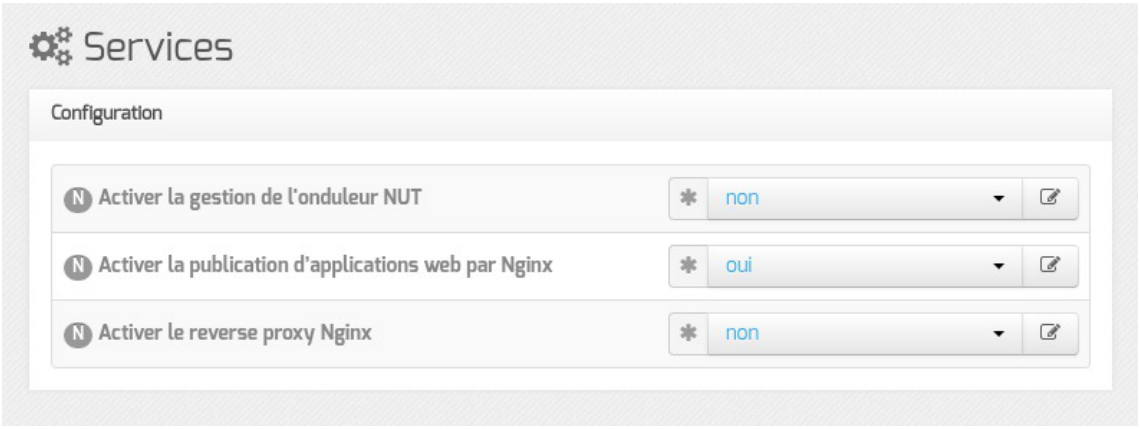
2.2. Onglet Services

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

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



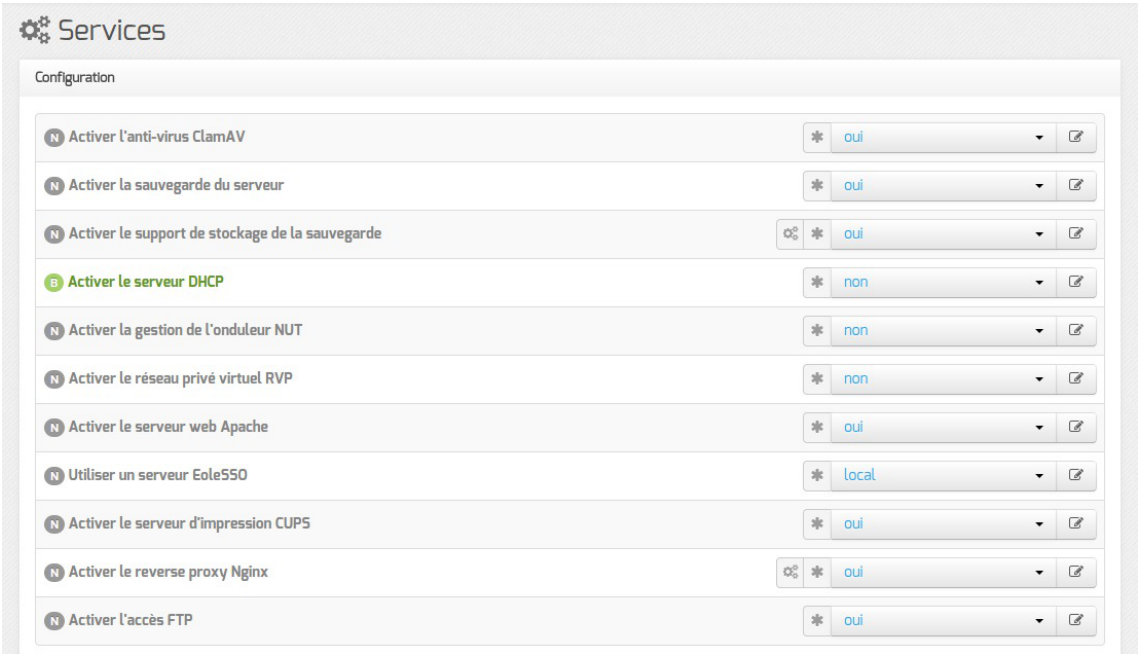
Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un onglet de configuration propre au service.



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.895].

En mode normal la liste des services activables ou désactivables est beaucoup plus conséquente.



Vue de l'onglet Services en mode normal

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

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

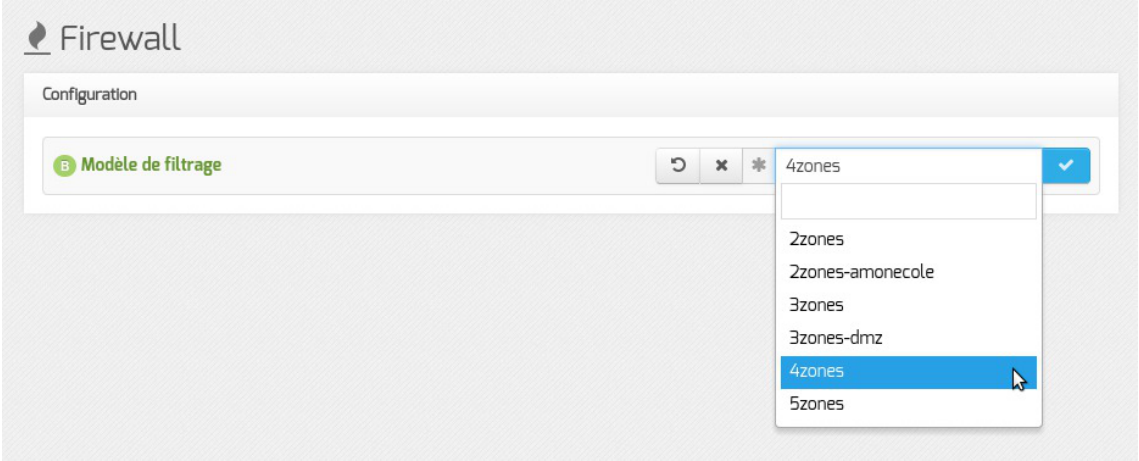
Les services de base propres au module AmonEcole sont les suivants :

- l'anti-virus ClamAv ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le réseau privé virtuel RVP ;
- le serveurs web ;
- le serveur d'authentification unique EoleSSO ;
- le serveur d'impression avec CUPS ;
- le proxy inverse Nginx ;
- l'accès FTP.

2.3. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

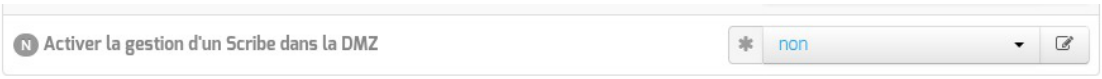
- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

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

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.884] des règles propres à la DMZ[p.887].



Si l'on souhaite mettre en place l'architecture suivante avec Amon :

- un réseau administratif ;
- un réseau pédagogique ;
- une DMZ contenant un serveur Scribe hébergeant des services web à ouvrir depuis l'extérieur.

La configuration recommandée sera :

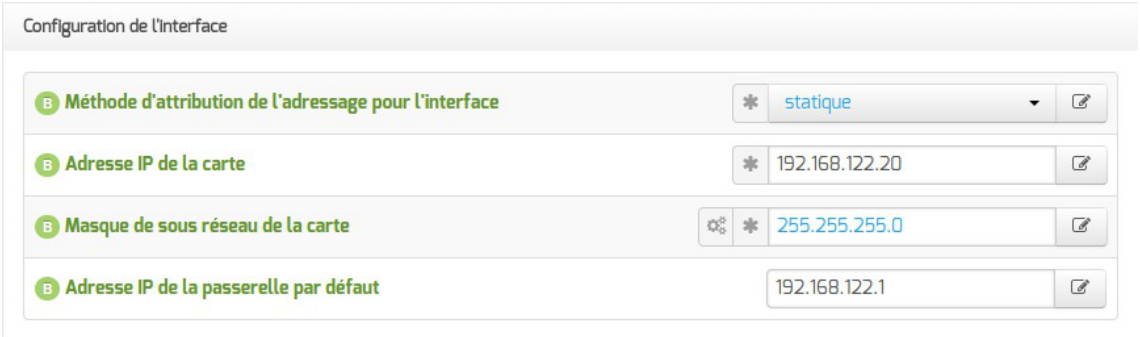
- `Nombre d'interfaces à activer` : `4` (onglet `Général` en mode basique) ;
- `Modèle de filtrage` : `4zones` (onglet `Firewall` en mode basique) ;
- `Activer la gestion d'un Scribe dans la DMZ` : `oui` (onglet `Firewall` en mode normal).

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ

2.4. Onglet Interface-0

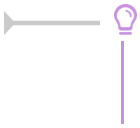
Configuration de l'interface



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

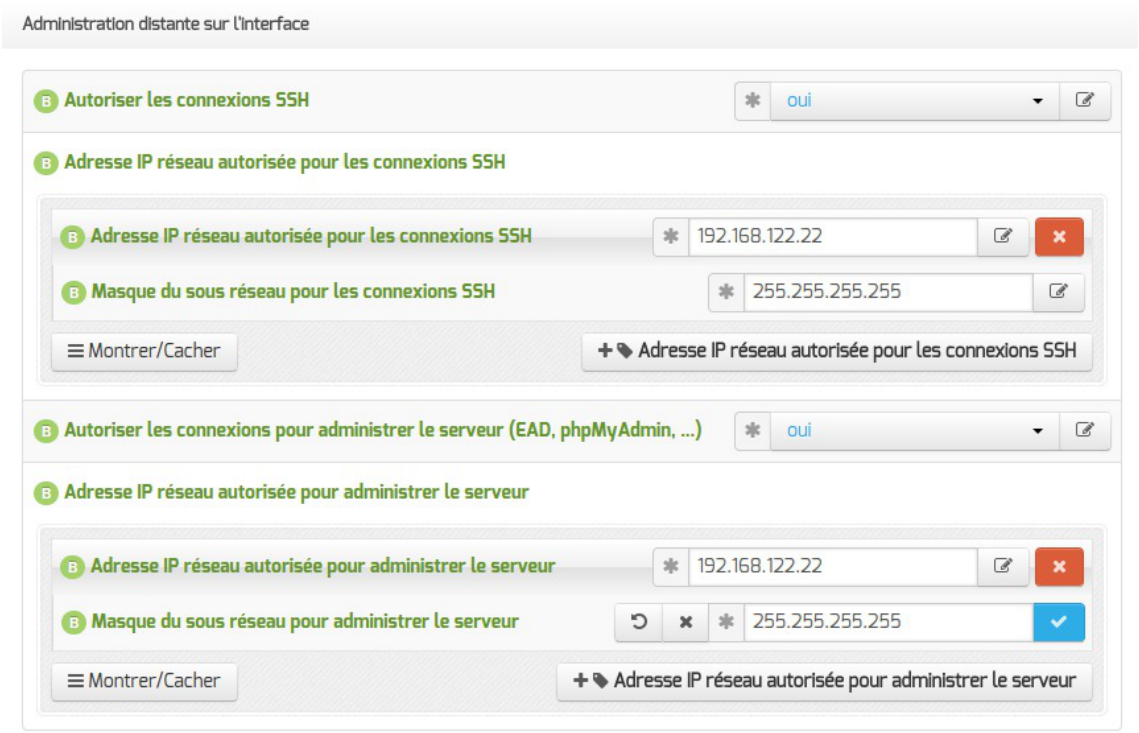
Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.887] et PPPoE[p.898].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.



EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

Administration à distance



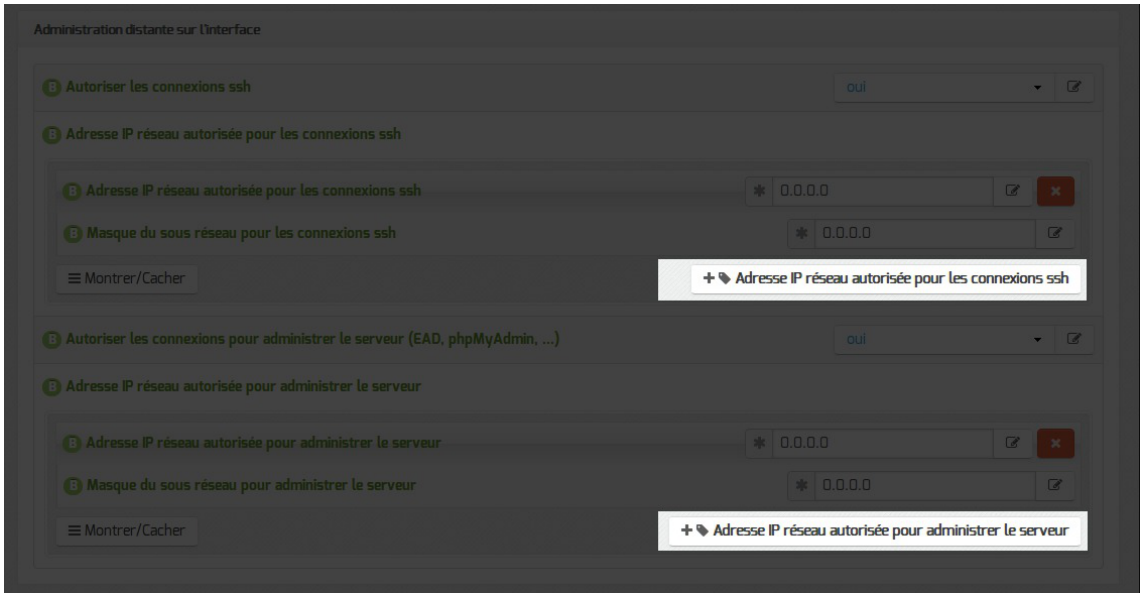
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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

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



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

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

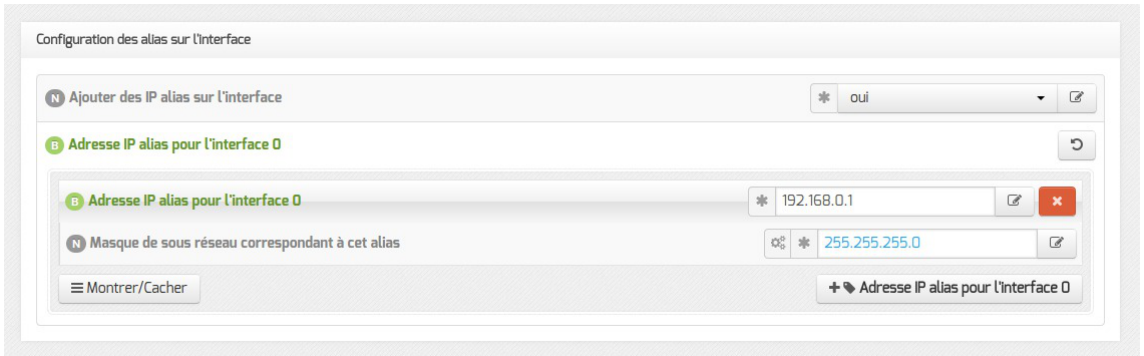
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

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

Configuration des alias sur l'interface

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



Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et

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

configurer l'adresse IP et le masque de sous réseau.

Si l'agrégation de liens est activée. Il faut obligatoirement configurer une passerelle particulière pour cet alias.

Agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.



Un nouvel onglet, `Agrégation`, est disponible.

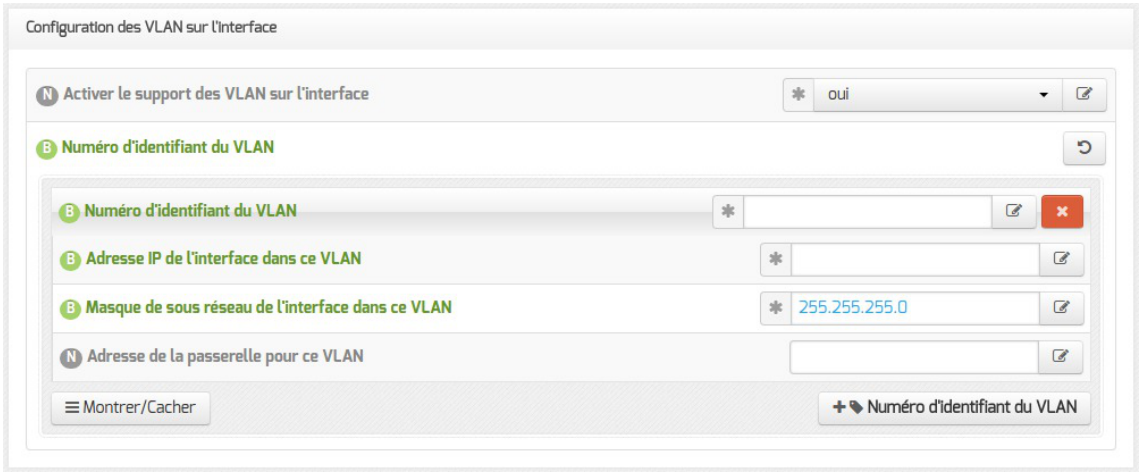


Si l'agrégation de liens est activée il faut obligatoirement configurer une passerelle particulière pour l'alias activé dans la rubrique `Configuration des alias sur l'interface`.



Configuration des VLAN sur l'interface

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



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

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

configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).
Il est possible de configurer une passerelle particulière pour ce VLAN.

Voir aussi...

> Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.60]

2.5. Onglet Interface-1

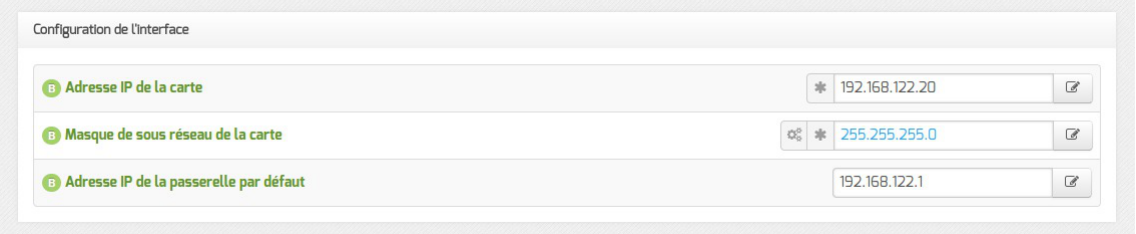
Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.
Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.



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

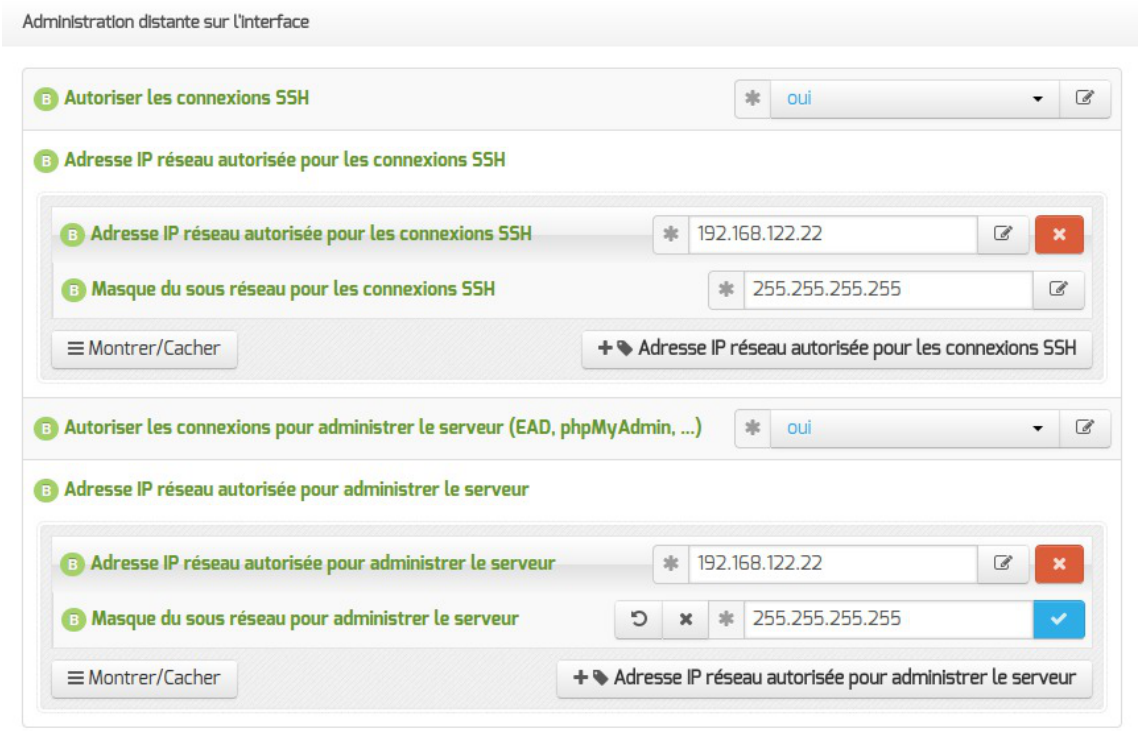
Configuration de l'interface



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)

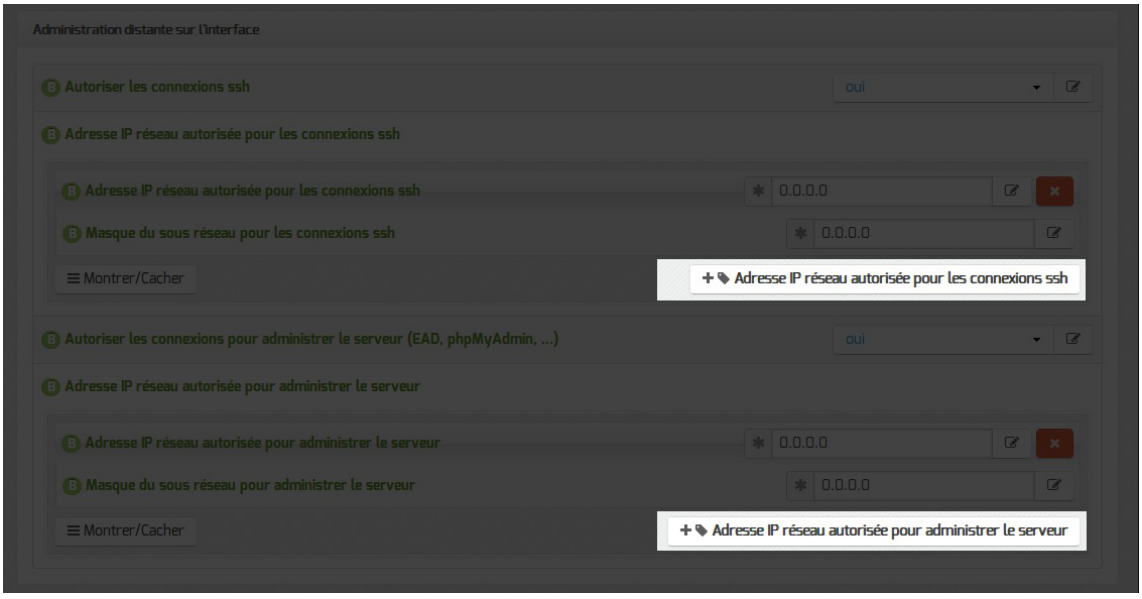


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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)

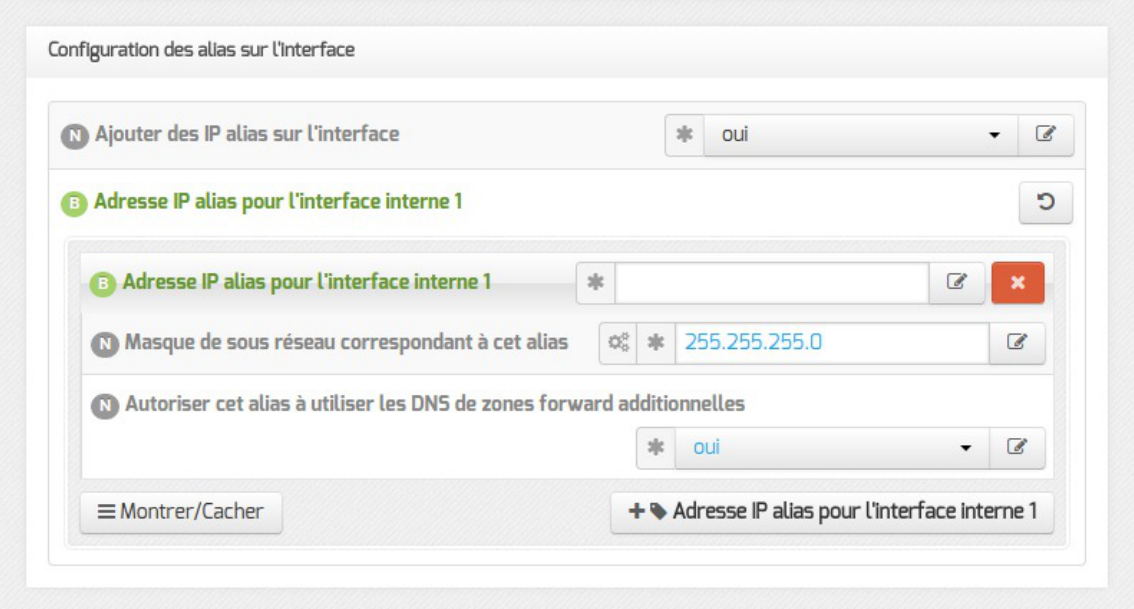
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

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

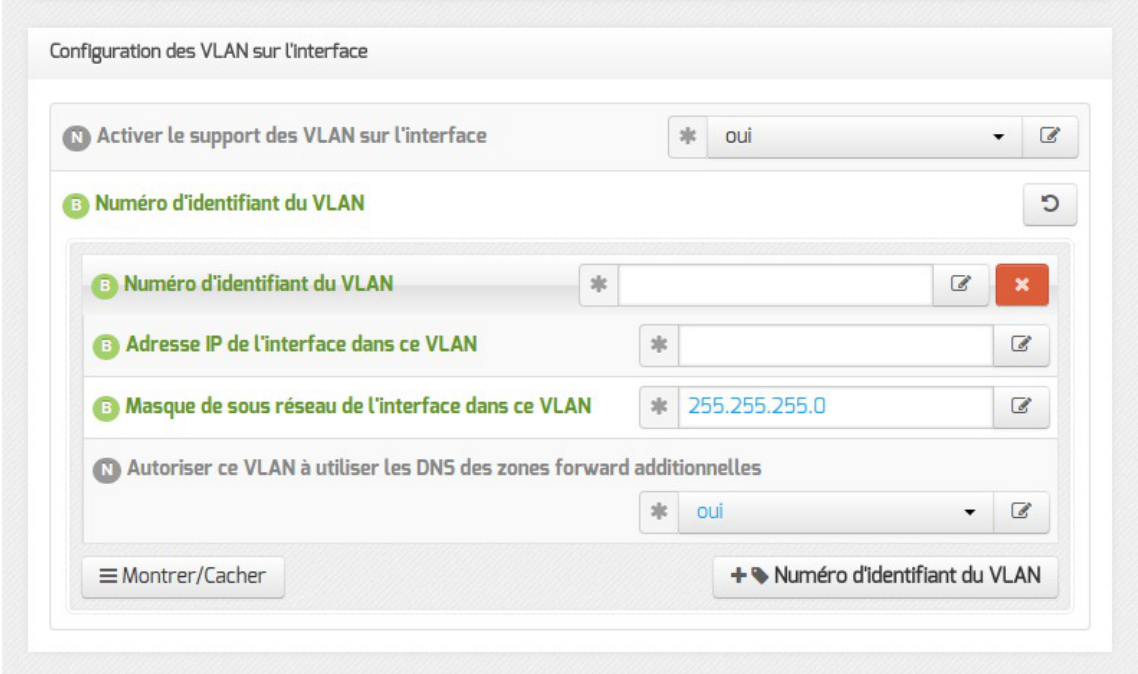
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

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

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



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

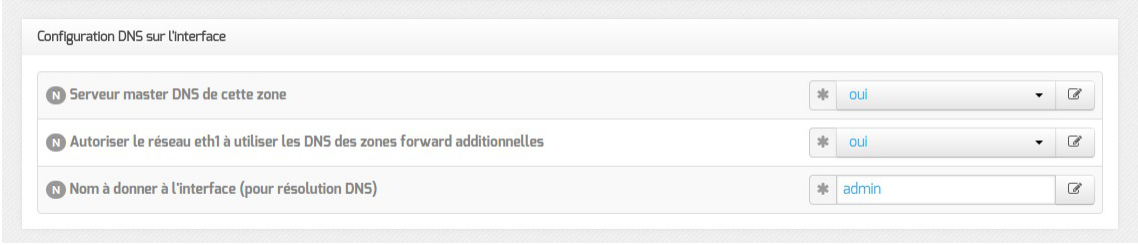
`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward`

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

`additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

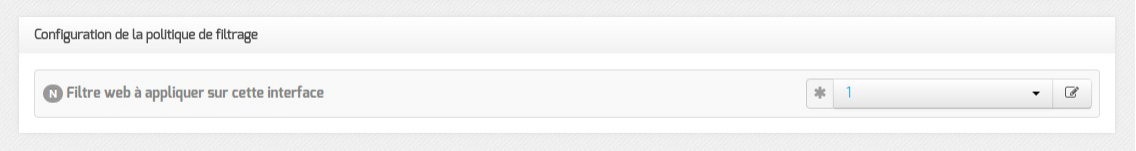
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

> Onglet Filtrage web : Configuration du filtrage web [p.209]

2.6. Onglet Interface-n

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

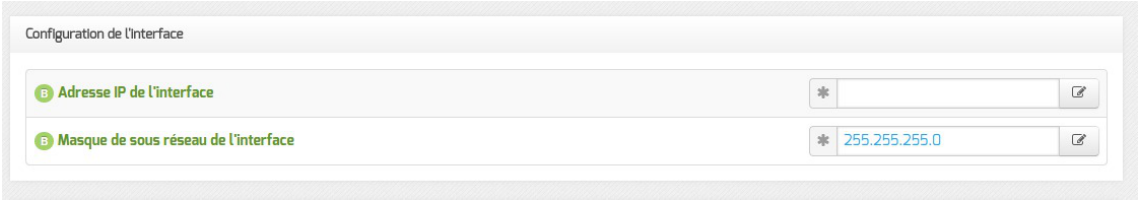
Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.



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

Configuration de l'interface

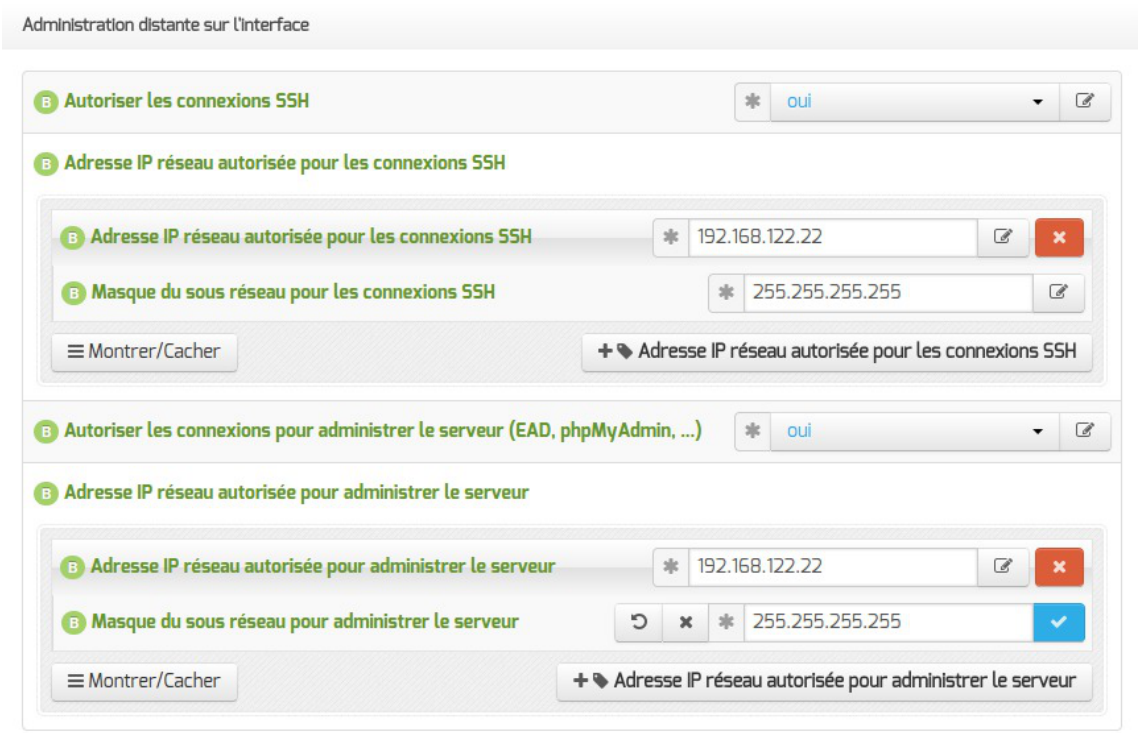
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

Administration à distance



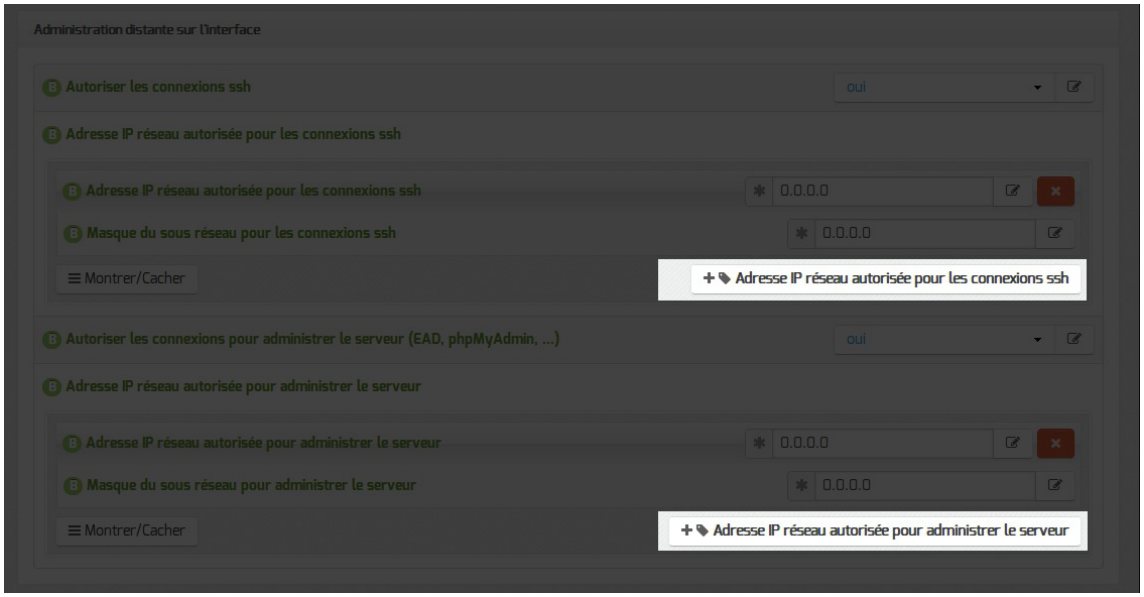
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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

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



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

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

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

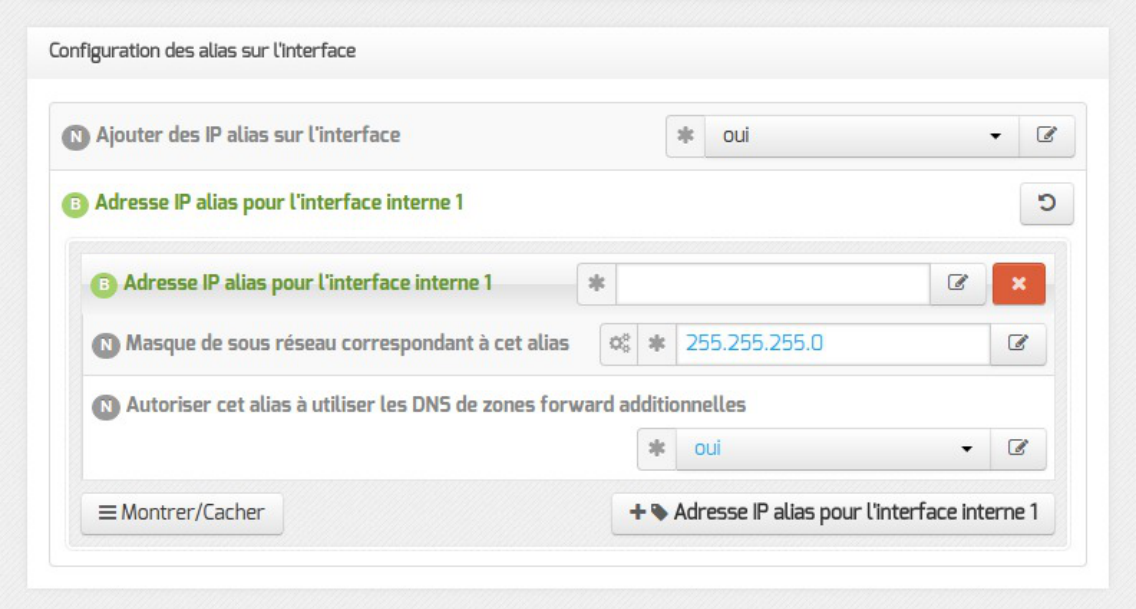
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`

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

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

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

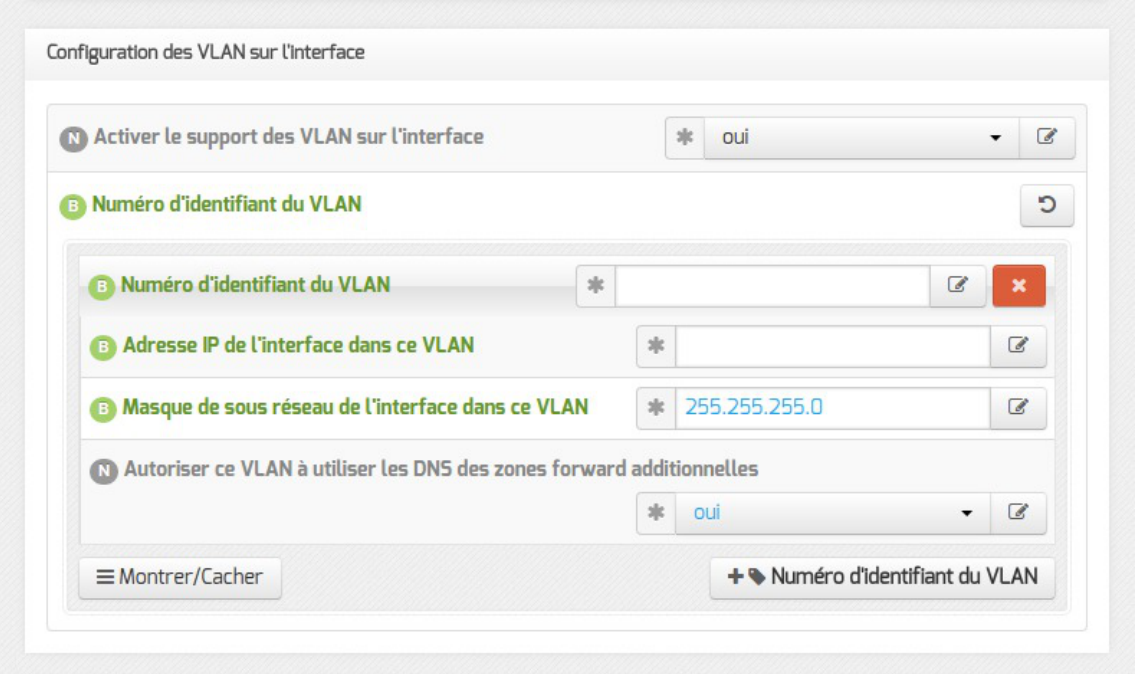
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (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 son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

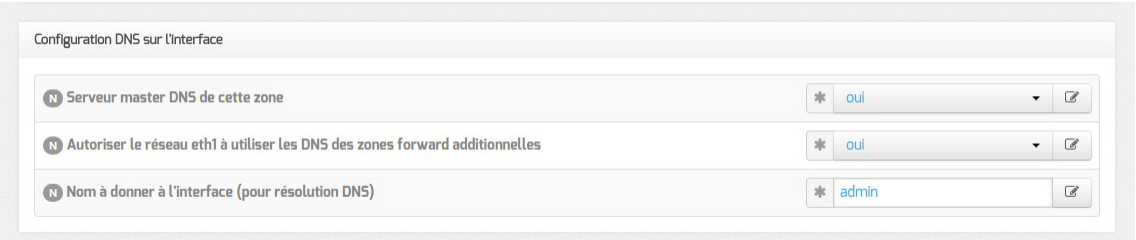
`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

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

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

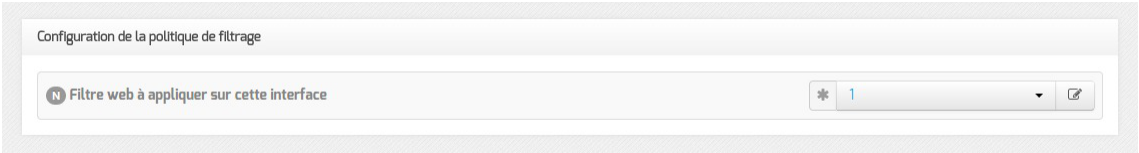
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.209]

2.7. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité

Présentation et mise en place de l'agrégation de liens

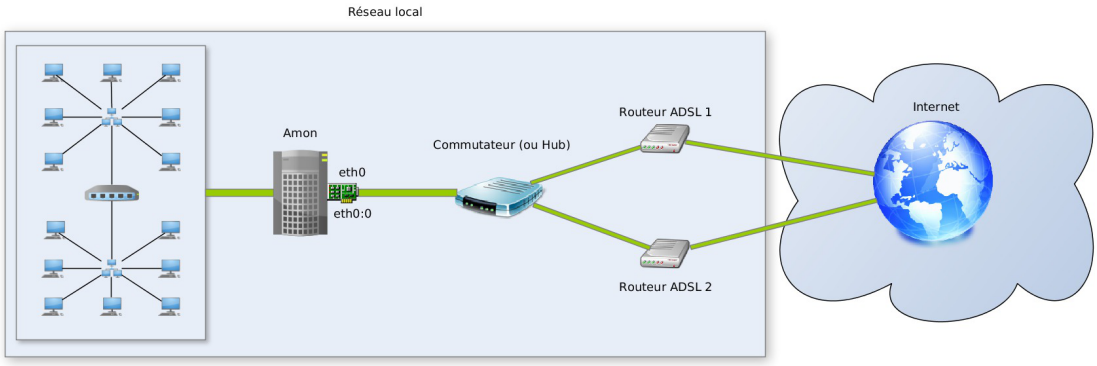
L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Les deux routeurs sont reliés entre eux par un commutateur (ou un Hub) à la carte eth0 du module Amon.

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP [p.899] et OSPF [p.896] ;
- il faut un service qui surveille l'état de chacun des liens.

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



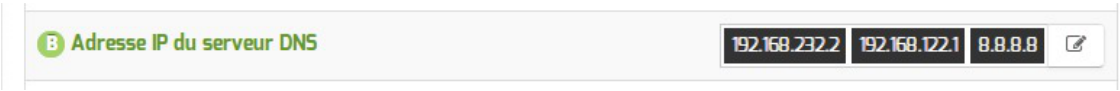
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie.

La première version a été réalisée par l'académie de Versailles, puis elle a été améliorée successivement par les académies de Nantes et de Lyon.

Onglet Général

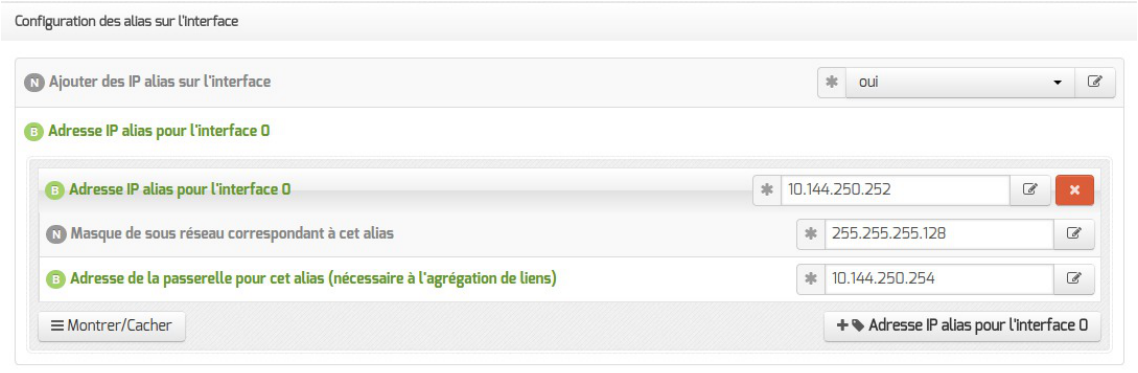
Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

Il faut, en premier lieu, déclarer un alias sur l'interface eth0 dans la section `Configuration des alias sur l'interface`.

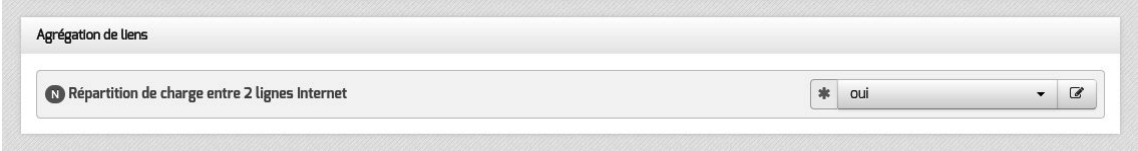
Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



Création d'un alias sur eth0 pour l'agrégation de liens

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

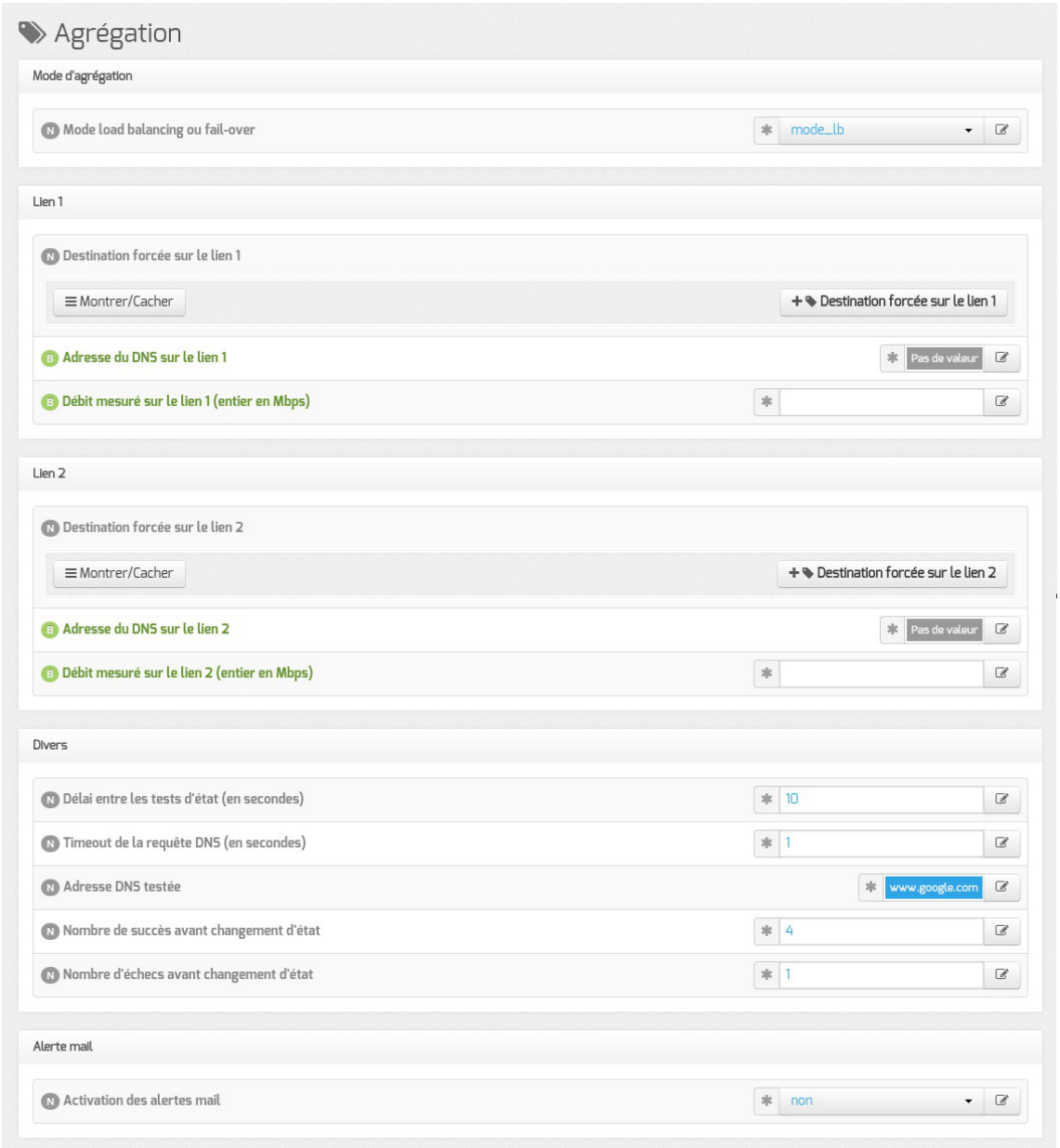
L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.



Un nouvel onglet, `Agrégation`, est disponible.

Onglet Agrégation : Configuration de l'agrégation de liens

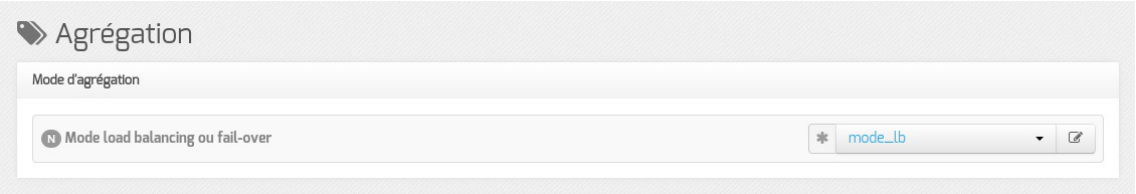
Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.



Paramétrage de l'agrégation de liens

Modes d'agrégation

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



Il existe deux modes d'agrégation :

- le mode `mode-lb` (pour load balancing) correspond à la répartition de charge et fonctionne avec la notion de poids à utiliser sur les différentes passerelles ;
- le mode `mode-fo`, (pour fail-over) un seul lien est utilisé à la fois, il n'y a plus de notion de poids et il n'y a plus qu'une seule route par défaut.

Dans les deux modes il est possible de forcer des destinations IP ou réseau, et dans les deux cas si un lien tombe tous les flux (et également les destinations forcées) sont redirigés vers le second lien.

Quand les deux liens sont fonctionnels, on se retrouve dans la configuration de départ.



Le VPN, de par son mode de fonctionnement, ne peut pas être réparti entre plusieurs abonnements.

Tout le trafic devant passer par un seul lien, il est nécessaire d'utiliser le mécanisme de destination forcée.

Que le `Lien 1` ou le `Lien 2` soit choisi pour faire transiter le VPN, s'il devient indisponible, le VPN ne fonctionnera plus.

Adresse des DNS

Les champs `Adresse du DNS sur le lien 1` et `Adresse du DNS sur le lien 2` sont des champs obligatoires pour le bon fonctionnement de l'agrégation.



Les adresses DOIVENT être différentes sur chaque lien car c'est avec ces DNS que se font les tests d'état des liens.

Adresse DNS testée

Il est possible de spécifier plusieurs mires de tests qui seront testées afin de déterminer l'état des liens (résolution DNS avec le serveur DNS de chacun des liens).



L'ensemble des DNS doit être déclaré dans l'onglet `Général`.

Alerte mail

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

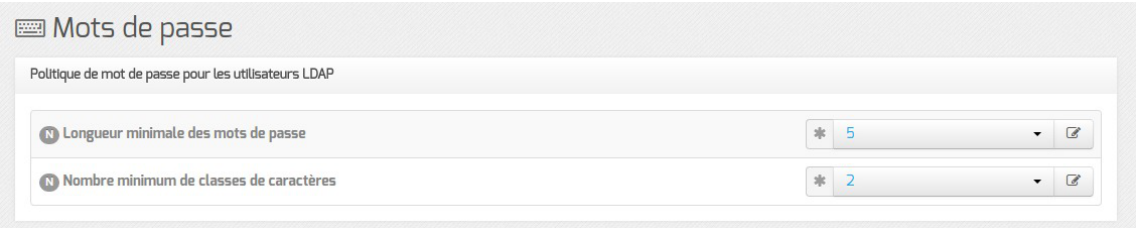


Lorsque l'un des liens est coupé, le message suivant est envoyé : `Seul le lien 2 est actif, redirection des flux sur ce lien`.

Quand les deux liens sont de nouveaux fonctionnels, le message suivant est envoyé : `Rechargement de la répartition sur les 2 liens`.

2.8. 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.



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 sera à terme propagée à toutes les interfaces fournissant cette fonctionnalité (EAD, portail...). 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.885] 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.

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

2.9. 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

L'onglet `Clamav` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer l'anti-virus ClamAV` à `oui`.

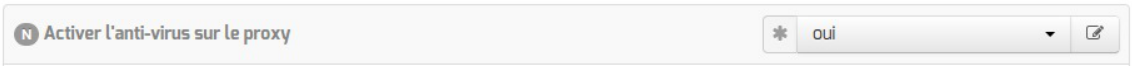
Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.



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 le proxy

Pour activer l'anti-virus en temps réel sur les fichiers filtrés par le proxy Internet, il faut passer la variable `Activer l'anti-virus sur le proxy` à `oui` dans l'onglet `Clamav`.

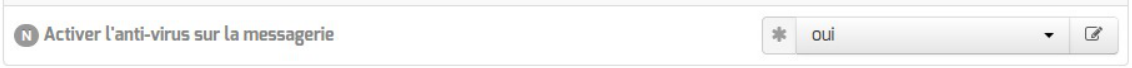


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.886]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

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`.



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

Contribuer

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

Il est possible de faire des signalements :

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

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

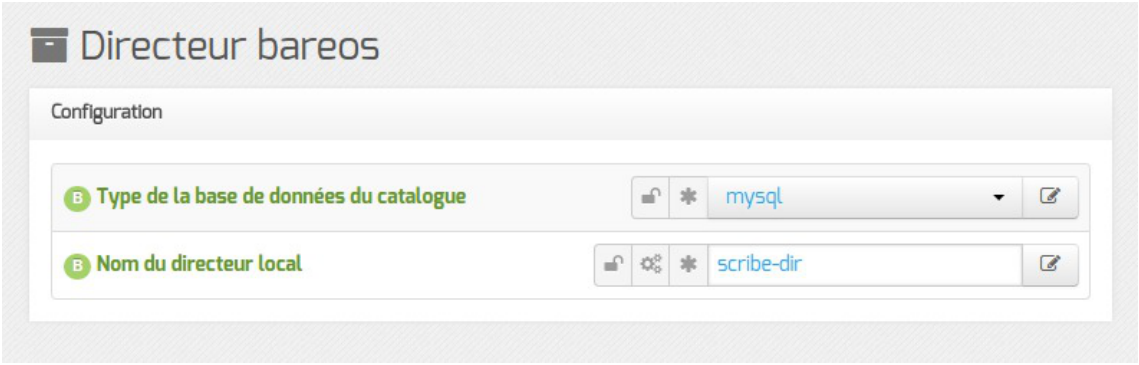
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

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

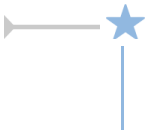


Il ne faut pas signaler des PUA[p.899] comme étant des faux positifs.

2.10. 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.

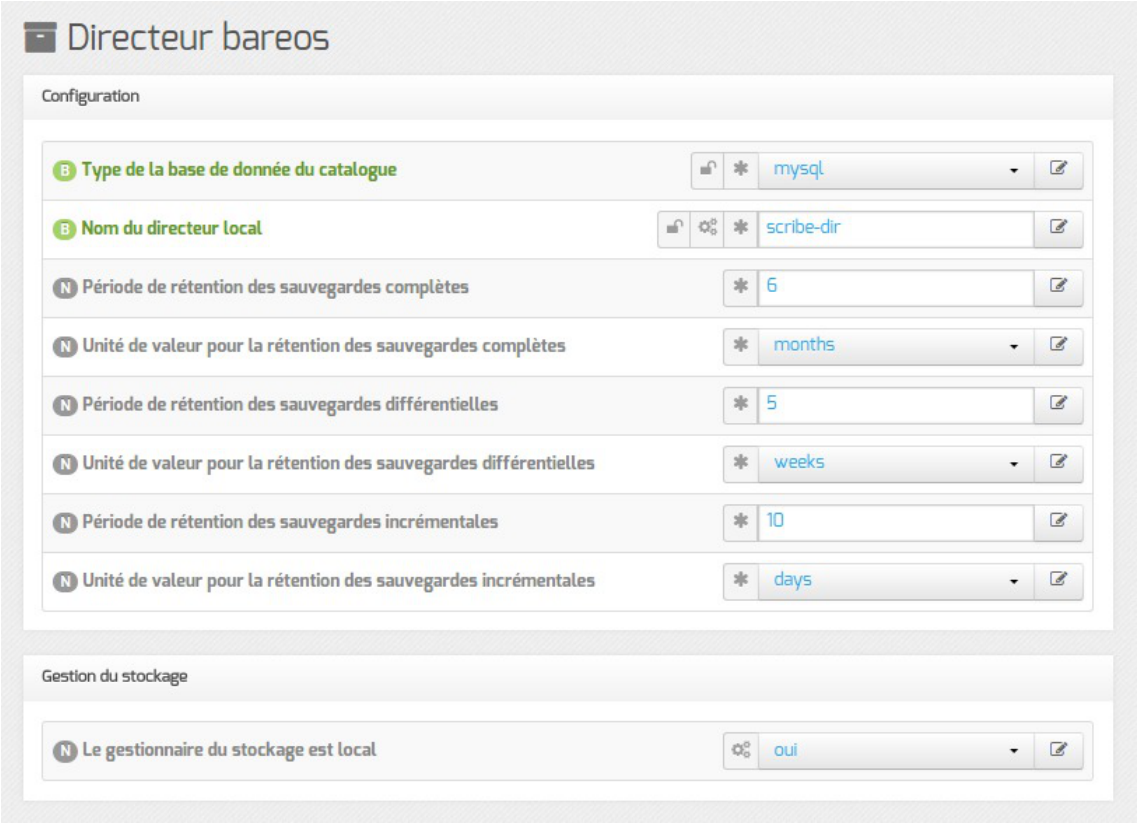


Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

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.888] 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.

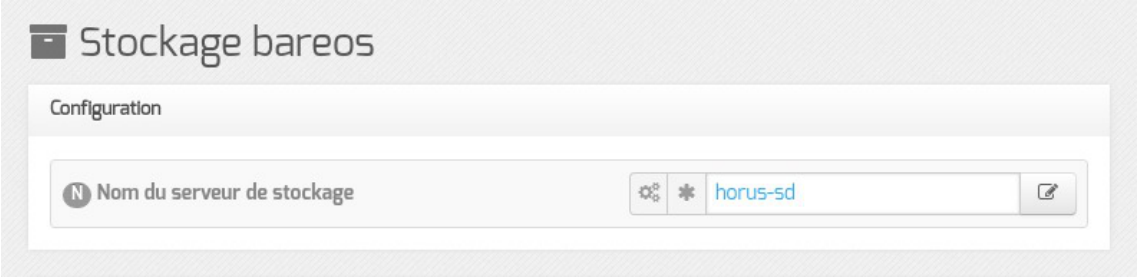
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

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)

2.11. Onglet Stockage bareos

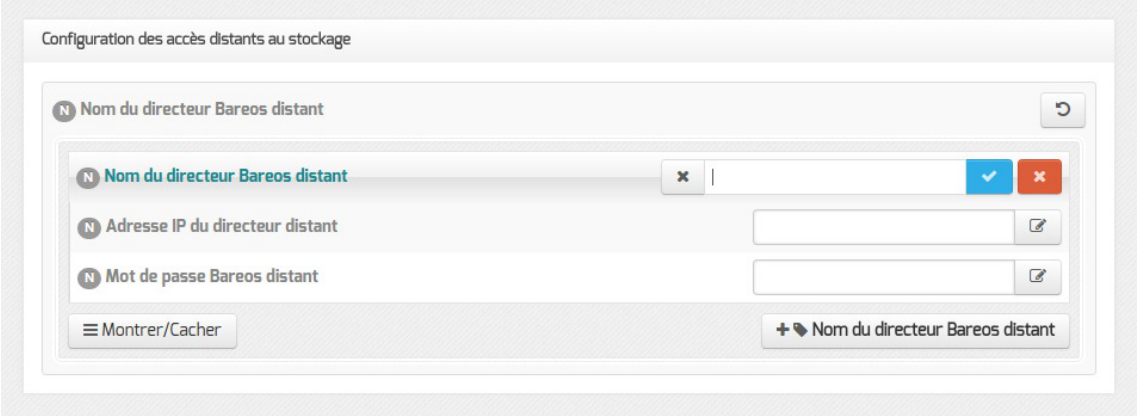
Dans l'onglet `Stockage bareos` il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



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.

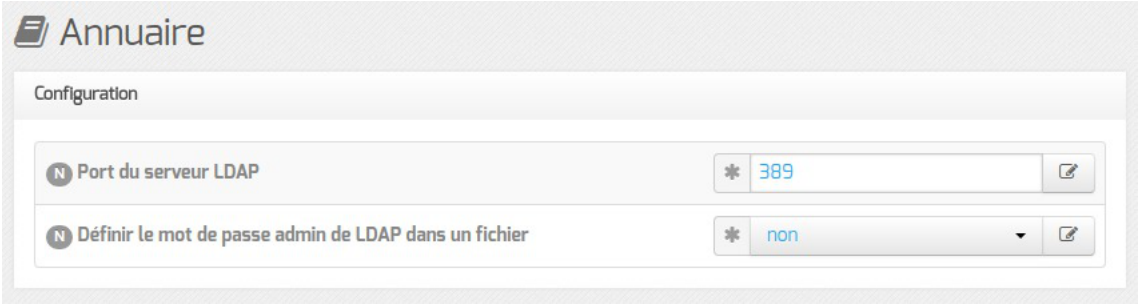
Voir aussi...

Les mots de passe

2.12. Onglet Annuaire

Sur le module Scribe l'annuaire OpenLDAP est local.

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



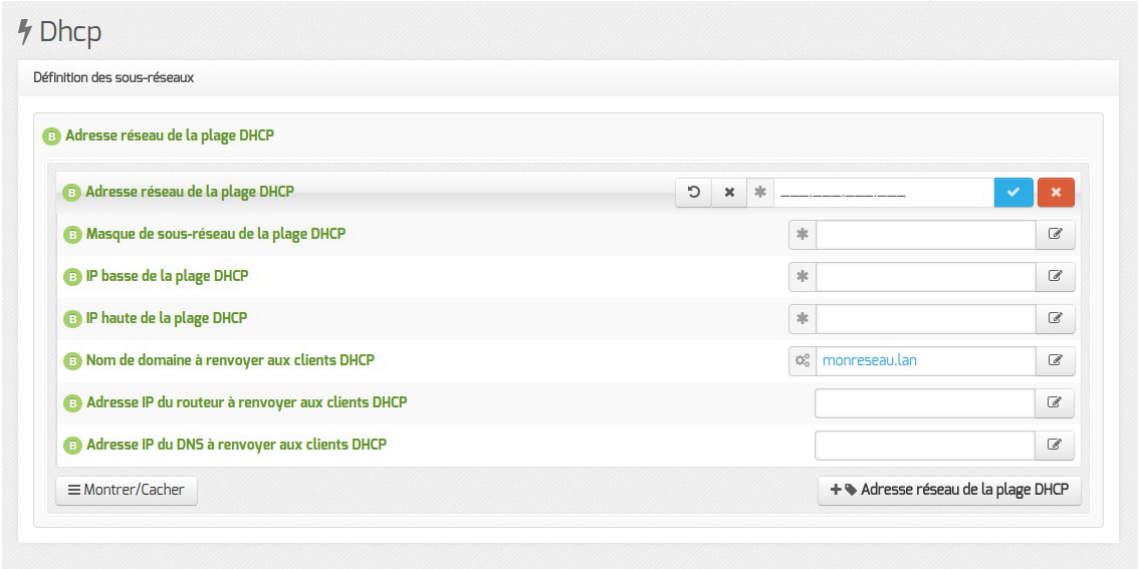
Lorsque l'annuaire est configuré comme étant local, l'onglet propose 2 paramètres :

- `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`.

2.13. Onglet Dhcp : Configuration du serveur DHCP

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

L'onglet `Dhcp` apparaît uniquement s'il est activé.



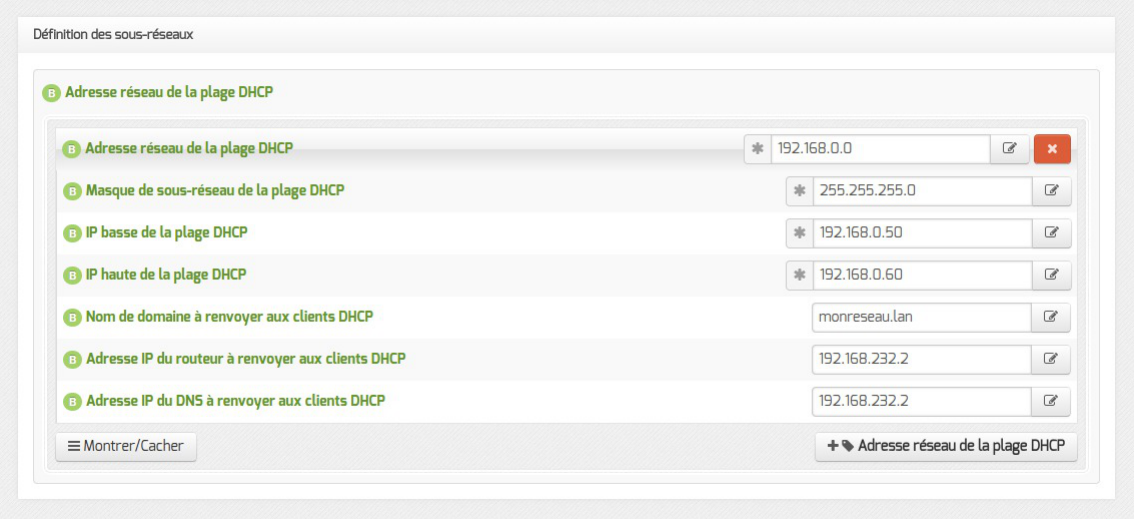
Sur les modules Scribe et Horus (mode une carte), les adresses servies doivent généralement être dans le même réseau que celui de l'Interface-0 (eth0).

Sur le module AmonEcole et ses dérivés, les adresses servies sont celles sur réseau interne (interface `eth1`).

Si le serveur est installé en DMZ, on pourra renseigner des adresses du réseau administratif/pédagogique mais dans ce cas, il faudra activer le relayage du DHCP sur le pare-feu.

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.

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.889] 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 préférable d'utiliser le module comme relais DNS[p.887], 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

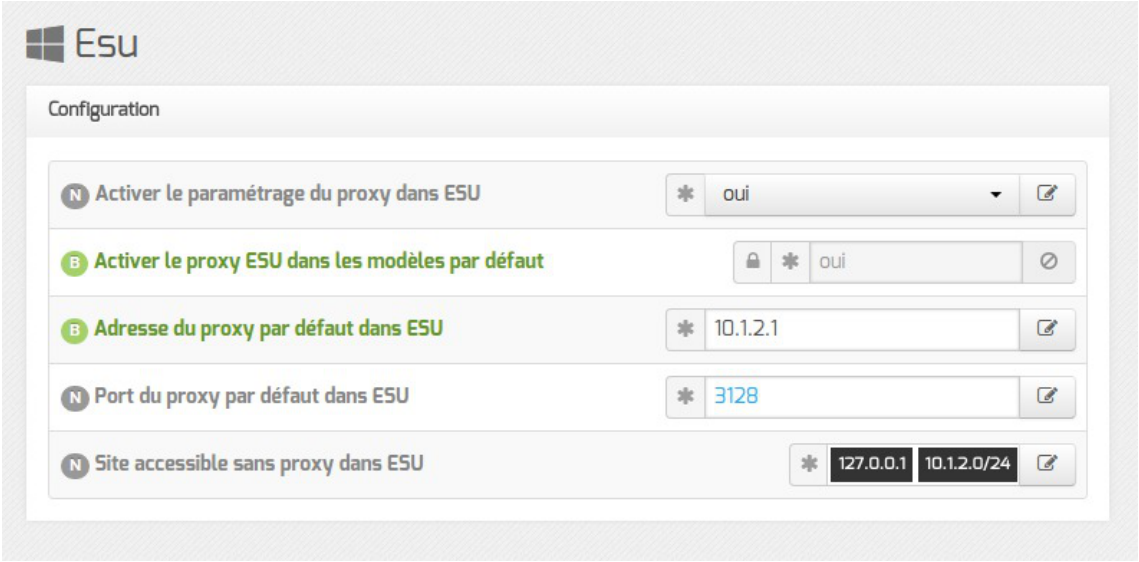
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Interface-1 de l'interface de configuration du module.

2.14. 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.



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 varibles 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

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

`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`).

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.882] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG[p.882] tels que celui fourni par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

2.15. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.898]) 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.).

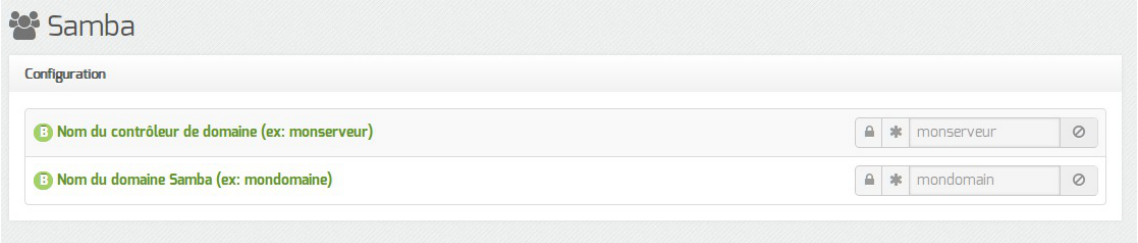
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

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

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

Le champ `Nom du contrôleur de domaine` (nom d'ordinateur NetBIOS[p.894]) 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 (*) ;
- 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`

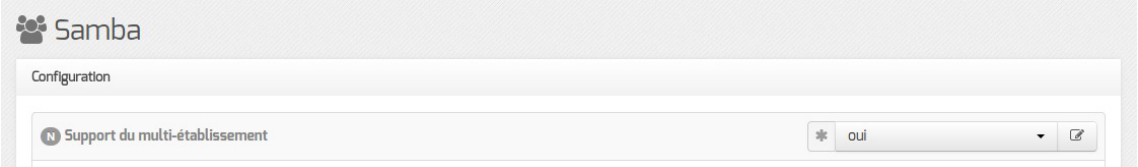
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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.901] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

Mode multi-établissement

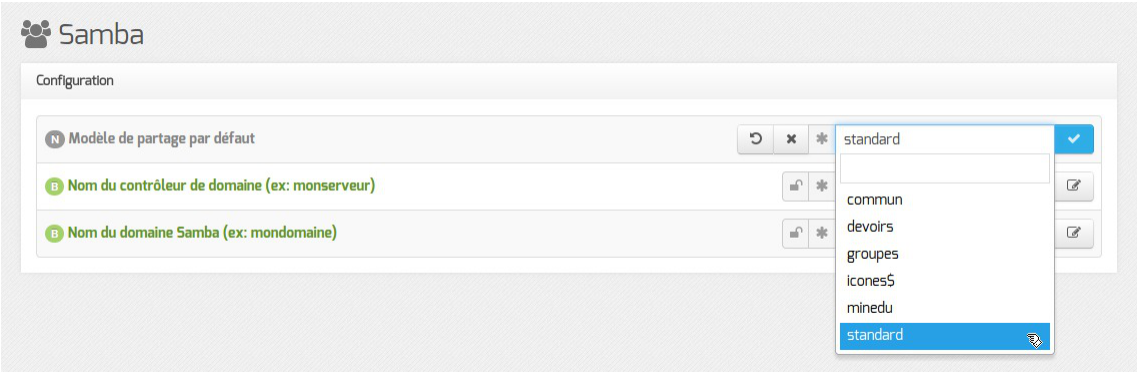
Pour certaines structures, une communauté de communes par exemple, il peut être intéressant de n'avoir qu'un seul module Scribe ou AmonEcole pour gérer plusieurs établissements.



Activation du mode multi-établissement dans l'interface de configuration du module

Pour activer le support du **mode multi-établissement** il faut passer la variable `Support du multi-établissement` à `oui` . Le paramétrage du mode multi-établissement se fait dans l'EAD.

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



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`

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

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

Anti-virus temps réel

Afin de limiter la propagation des virus à travers le réseau, une surveillance anti-virus temps réel est active sur les partages.

L'activation du service se gère en modifiant la variable `Activer l'anti-virus temps réel sur SMB` dans l'onglet `Clamav` de l'interface de configuration du module.

Attention cet onglet n'est visible que si le service ClamAV est lui même activé (`Activer l'anti-virus Clamav` à `oui`) dans l'onglet `Services`.

La durée de conservation des fichiers mis en quarantaine est paramétrable.

Lorsqu'un virus est détecté, il est renommé avec le préfixe `.virus:` et devient masqué pour l'utilisateur.



La consultation des fichiers infectés détectés et mis en quarantaine par le serveur peut se faire au travers de l'EAD.

Voir aussi...

- Onglet Clamav : Configuration de l'anti-virus
- Configuration du mode multi-établissement

2.16. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.895]. 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)

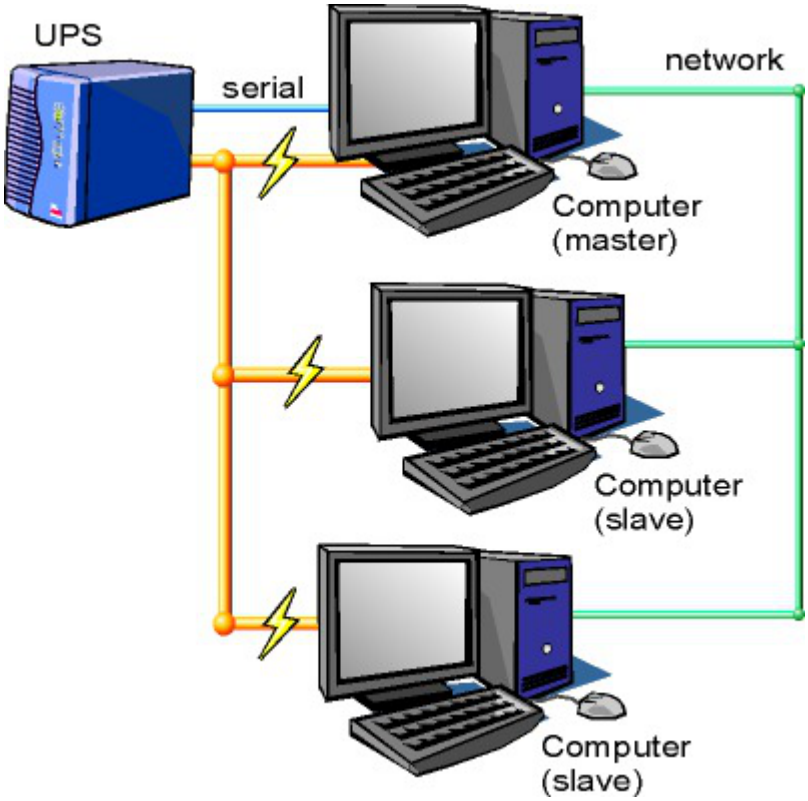


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

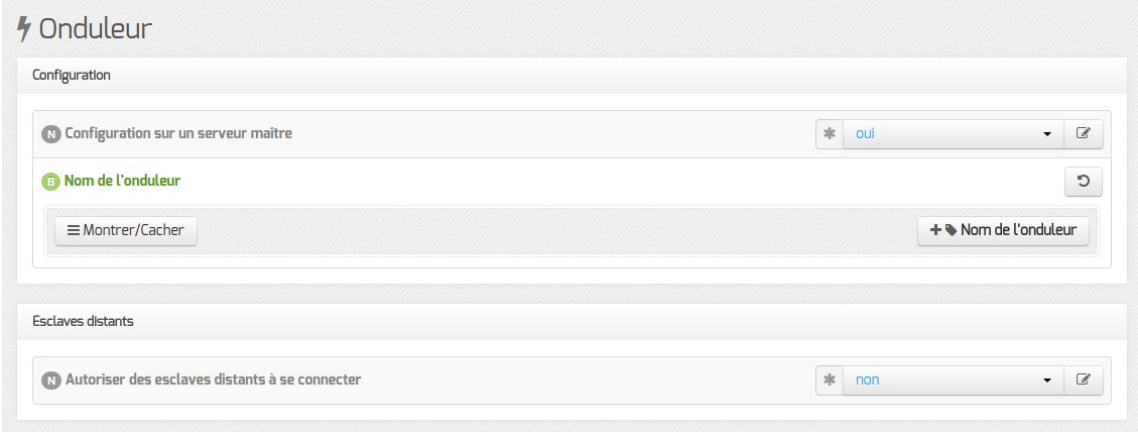
http://www.networkupstools.org/source/2.7/new-2.7.1.txt

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

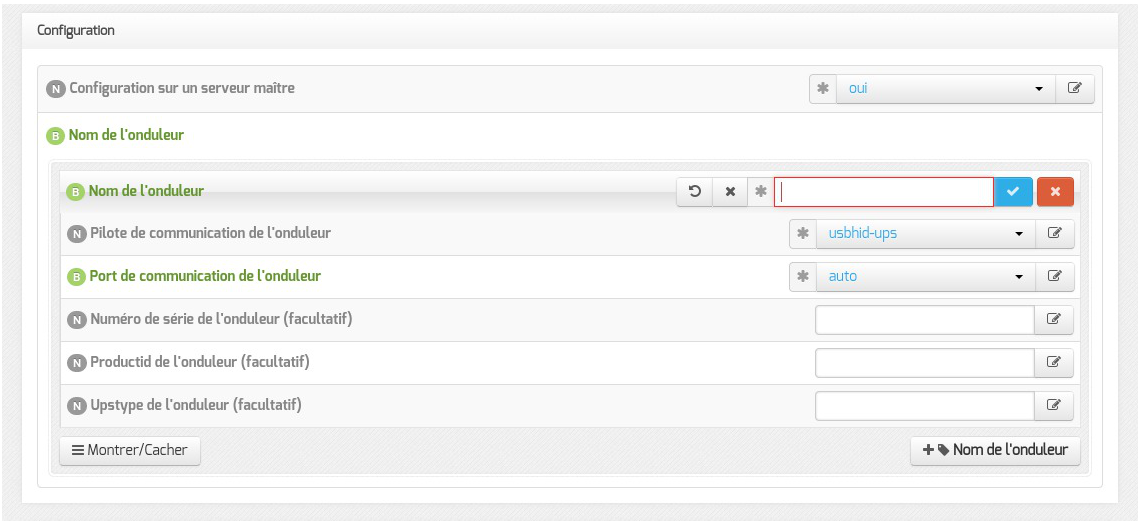
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

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)

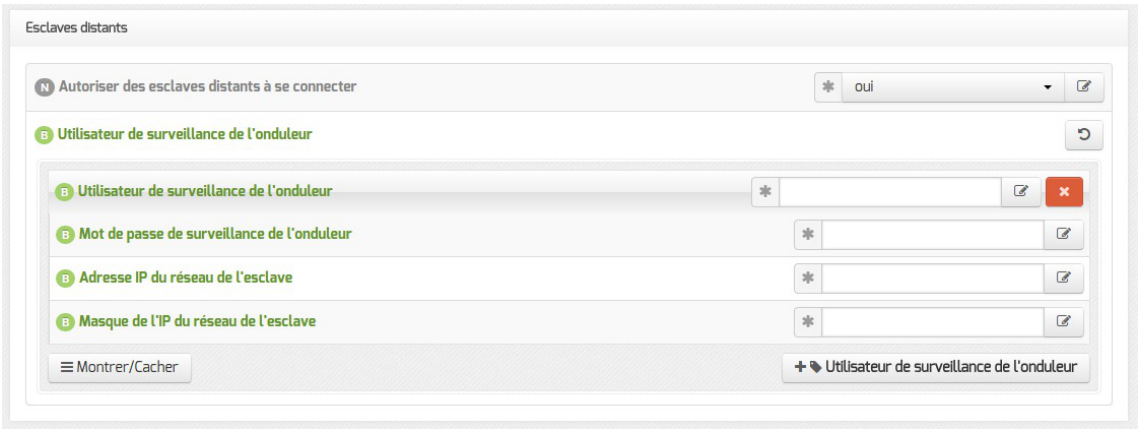
- Port de communication de l'onduleur : `auto`.

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/trusty/en/man5/ups.conf.5.html

Configurer un serveur esclave

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

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



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

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

Exemple de configuration

Sur le serveur maître :

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

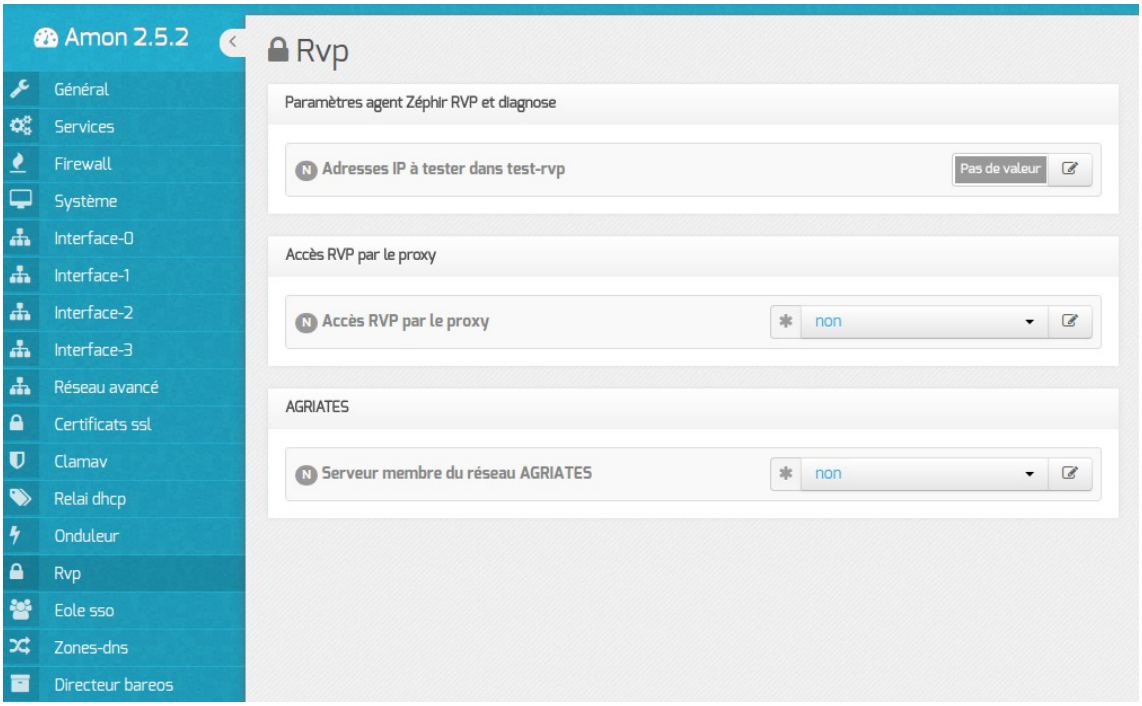
Sur le serveur esclave :

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

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`.

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

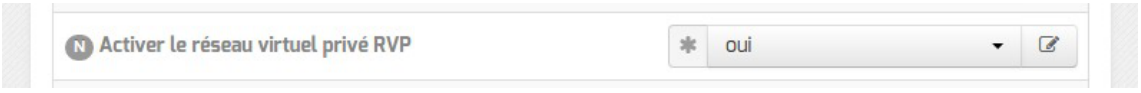


Onglet Rvp mode Normal

Le réseau virtuel privé[p.899] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

L'onglet `Rvp` apparaît après activation du service dans l'onglet `Services`.



Configuration des tunnels

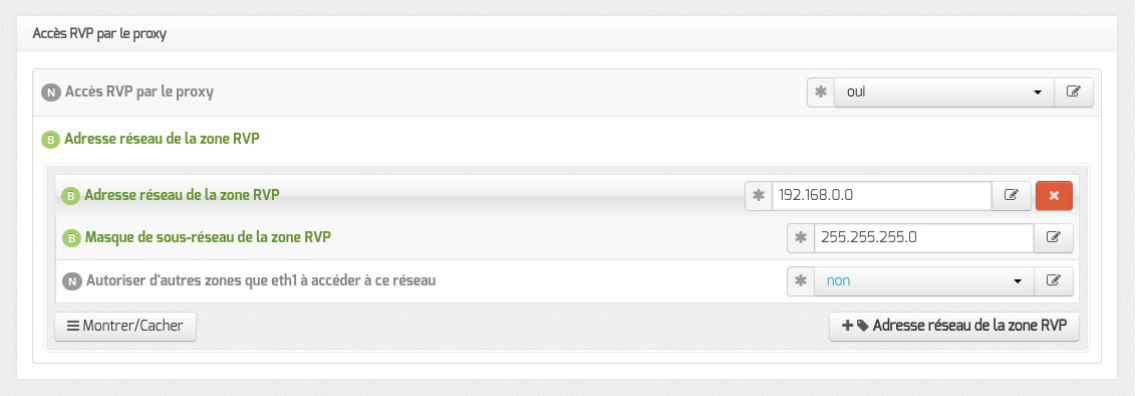
Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.1 du module Amon. La configuration des tunnels s'effectue d'office en mode fichier plat.

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

Accès RVP par le proxy

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

Pour paramétrer l'accès RVP par le proxy, il faut passer la variable `Accès RVP par le proxy` à `oui`.

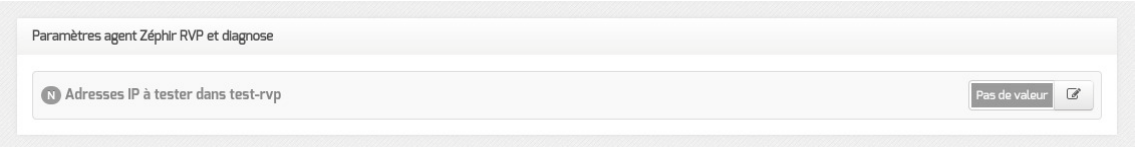


L'adresse réseau de la zone RVP permet la configuration du proxy Squid pour autoriser ou non, aux postes autres que sur l'interface eth1, l'accès via le VPN à un sous réseau.

Pour ajouter d'autres adresses réseau il faut cliquer sur le bouton `+Adresse réseau de la zone RVP`.

Paramètres agent Zéphir RVP et diagnose

Le champ `Adresses IP à tester dans test-rvp` permet de saisir une ou plusieurs adresses IP qui seront utilisées par le diagnose et par l'agent Zéphir pour tester des adresses IP à l'autre extrémité des tunnels.



AGRIATES

Si le serveur est membre d'AGRIATES il faut passer la variable `Serveur membre du réseau AGRIATES` à `oui`.



- `Adresse du DNS permettant de résoudre les in.ac-acad.fr` permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;
- `Nom DNS de la zone résolue par le DNS AGRIATES` : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

Application de la configuration et gestion du RVP

Activation du RVP au moment de l'instanciation du serveur Amon

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

Au lancement de l'instanciation, la question suivante vous est posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Deux choix sont alors proposés :

`1.Manuel` permet de prendre en compte la configuration RVP présente sur une clé USB ;

`2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

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



Lors de cette phase de configuration du VPN sur Amon, les tunnels peuvent se couper dans les secondes qui suivent et dans certaines circonstances uniquement. Le problème est corrigé à partir de la version strongSwan 5.5.0 qui n'est pas disponible sur cette version d'EOLE.

Toutefois, le problème est très ponctuel et les tunnels seront relancés automatiquement par l'agent Zéphir assez rapidement.

Suppression du RVP

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

2.18. 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.

Bien que l'utilisation de l'adresse IP de la carte eth0 soit possible pour une utilisation des applications sur le réseau local du module, il est fortement recommandé d'utiliser un nom de domaine.

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 sur le module Scribe 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`. Déclarer le proxy inverser permet également de mettre en place correctement certaines restrictions sur les applications web

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 par contre une entête qui contient une adresse IP qui peut être falsifiée depuis la machine source.

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



Cette fonctionnalité était implémentée via le module Apache additionnel RPAF : https://github.com/gnif/mod_rpaf.

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`.

Activer EOE

Cette variable permet d'activer/désactiver l'application web EOE sur le module.

EOE propose une interface simple contenant un ensemble d'outils à destination des élèves.

Activer EOP

Cette variable permet d'activer/désactiver l'application web EOP sur le module.

EOP propose une interface simple contenant un ensemble d'outils à destination des enseignants.

Activer Roundcube (webmail)

Cette variable permet d'activer/désactiver l'application web Rouncube sur le module.

Roundcube est une application web qui permet à l'utilisateur de gérer ses courriers électroniques au travers d'un navigateur.

Permettre aux utilisateurs d'ajouter des comptes de courrier électronique personnels

`Permettre aux utilisateurs de paramétrer leurs propres mails via serveur pop` permet aux utilisateurs d'ajouter des comptes de courrier électronique autres que ceux géres par l'annuaire du module.

Activer Pydio (gestionnaire de fichiers)

Cette variable permet d'activer/désactiver l'application web Pydio (anciennement Ajaxplorer) sur le module.

Pydio est une application web qui permet à l'utilisateur de gérer ses fichiers au travers d'un navigateur.

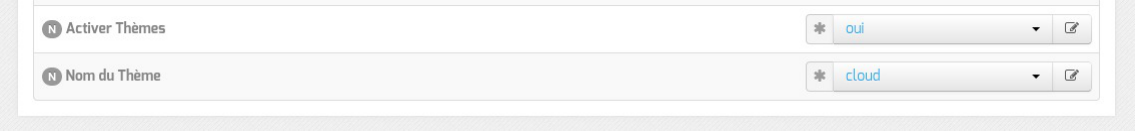


Toutes les applications web pré-packagées installées manuellement apparaissent dans cet onglet pour éventuellement être désactivées.

Envole

L'installation d'Envole[p.888] fait apparaître des variables supplémentaires dans cet onglet et un onglet `Envole`.

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



La gestion des thèmes pour Envole et les applications web est désactivable. Il est également possible de choisir le thème à utiliser parmi une liste.

Beaucoup d'applications web seront impactées : portail Envole, Dokuwiki, EAD, edispatcher, EoleSSO, Moodle, OpenSondage, WordPress, …

Voir aussi...

> Les applications web sur le module Scribe
>
> Espace Numérique Personnel pour l'Éducation avec Envole [p.649]

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

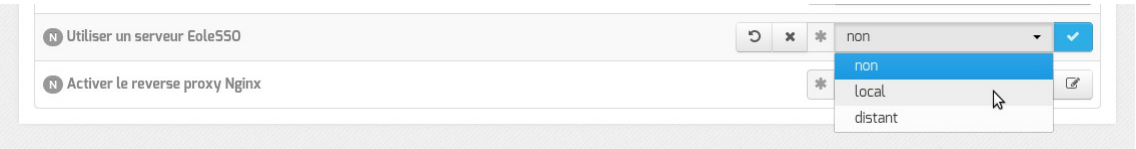
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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

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

Serveur local ou distant

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



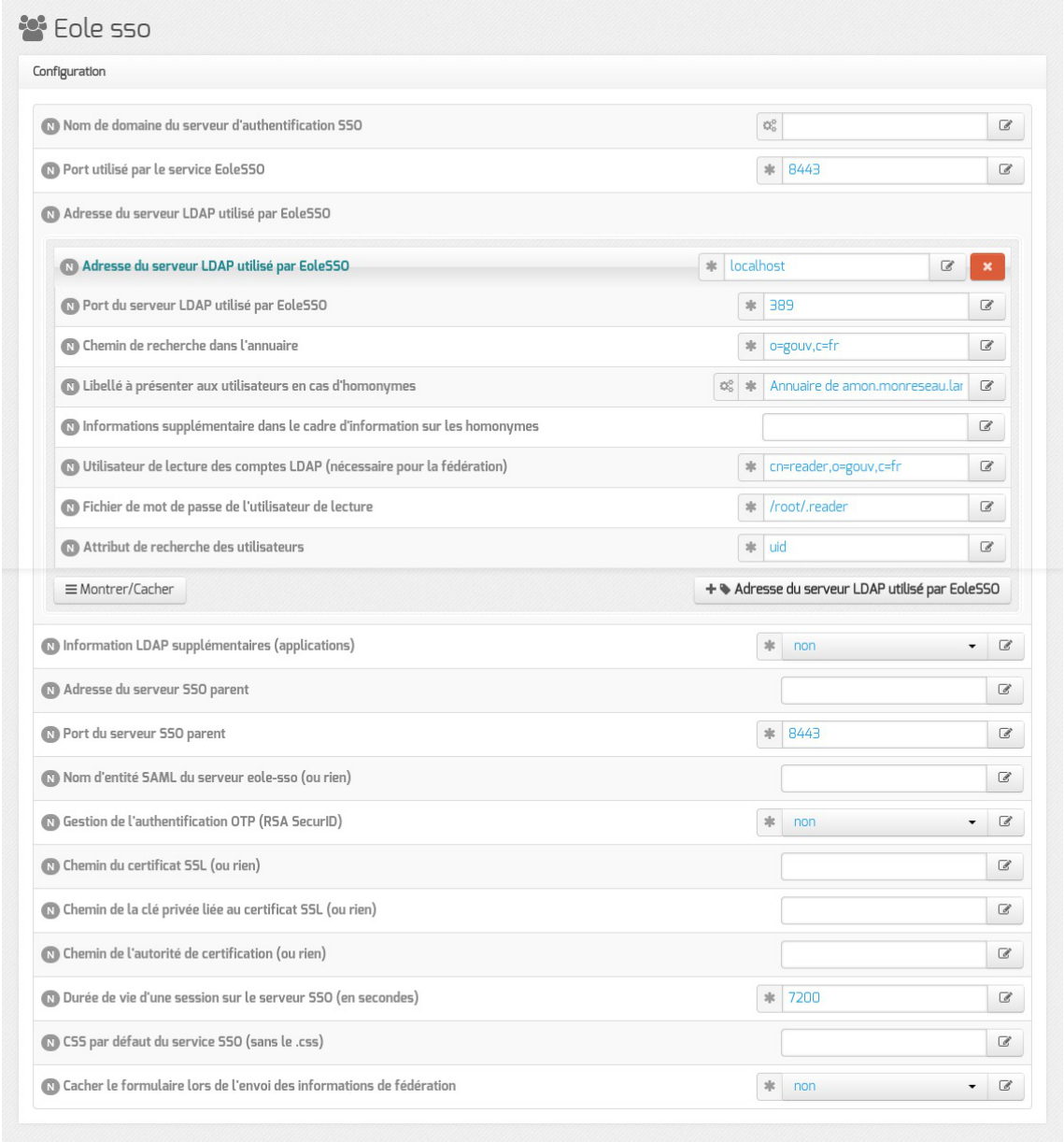
La variable `Utiliser un serveur EoleSSO` permet :

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

Adresse et port d'écoute

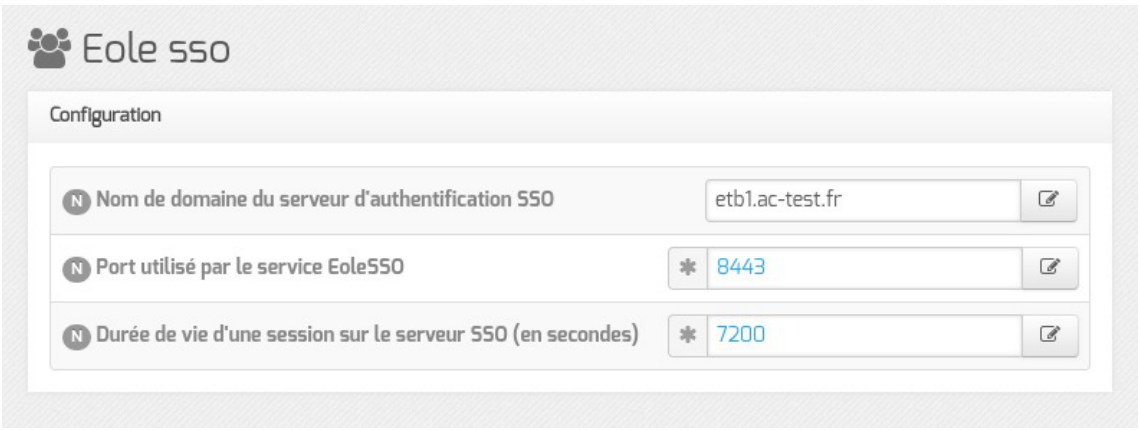
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

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



Configuration d'un serveur EoleSSO local

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



Configuration d'un serveur EoleSSO distant

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.

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

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

Configuration LDAP

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

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.897] si disponible *(voir plus loin)*.

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

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

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

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

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

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

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

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

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

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.906] 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.901] 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

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

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.891] 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.901] (version 2).

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

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

Autres options

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

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

Voir aussi...

> Gestion des sources d'authentification multiples [p.286]

2.20. Onglet Messagerie

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

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

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

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

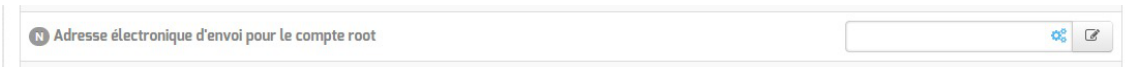
Serveur d'envoi/réception



Les paramètres communs à renseigner sont les suivants :

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

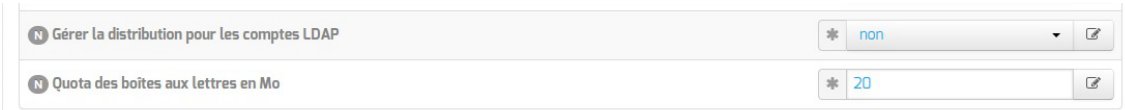
> Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.
>
> Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.
>
> Cette contrainte permet de faire en sorte que les courrier électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.



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

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

Toujours en mode normal d'autres paramètres sont modifiables.



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

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

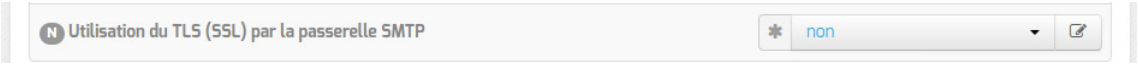
Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

Relai des messages



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

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



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.903] pour l'envoi de message. Si la passerelle SMTP[p.901] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.902] (port 25) ou non (port 465).

2.21. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet Authentification : `Activer l'authentification web (proxy)`.



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

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Activer une deuxième instance de Squid

Activer une deuxième instance de Squid permet une double authentification, c'est à dire la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Pour profiter de cette fonctionnalité, il faut passer `Activer une deuxième instance de Squid` à `oui`.

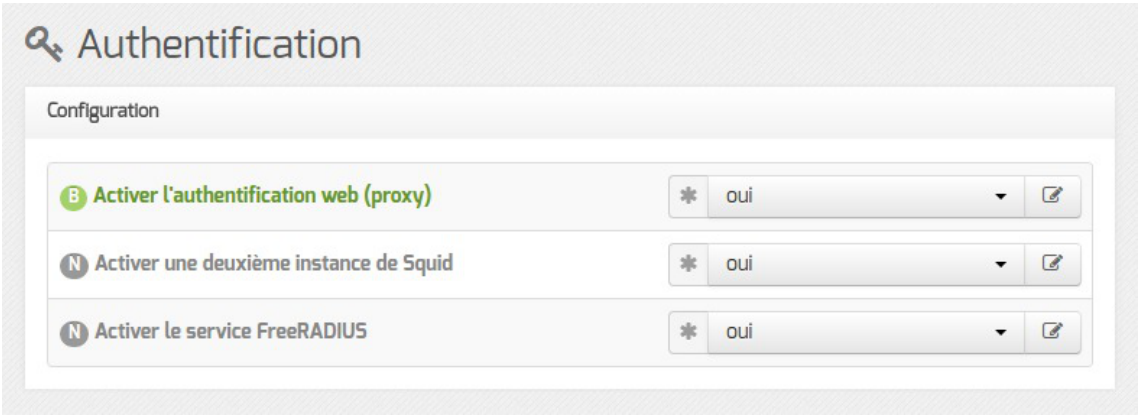


Cela fera apparaître l'onglet `Proxy authentifié 2`.

Activer le service FreeRADIUS

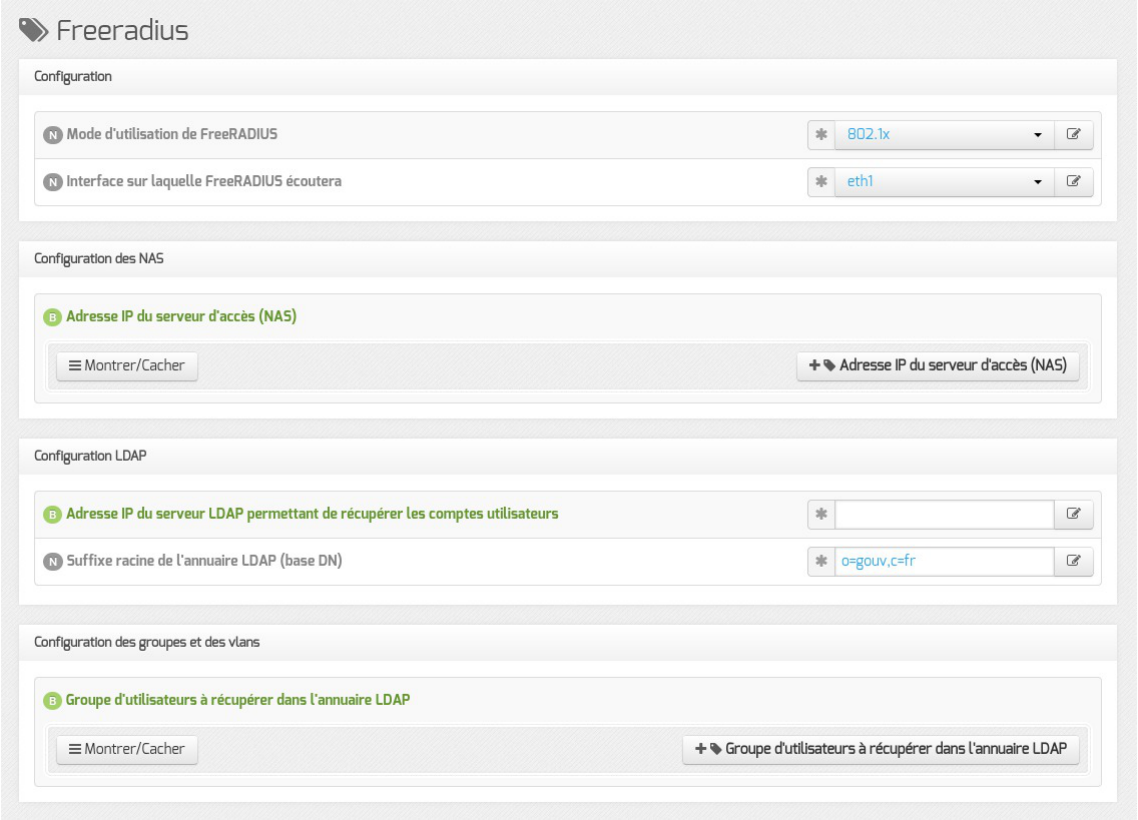
EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.899].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui`.



Cela fera apparaître l'onglet `Freeradius`.

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



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

Voir aussi...

Onglet Proxy authentifié : 5 méthodes d'authentification [p.95]

Onglets Proxy authentifié 2 : Double authentification [p.100]

Onglet Freeradius : Configuration de l'authentification Radius [p.105]

2.22. Onglet Proxy authentifié : 5 méthodes d'authentification

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.

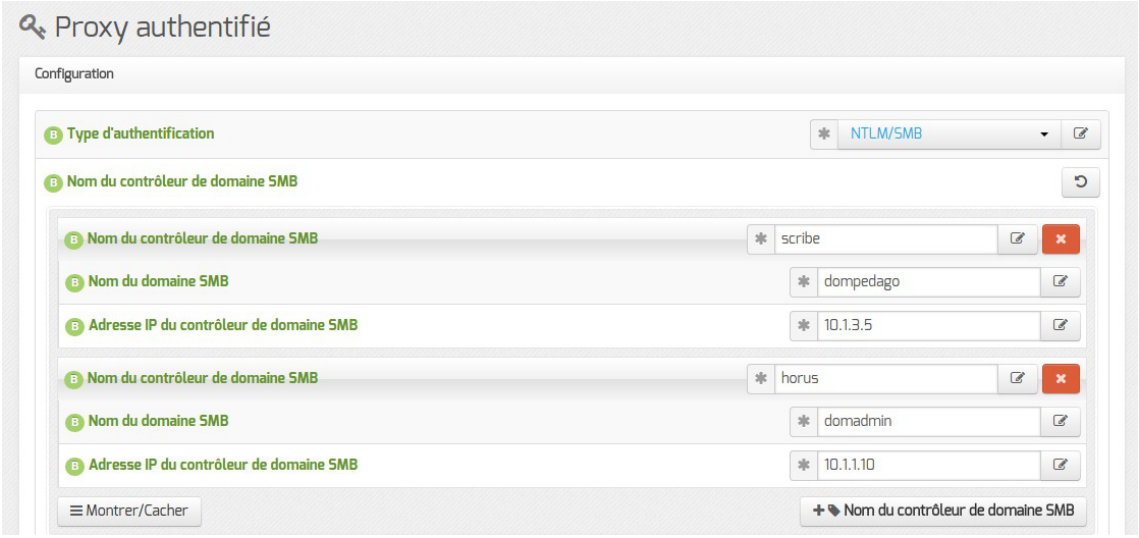


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.



Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

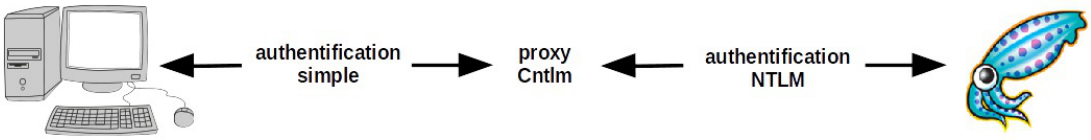
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : http://technet.microsoft.com/en-us/library/cc960646

Authentification NTLM/SMB poste hors domaine

En mode normal, l'authentification NTLM[p.895] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.886].

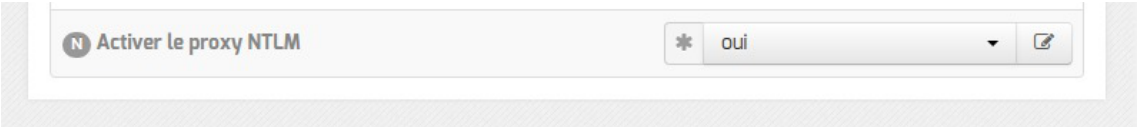
Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



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

Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

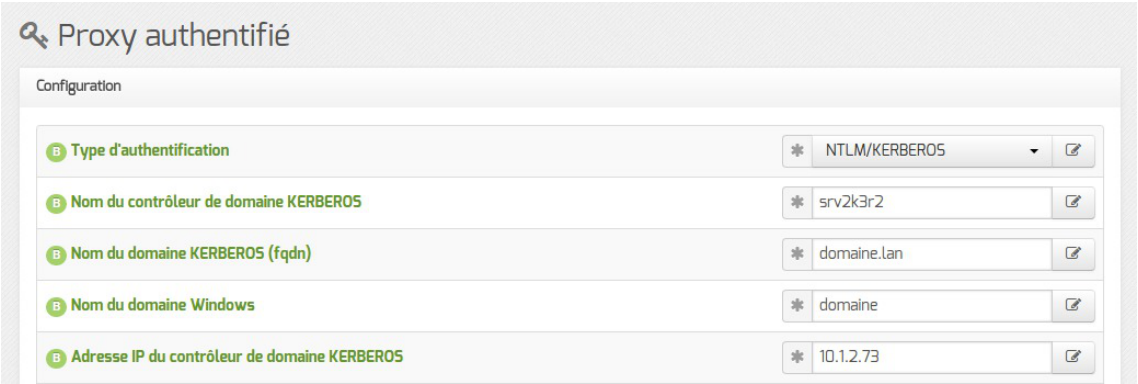
Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

C'est le premier domaine spécifié qui sera utilisé par Cntlm.

Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

L'intégration peut être réalisée lors de l'instanciation du module en répondant `oui` à la question suivante :

```
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?
```

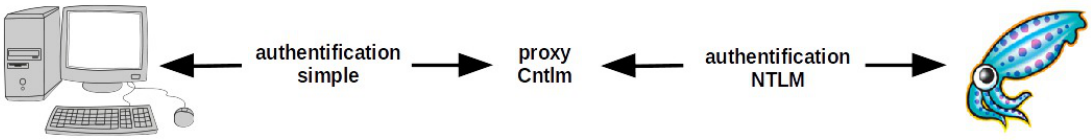
Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

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

Authentification NTLM/KERBEROS poste hors domaine

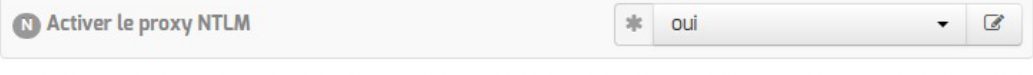
En mode normal, l'authentification NTLM[p.895] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.886].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

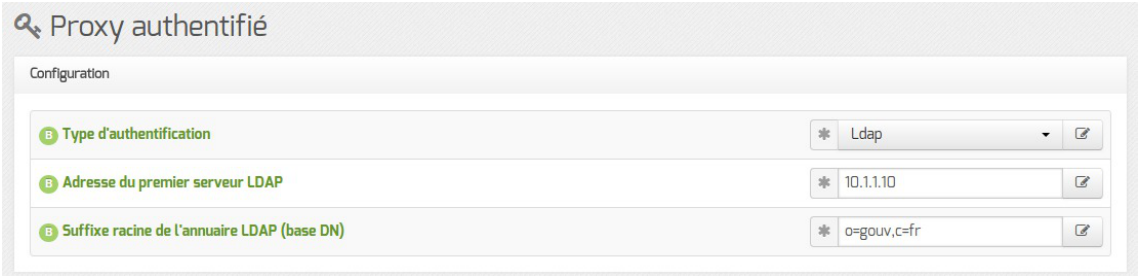
Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.



Ce type d'authentification est recommandé pour les postes hors domaine.

En mode normal, il est possible de déclarer un annuaire de secours.

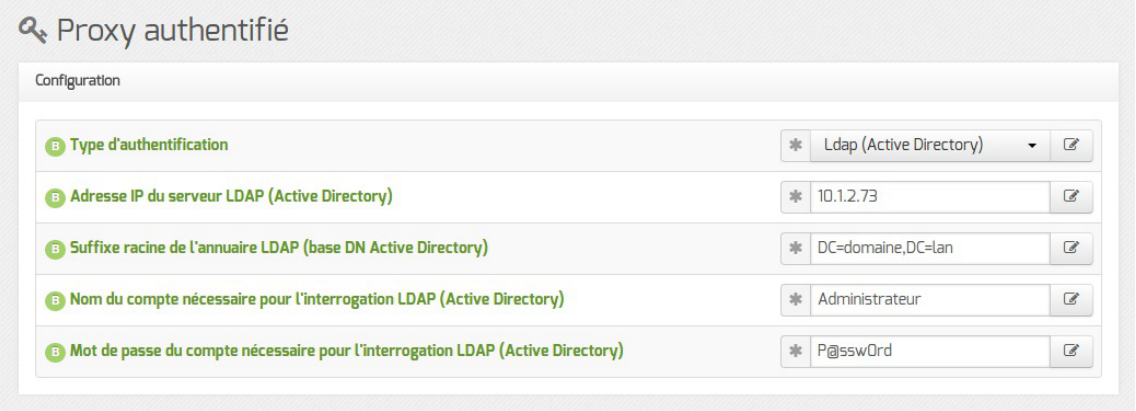


Cet annuaire est interrogé uniquement si le premier ne répond pas.

Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

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

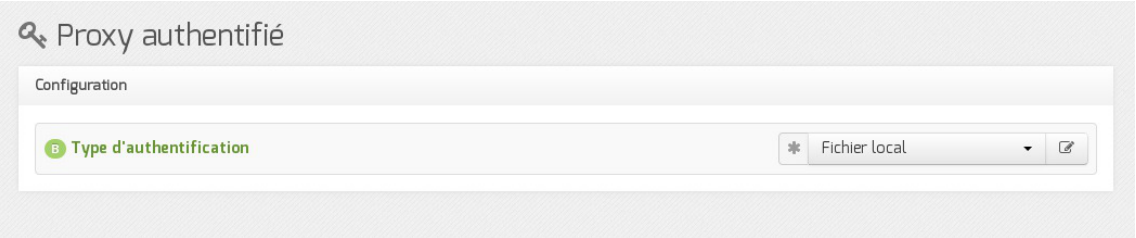
Authentification LDAP (Active Directory)



Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory.

Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local



Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux.

Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format *htpasswd* et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```



En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

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

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette interface (s'applique aussi aux VLAN)`.

2.23. Onglets Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

1. Activation de la deuxième instance de Squid dans l'onglet `Authentification` :



2. Configuration du type d'authentification dans l'onglet `Proxy authentifié 2` :



Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log`

Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

2.24. Onglet Exceptions proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

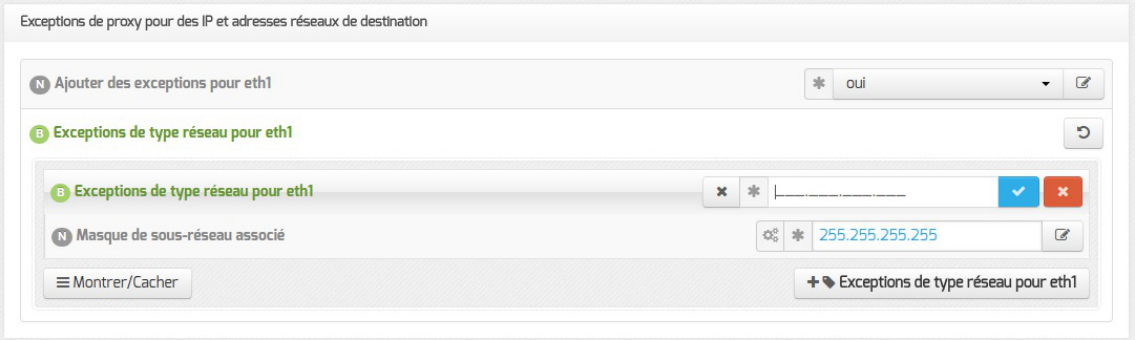
Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage

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

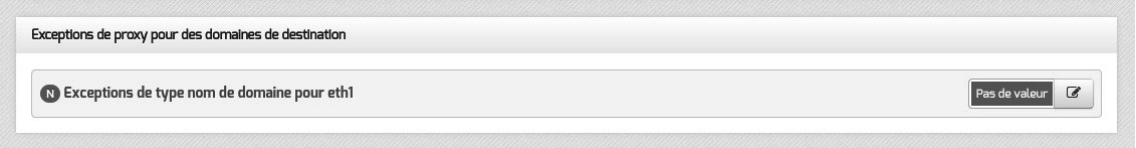
d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

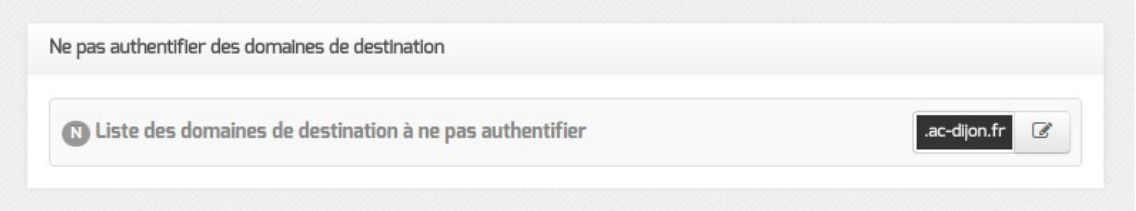
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

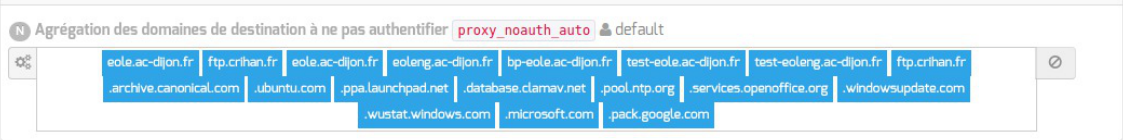
Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée

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

`proxy_noauth_auto`.

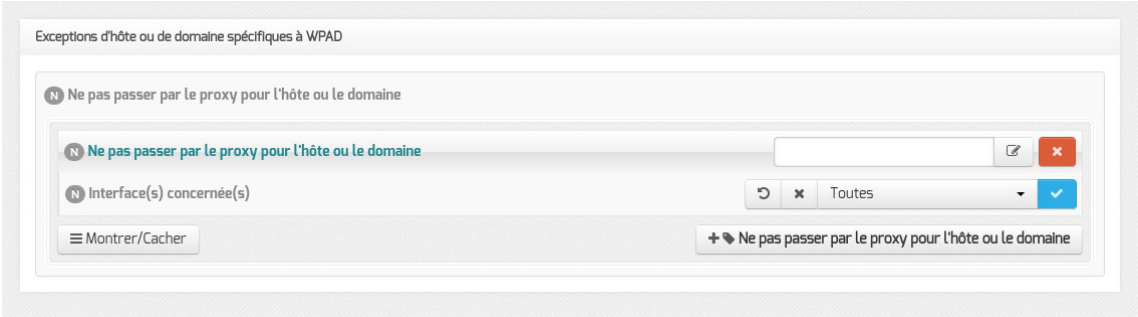
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.



Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.



Compléments sur `Ne pas passer par le proxy pour le` domaine (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

2.25. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.894].

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

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.887] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.902].

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.891]*/DNAT*.

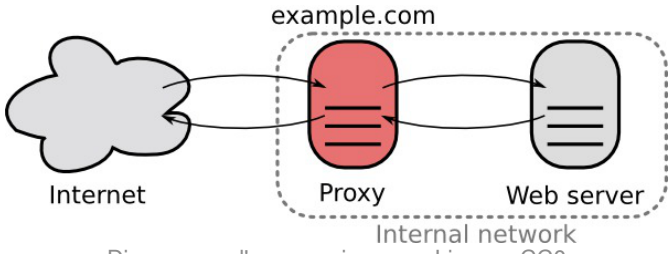
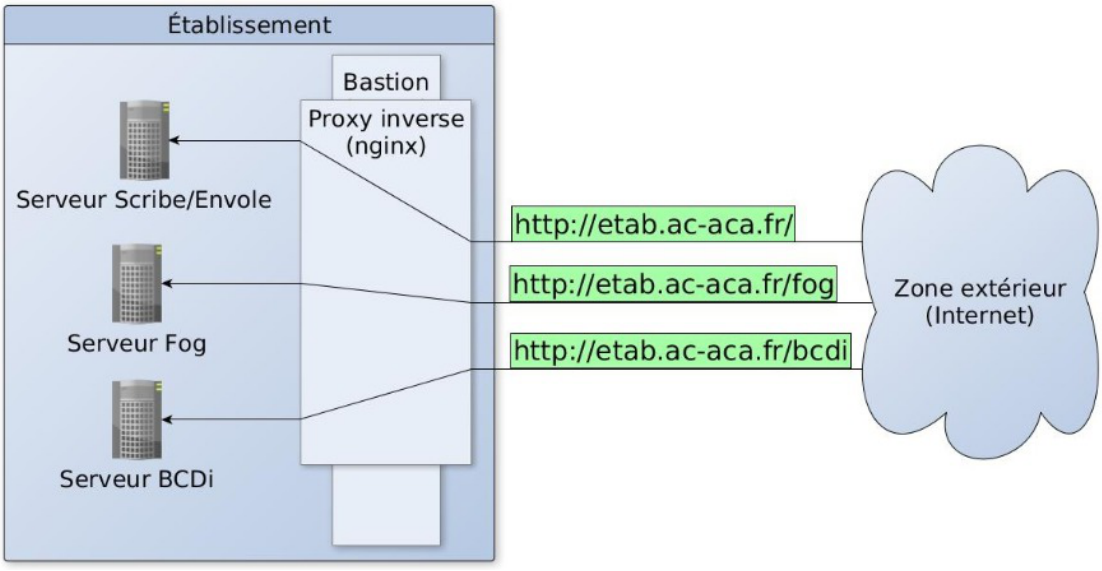


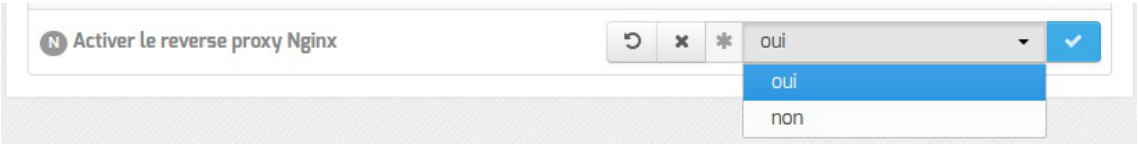
Diagramme d'un proxy inverse - Licence CC0

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

- serveur EoleSSO ;
- outil d'administration EAD[p.888] ;
- application EOP ;
- protocole HTTP[p.890] ;
- protocole HTTPS[p.890].



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



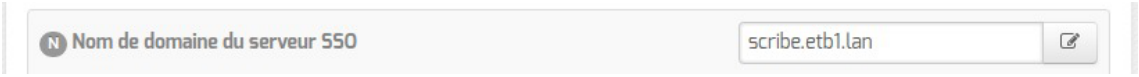
L'activation du service fait apparaître un nouvel onglet.

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



Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

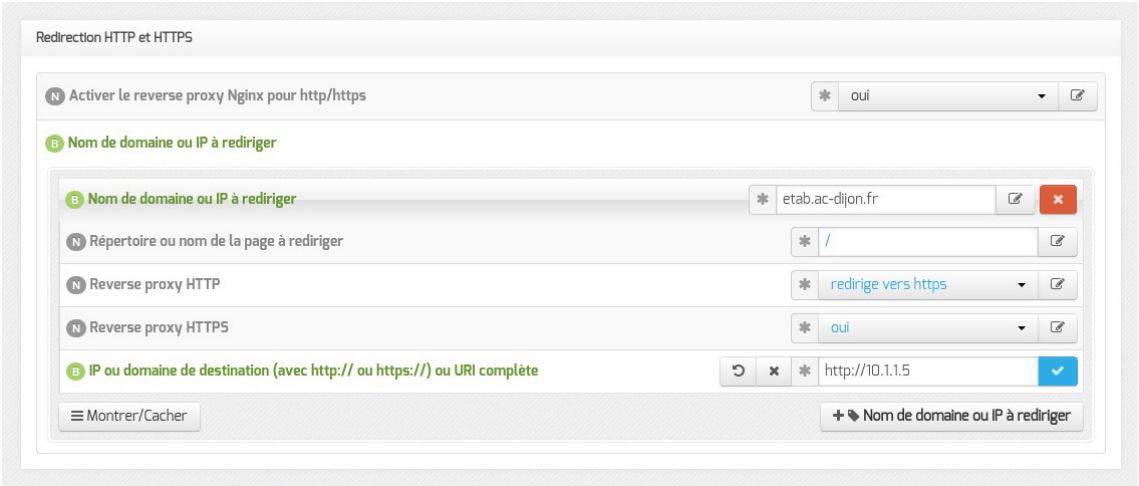


Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.



Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

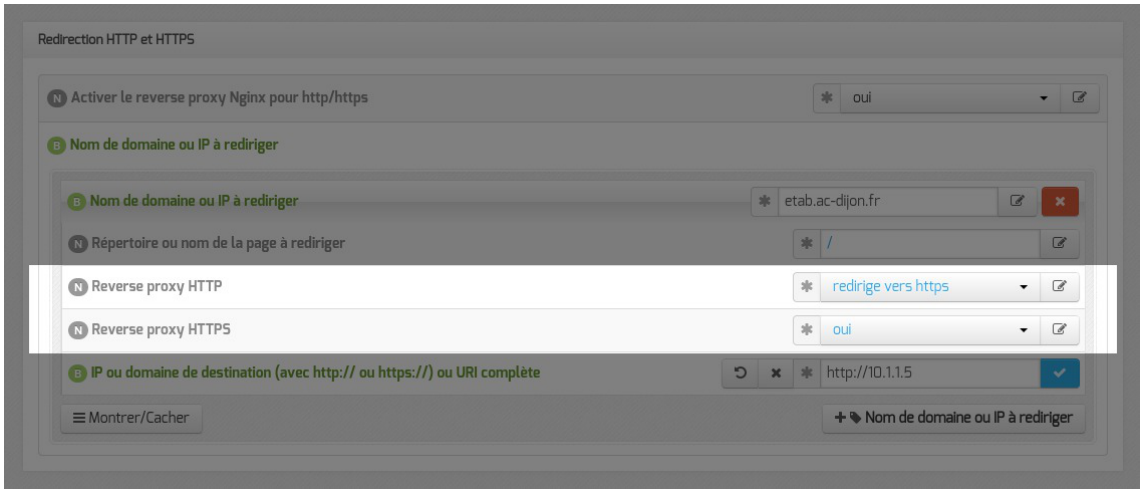


Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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 ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;

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

- 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.904] (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`.



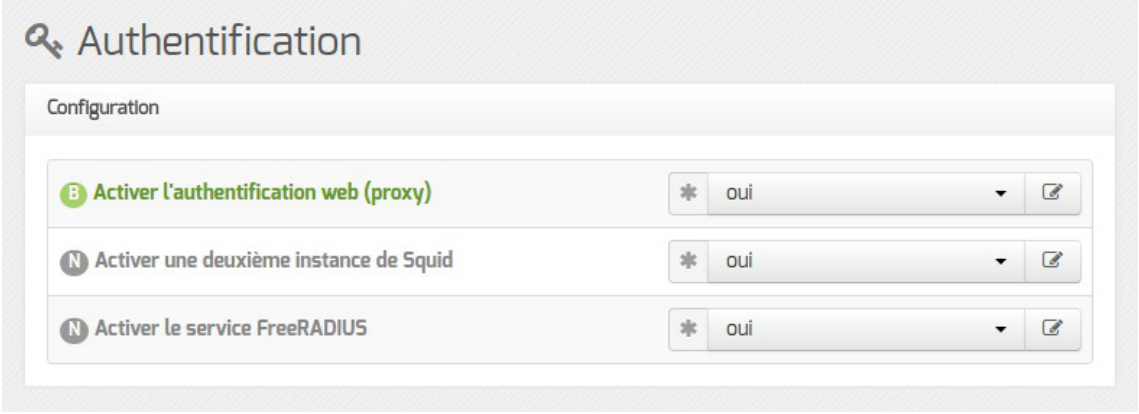
Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.898], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

2.26. Onglet Freeradius : Configuration de l'authentification Radius

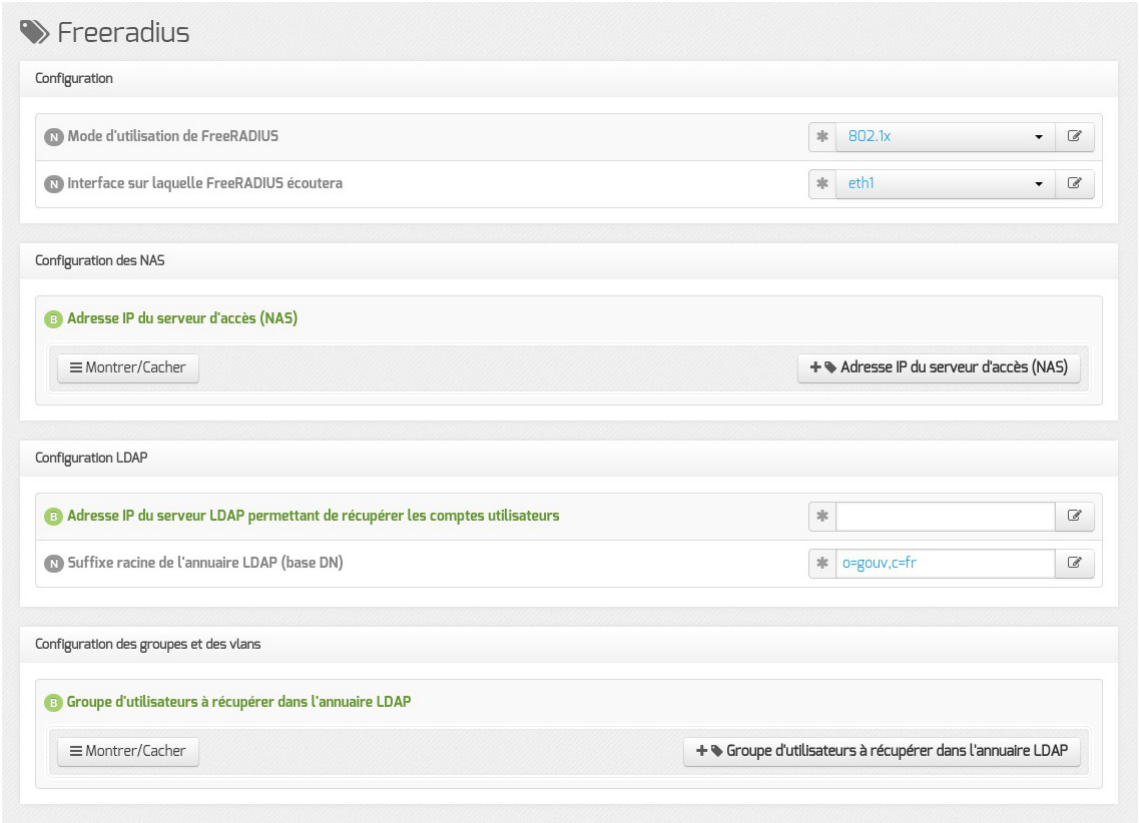
EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.899].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui` dans l'onglet `Authentification`.

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



Cela fera apparaître l'onglet `Freeradius`.



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

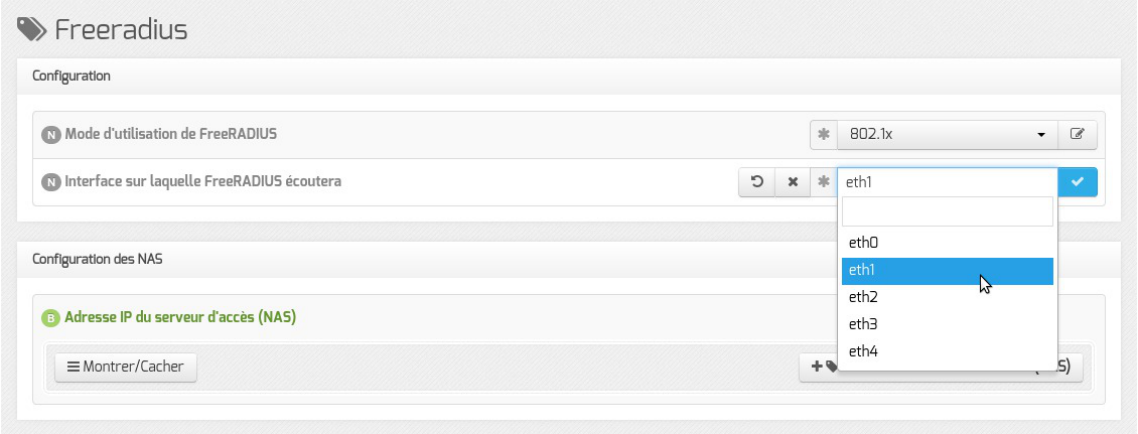
Il est possible de choisir entre 2 modes d'utilisation de FreeRADIUS :

- 802.1x ;
- accounting.

Le mode 802.1x

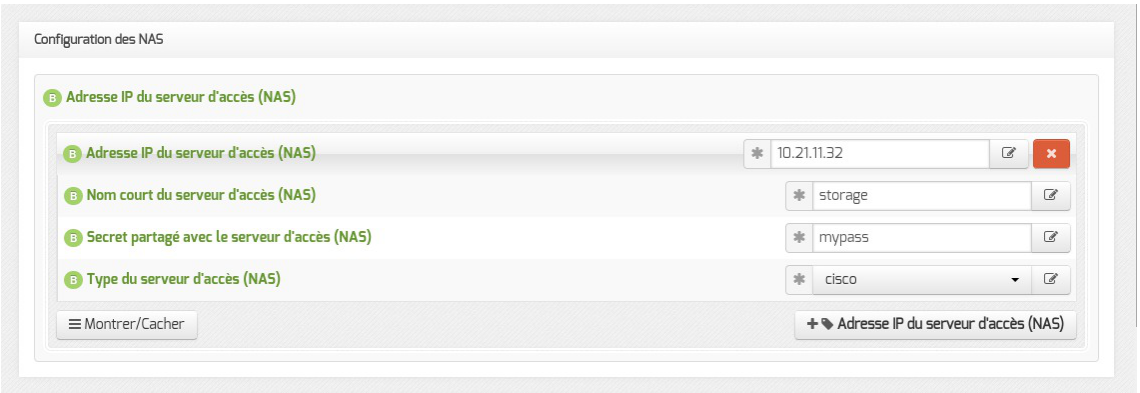
Le mode `802.1x` permet de taguer dynamiquement des ports d'un switch (NAS[p.893]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.

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



`Interface sur laquelle FreeRADIUS écoutera` : définition de l'interface d'écoute de FreeRADIUS.

Configuration des NAS



`Adresse IP du serveur d'accès (NAS)` : adresse IP du switch.

`Nom court du serveur d'accès (NAS)` : libellé du switch.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et le switch.

`Type du serveur d'accès (NAS)` : type de switch.

Configuration LDAP

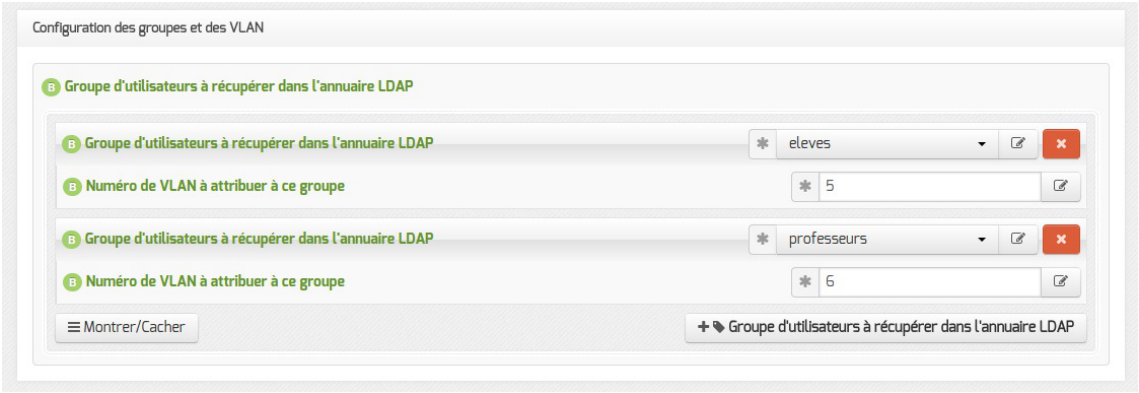


`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP LDAP.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

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

Configuration des groupes et des VLAN



`Groupe d'utilisateurs à récupérer dans l'annuaire LDAP` : saisir ou choisir un groupe existant dans l'annuaire.

`Numéro de VLAN à attribuer à ce groupe` : les machines se connectant avec un utilisateur appartenant au groupe indiqué ci-dessus verra son port tagué sur ce numéro de VLAN.

Le mode accounting

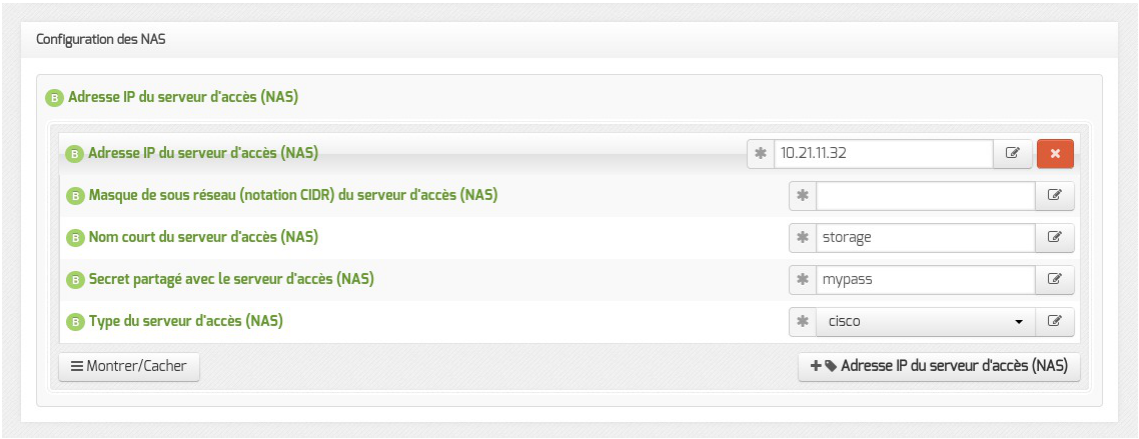
Le mode accounting permet de créer un réseau Wi-Fi WPA enterprise sur une borne Wi-Fi (NAS) ayant pour identifiants autorisés les compte/motDePasse de l'annuaire LDAP déclaré.



Onglet Freeradius - mode accounting

`Adresse IP sur laquelle FreeRADIUS écoutera` : l'adresse IP d'une des interfaces du serveur.

Configuration des NAS



Onglet Freeradius - mode accounting

`Adresse IP du serveur d'accès (NAS)` : adresse IP de la borne Wi-Fi.

`Masque de sous réseau (notation CIDR) du serveur d'accès (NAS)` : 24 (en notation

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

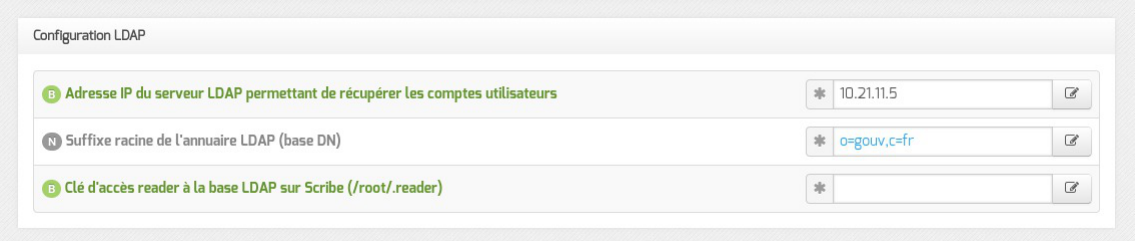
CIDR[p.885]) si le réseau est de classe C.

`Nom court du serveur d'accès (NAS)` : libellé de la borne Wi-Fi.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et la borne Wi-Fi.

`Type du serveur d'accès (NAS)` : type de borne (other en général).

Configuration LDAP



Onglet Freeradius - mode accounting

`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP ldap.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

`Clé d'accès reader à la base ldap sur Scribe (/root/.reader)` : à récupérer sur le serveur LDAP.

3. Configuration en mode expert

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

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

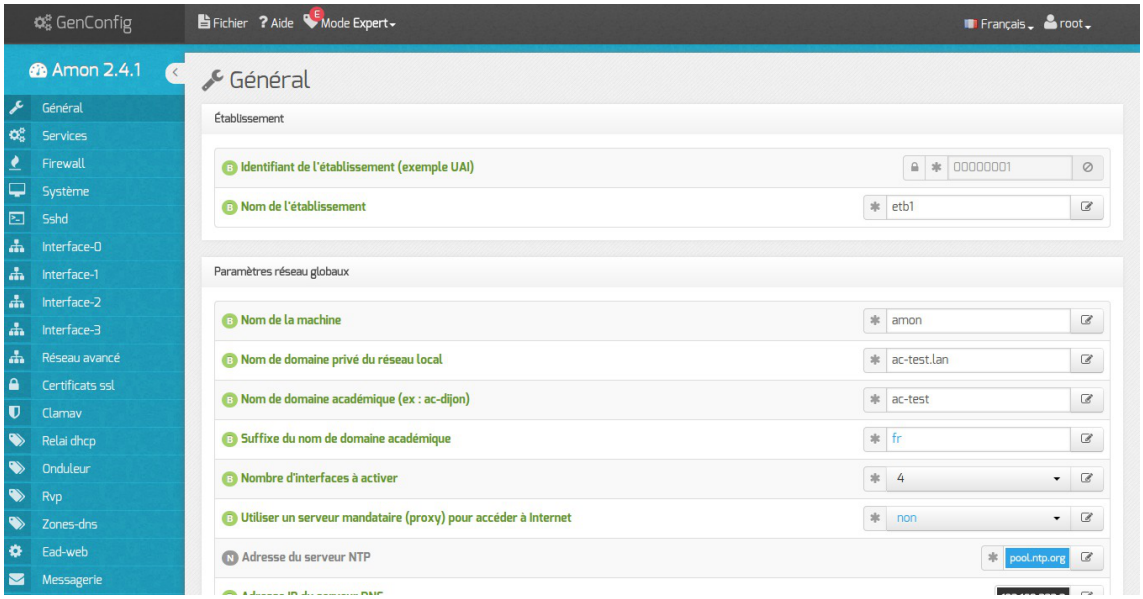
- `Général` ;
- `Services` ;
- `Firewall` ;
- `Système` ;
- `Sshd` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificat ssl` ;
- `Apt-cacher` ;
- `Agregation` ** ;
- `Mots de passe` ;

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

- Clamav ;
- Directeur bareos ;
- Stockage bareos ;
- Annuaire ;
- Dhcp * ;
- Tftp * ;
- Esu ;
- Samba ;
- Nscd ;
- Onduleur * ;
- Rvp * ;
- Application web ;
- Apache ;
- Eole sso * ;
- Zone-dns ;
- Ead-web ;
- Mysql ;
- Messagerie ;
- Openldap ;
- Authentification ;
- Dansguardian ;
- Squid ;
- Squid2 **;
- Proxy authentifié ;
- Proxy authentifié 2 **;
- Exceptions proxy ;
- Cups ;
- Proxy parent ;
- Reverse proxy * ;
- Proftpd ;
- Freeradius **;
- Eoleflask ;
- Ent .

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.

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

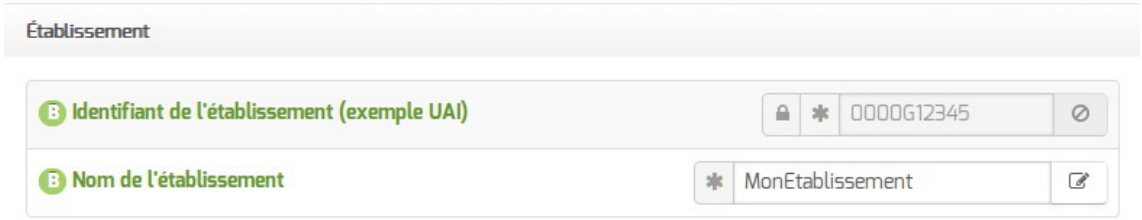


Vue générale de l'interface de configuration du module

3.1. Onglet Général

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

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

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

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

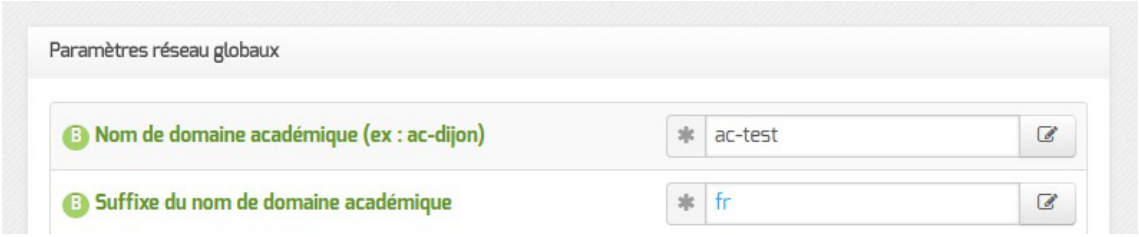
Sur les modules fournissant un annuaire LDAP[p.892] local, ces variables sont utilisées pour créer l'arborescence.



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

Paramètres réseau globaux

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



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

Cette information est découpée en plusieurs champs :

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

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

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

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

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

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

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

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

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

Proxy

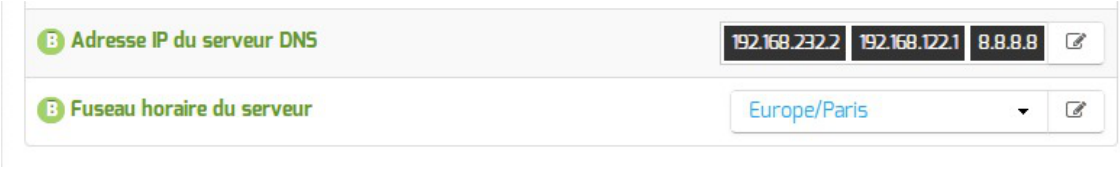
Si le module doit utiliser un proxy pour accéder à Internet, il faut activer cette fonctionnalité en passant la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.



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

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

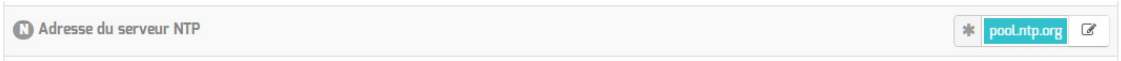
DNS et fuseau horaire



La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS[p.887].

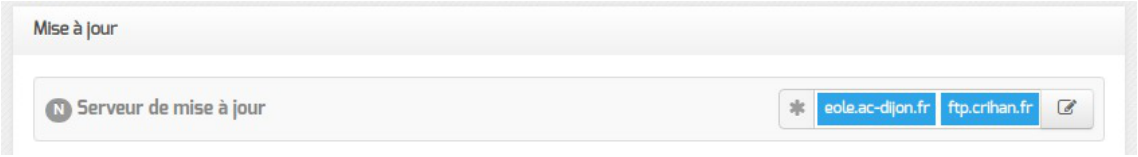
La variable `Fuseau horaire du serveur` vous permet de choisir votre fuseau horaire dans une liste conséquente de propositions.

NTP



Une valeur par défaut est attribuée pour le serveur de temps NTP[p.895]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

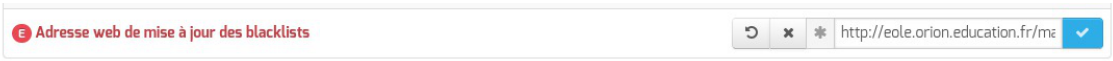


Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.



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

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

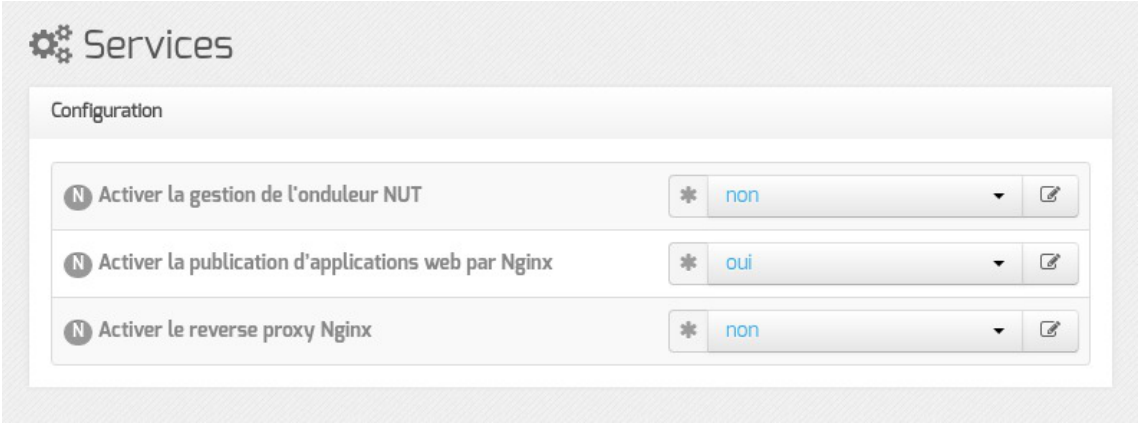


Le champ `Adresse web de mise à jour des blacklists` permet de personnaliser l'adresse à utiliser pour le téléchargement des bases de filtres (blacklists[p.892]).

Voir aussi...

- Onglet Interface-n
- Les différents types de mises à jour
- Bases de filtres optionnels [p.409]

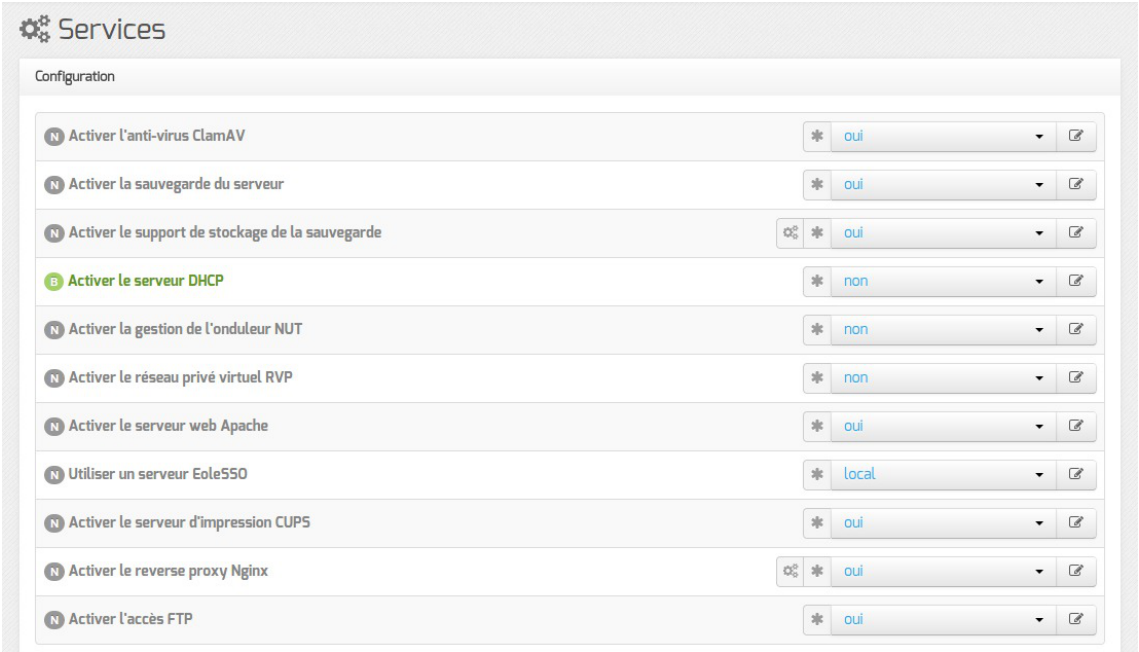
3.2. Onglet Services



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT[p.895].

En mode normal la liste des services activables ou désactivables est beaucoup plus conséquente.



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

Vue de l'onglet Services en mode normal

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

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

- l'anti-virus ClamAv ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le réseau privé virtuel RVP ;
- le serveurs web ;
- le serveur d'authentification unique EoleSSO ;
- le serveur d'impression avec CUPS ;
- le proxy inverse Nginx ;
- l'accès FTP.

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

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

Les services propres au module AmonEcole en mode expert sont :

- l'activation du cache APT ;
- le service PXE/TFTP, il est désactivé par défaut ;
- le filtrage sur le proxy.

Voir aussi...

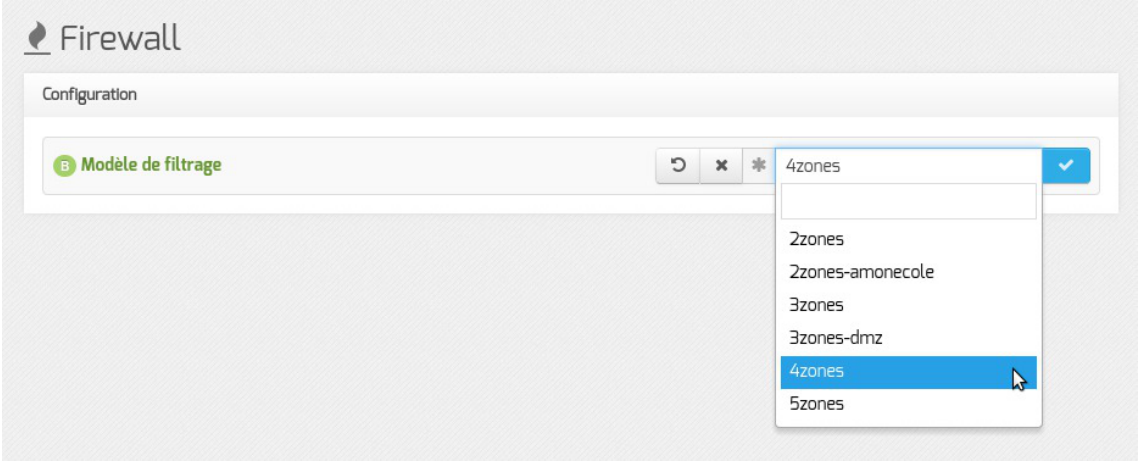
Onglet Logs : Gestion des logs centralisés

3.3. Onglet Firewall

Modèle de filtrage

Le modèle de filtrage doit être choisi en fonction du nombre d'interfaces activées et des services que l'on souhaite mettre en place.

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



Par convention le premier caractère des modèles de filtrage proposés est un chiffre qui correspond au nombre d'interfaces désirées.

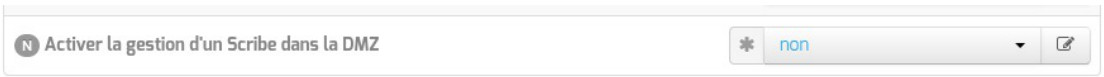
Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

- **2zones** : gestion d'une zone admin ou pedago sur eth1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur eth1) ;
- **3zones** : gestion d'une zone admin sur eth1 et d'une zone pedago sur eth2 ;
- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.884] des règles propres à la DMZ[p.887].



Si l'on souhaite mettre en place l'architecture suivante avec Amon :

- un réseau administratif ;
- un réseau pédagogique ;

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

- une DMZ contenant un serveur Scribe hébergeant des services web à ouvrir depuis l'extérieur.

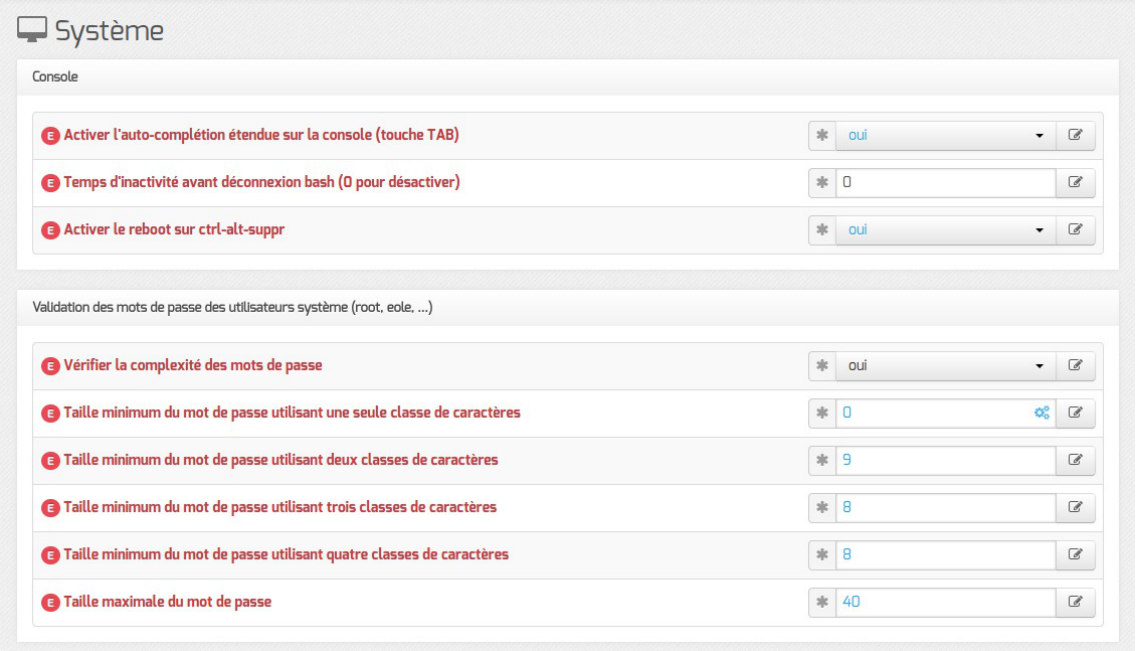
La configuration recommandée sera :

- `Nombre d'interfaces à activer` : `4` (onglet `Général` en mode basique) ;
- `Modèle de filtrage` : `4zones` (onglet `Firewall` en mode basique) ;
- `Activer la gestion d'un Scribe dans la DMZ` : `oui` (onglet `Firewall` en mode normal).

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ

3.4. Onglet Système



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

Paramétrage de la console

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

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

Optimisations système



- `Poids relatif de l'utilisation de la swap par rapport à la mémoire vive` : Le swappiness est un paramètre du noyau Linux permettant de définir avec quelle sensibilité il va écrire dans la swap si la quantité de RAM à utiliser devient trop importante. Le système accepte des valeurs comprises entre 0 et 100. La valeur `0` empêchera au maximum le système d'utiliser la partition d'échange.
- `Activer le service de génération de nombres aléatoires rng-tools` : Le démon `rngd` agit comme une passerelle entre un vrai générateur de nombres aléatoires, matériel (TRNG), tel que ceux que l'on peut trouver dans les puces Intel/AMD/VIA et le pseudo-générateur de nombres aléatoires du noyau (PRNG).



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

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

Validation des mots de passe



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

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

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

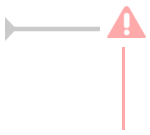
Si la vérification de la complexité des mots de passe est activée, celle-ci peut être régler plus finement à l'aide des paramètres suivants :

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

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

- `Taille maximale du mot de passe`.

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



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

Voir aussi...

Les mots de passe

3.5. Onglet Sshd : Gestion SSH avancée



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

Ils permettent :

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

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

`Permission denied (publickey).`



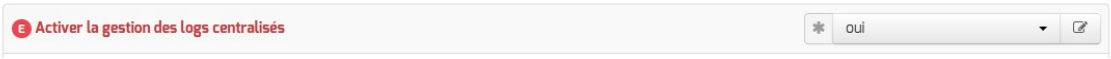
Par défaut les groupes Unix autorisés sont `root` et `adm`.

3.6. Onglet Logs : Gestion des logs centralisés

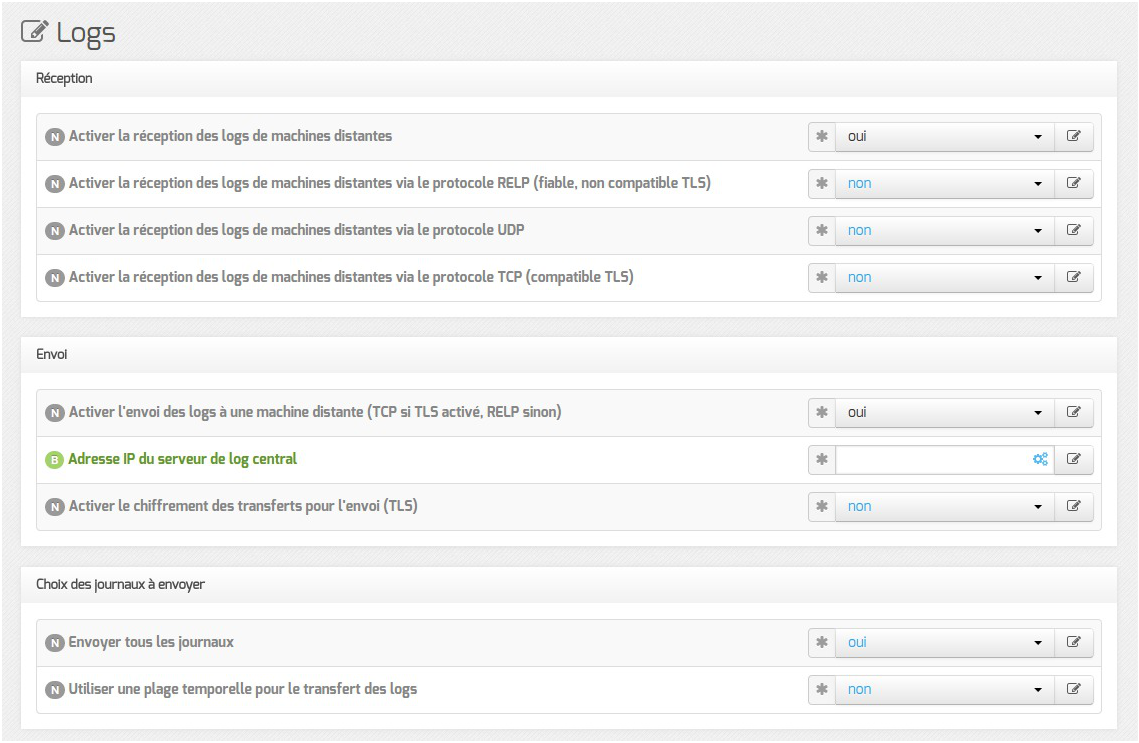
La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.906]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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

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



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



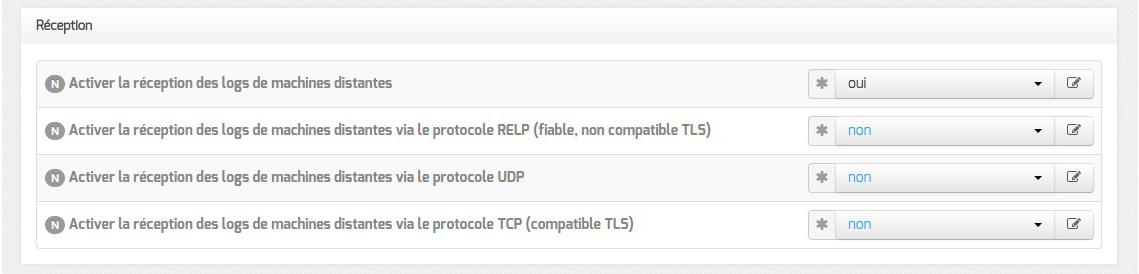
Vue de l'onglet Logs

Les options de cet onglet sont réparties en plusieurs sections :

- la configuration de la réception des logs permet de spécifier les protocoles de communication entre des machines distantes émettrices identifiées par leur adresse IP et le poste configuré ;
- la configuration de l'envoi des logs permet de spécifier l'adresse de la machine distante réceptrice. Le protocole (TCP[p.903] ou RELP[p.899]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.903]) ;
- 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.

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



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



Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.883].

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.



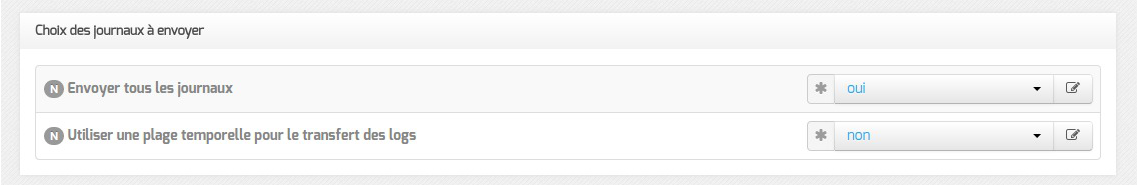
Le protocole (TLS over TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS).



Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI[p.883].

Choix des journaux à envoyer

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

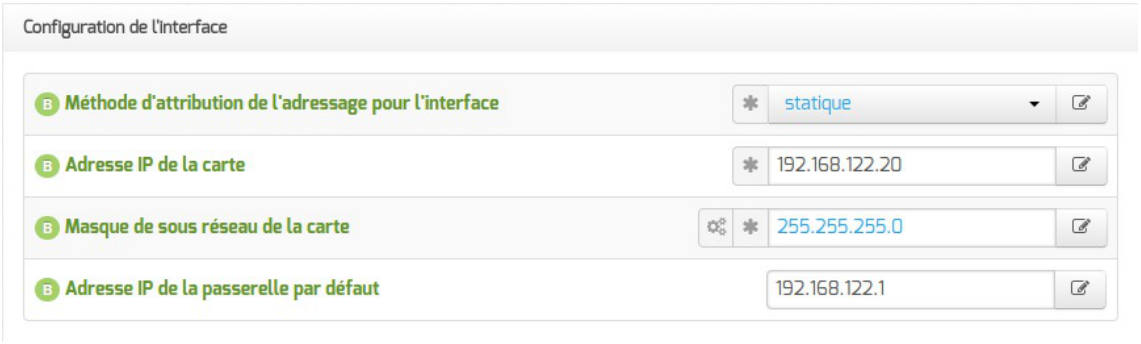


Il est également possible d'envoyer les journaux en temps réel ou en différé. L'heure de début et de fin (plage temporelle) de transfert des journaux est également paramétrable.

3.7. Onglet Interface-0

Configuration de l'interface

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

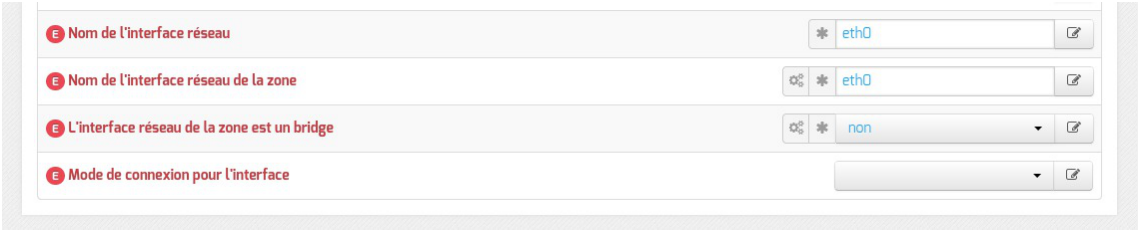


Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP[p.887] et PPPoE[p.898].

- Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.
- La configuration DHCP ne nécessite aucun paramétrage particulier.
- En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

> EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP fixe, certaines fonctionnalités ne seront plus disponibles.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

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

> Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.
>
> Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant

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

`L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.



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

Mode de connexion pour l'interface

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

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

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

Liste des valeurs possible :

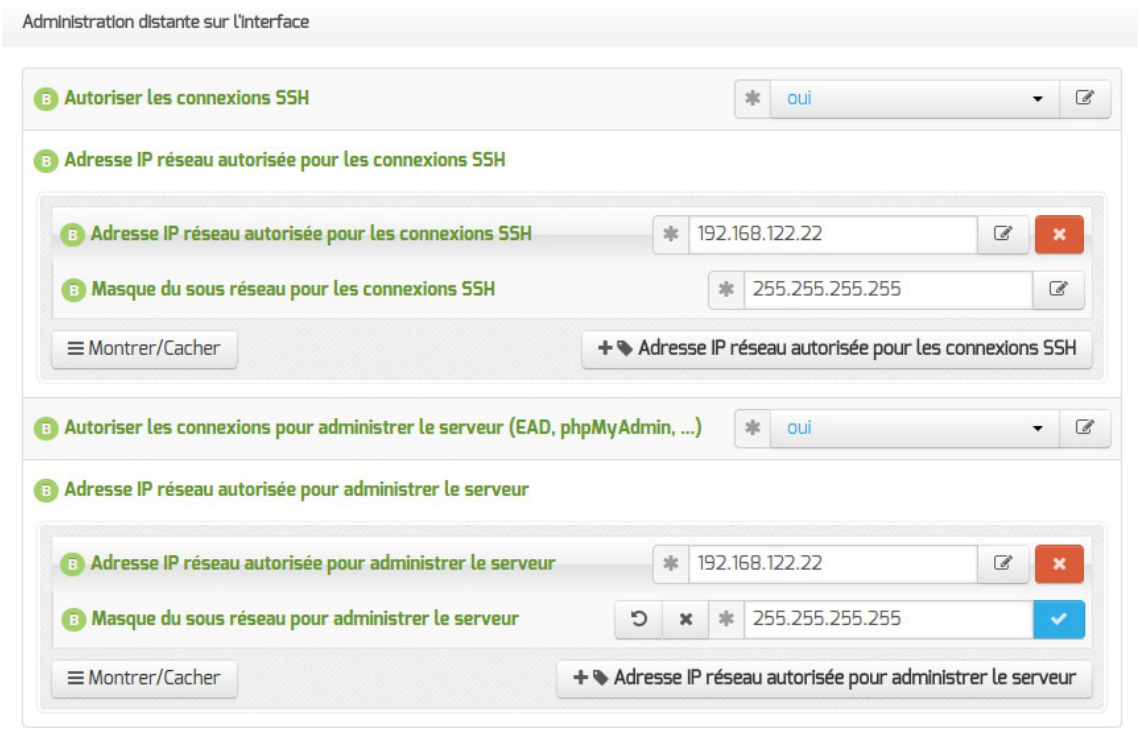
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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



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

Administration à distance

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

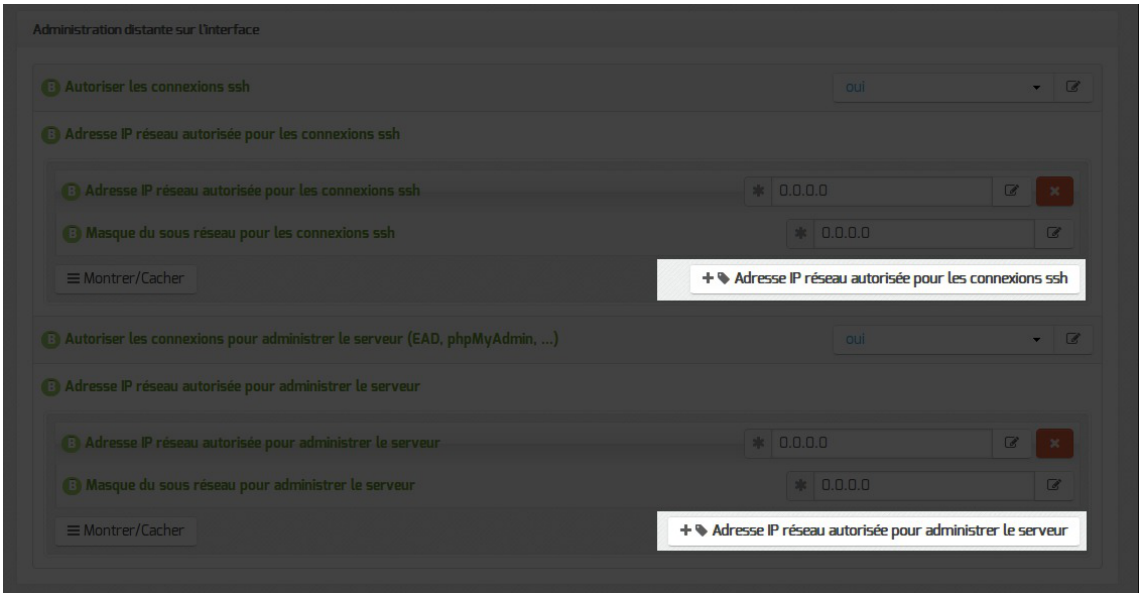


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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)

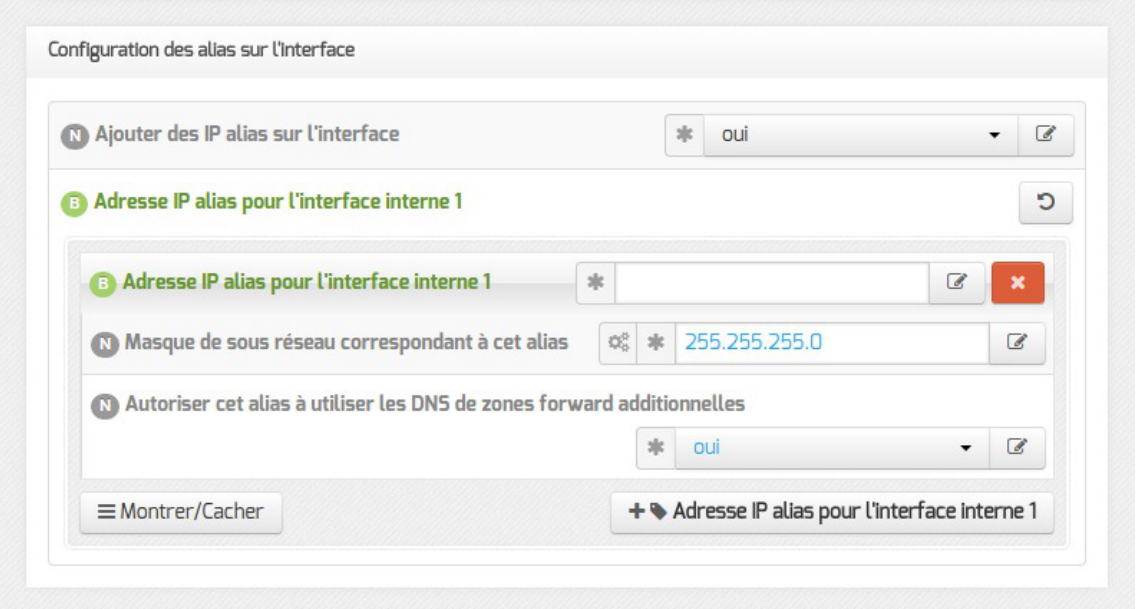
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

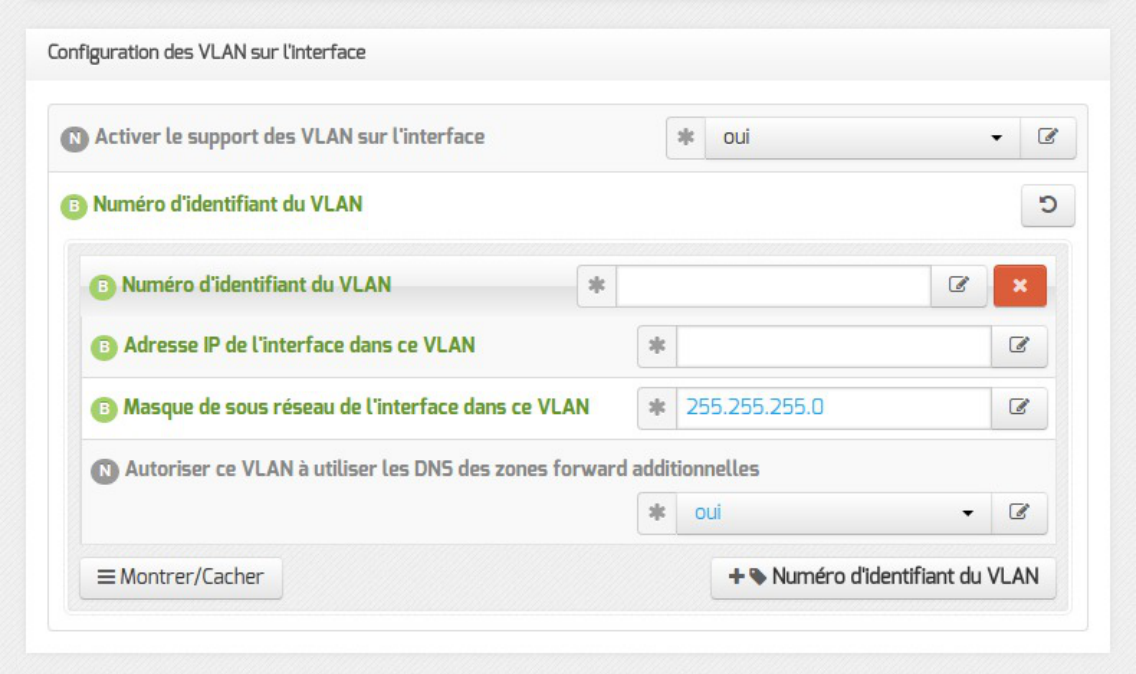
Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

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

Configuration des VLAN sur l'interface

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

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



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

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

Configuration DNS sur l'interface-0

Sur une installation en mode une carte (exemple : EoleBase + `eole-dns`), le DNS est activable ou désactivable dans l'onglet `Interface-0` avec la variable : `Activer le serveur DNS sur cette zone`.



Sur le module Amon et ses variantes (AmonEcole, AmonEcole+), cette question est également présente dans l'onglet `Interface-0`.

Pour chacune des interfaces configurées, il est possible de préciser si le DNS est maître de la zone en passant la variable `Serveur master DNS sur cette zone` à `oui`.



Au moins une des zones doit être configurée en maître de la zone.

Voir aussi...

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

> Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.60]

3.8. Onglet Interface-1

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

Configuration de l'interface



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

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

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

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



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

Un rechargement du module réseau ou plus simplement un redémarrage du système est

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

nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

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



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

Mode de connexion pour l'interface

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

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

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

Liste des valeurs possible :

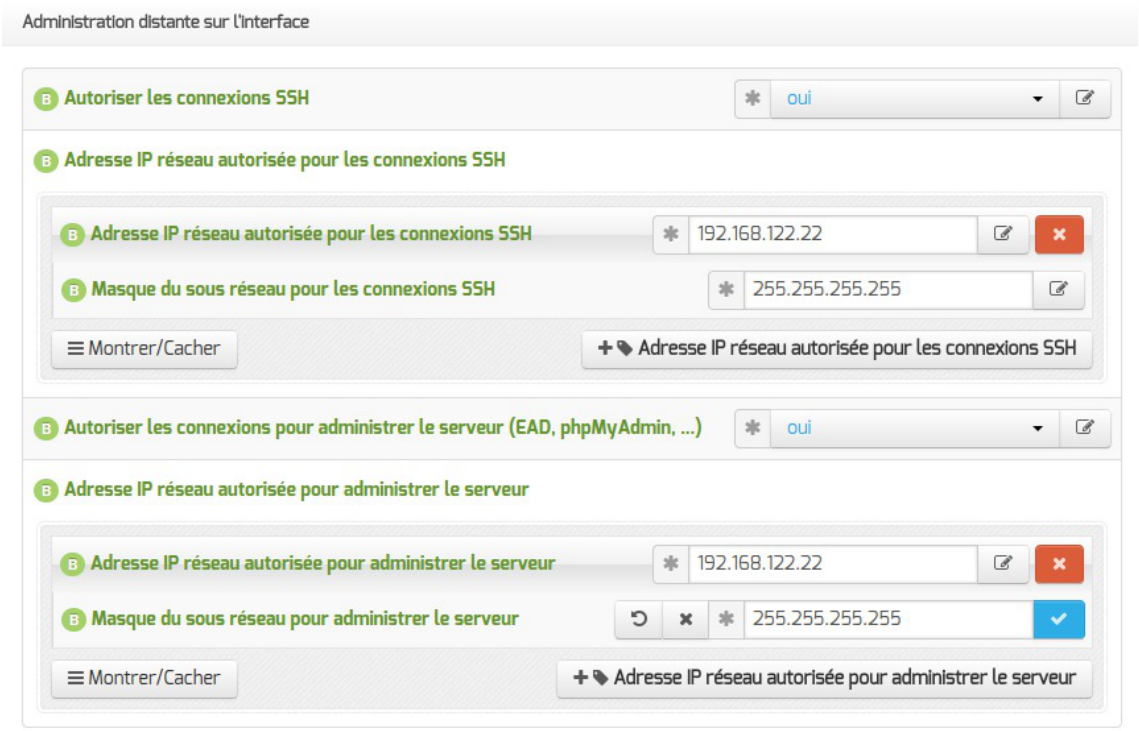
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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



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

Administration à distance

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

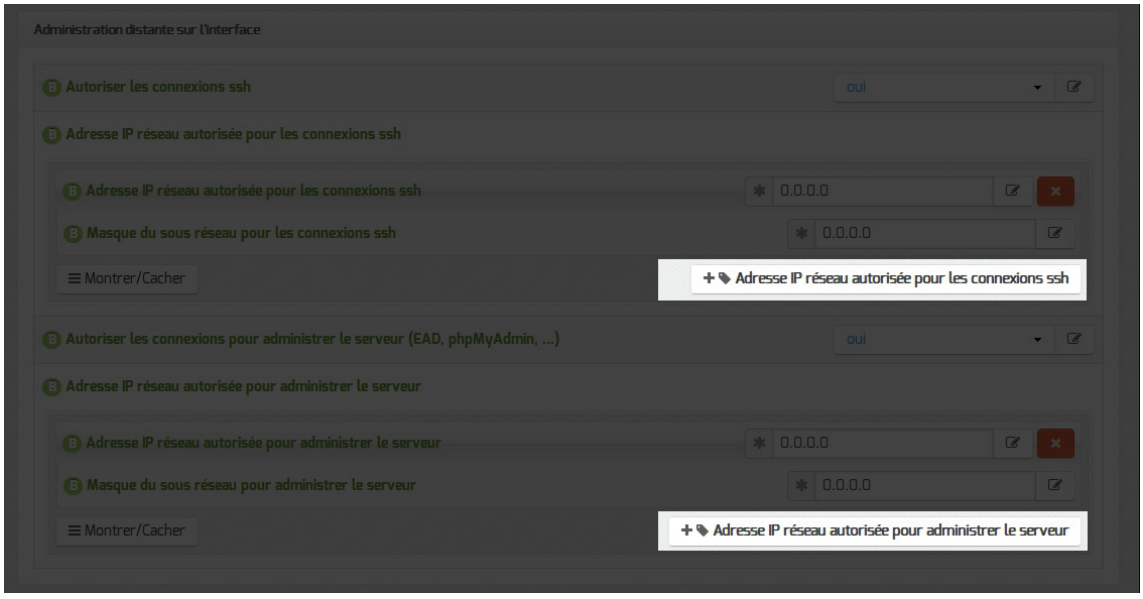


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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)

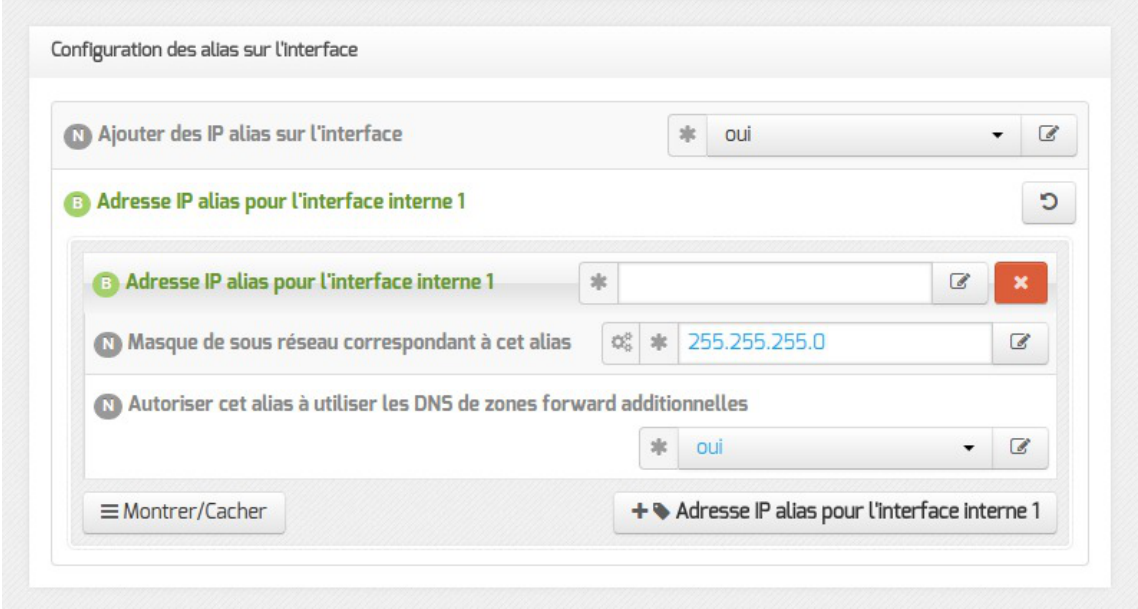
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

> 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.

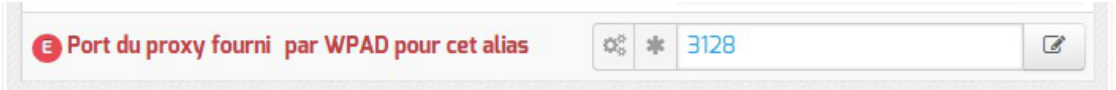


Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

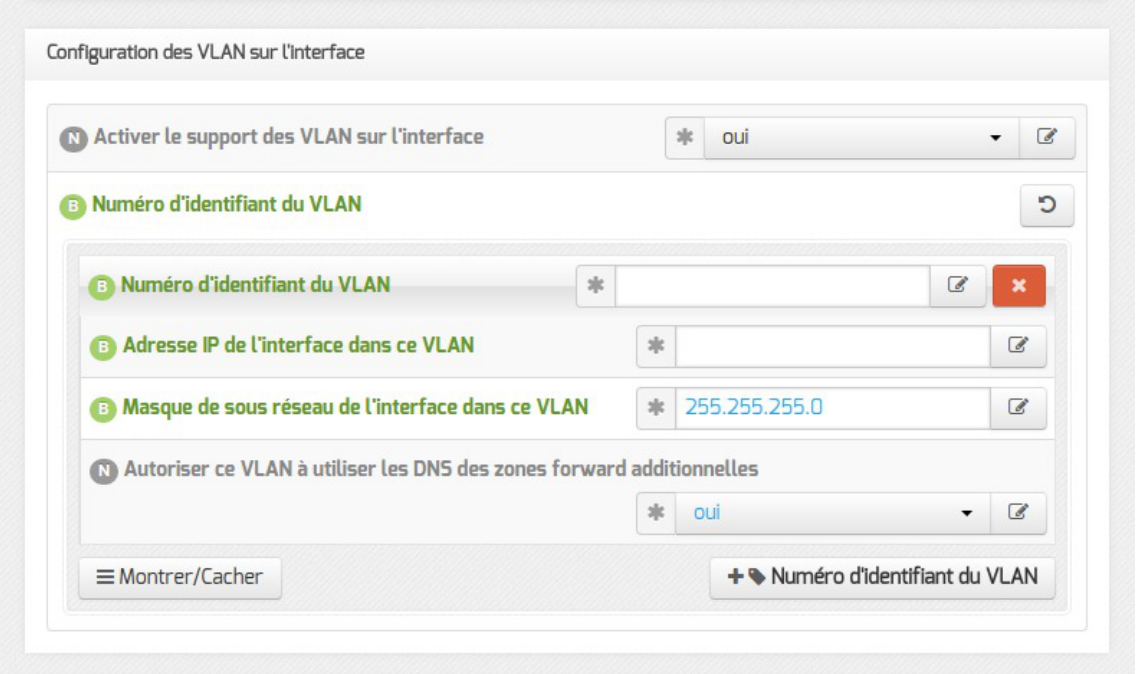


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration des VLAN sur l'interface

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



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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un VLAN donné.

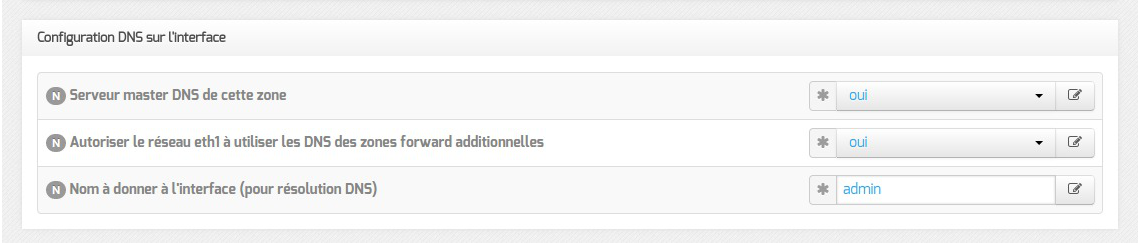


Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.

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



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.
- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

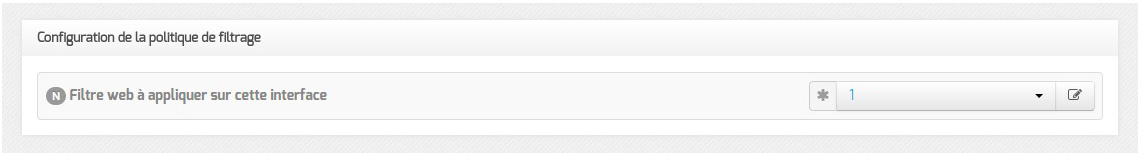
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Configuration de la détection automatique du proxy

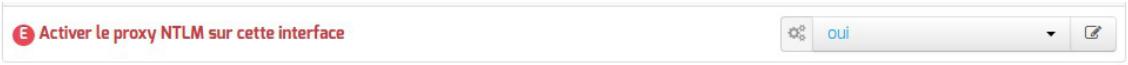
En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour l'interface.



> Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Si le proxy NTLM est activé, la variable `Activer le proxy NTLM sur cette interface` permet de le désactiver pour cette interface de façon spécifique.

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



Voir aussi...

> Onglet Filtrage web : Configuration du filtrage web [p.209]

3.9. Onglet Interface-n

Nombre d'interfaces

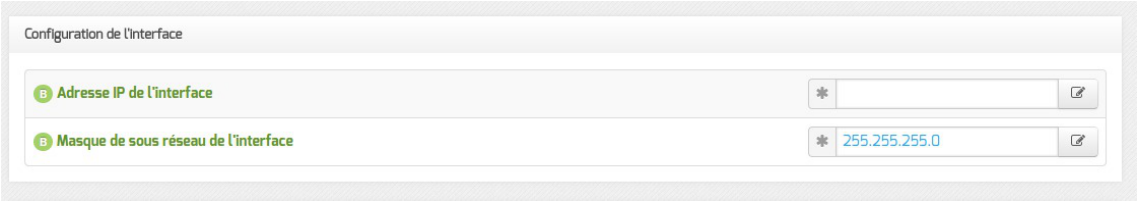
Un module Amon peut avoir de 2 à 5 cartes réseau.

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



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

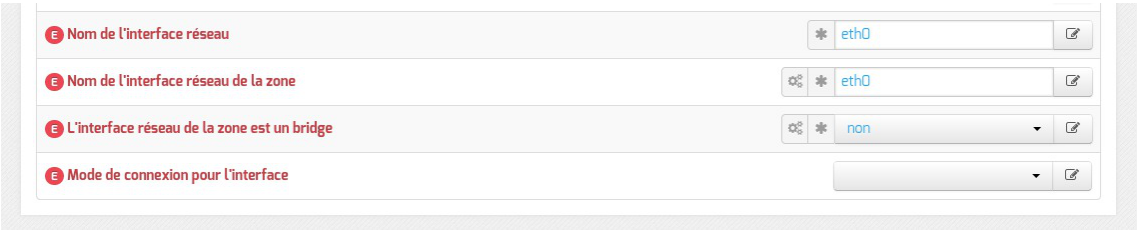
Configuration de l'interface



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

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

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

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



Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier

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

> `/etc/udev/rules.d/70-persistent-net.rules`.
>
> Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

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



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

Mode de connexion pour l'interface

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

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

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

Liste des valeurs possible :

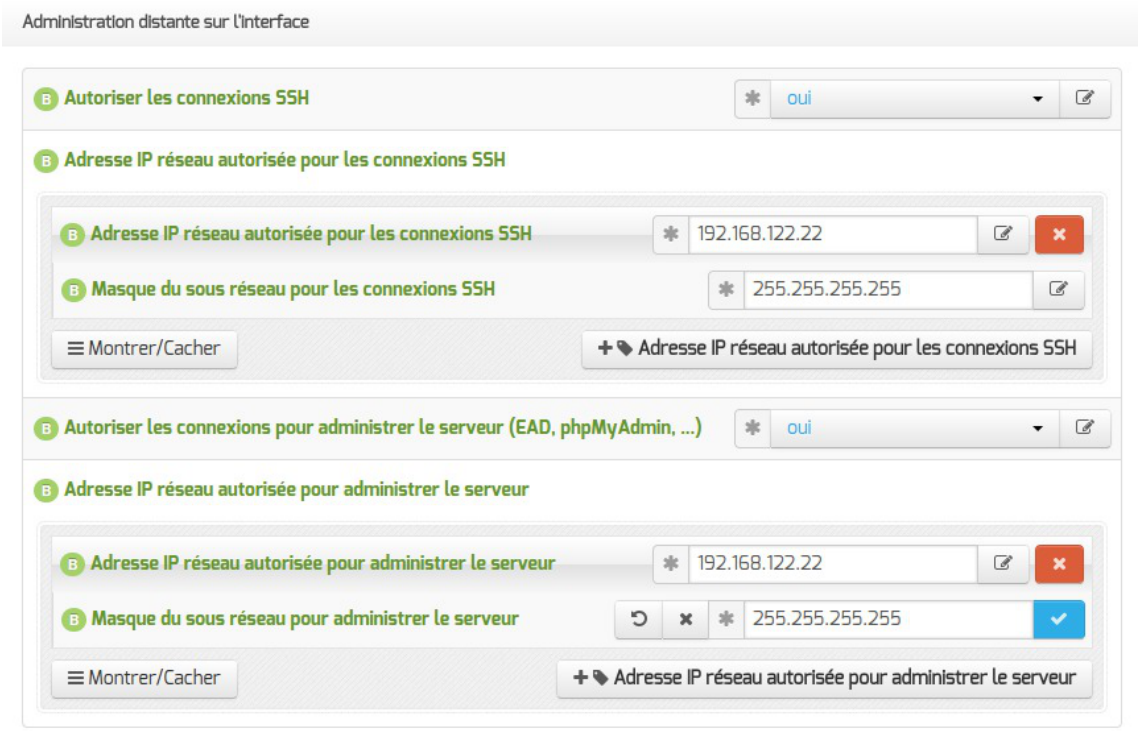
- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) :
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbits/s en half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



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

Administration à distance

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

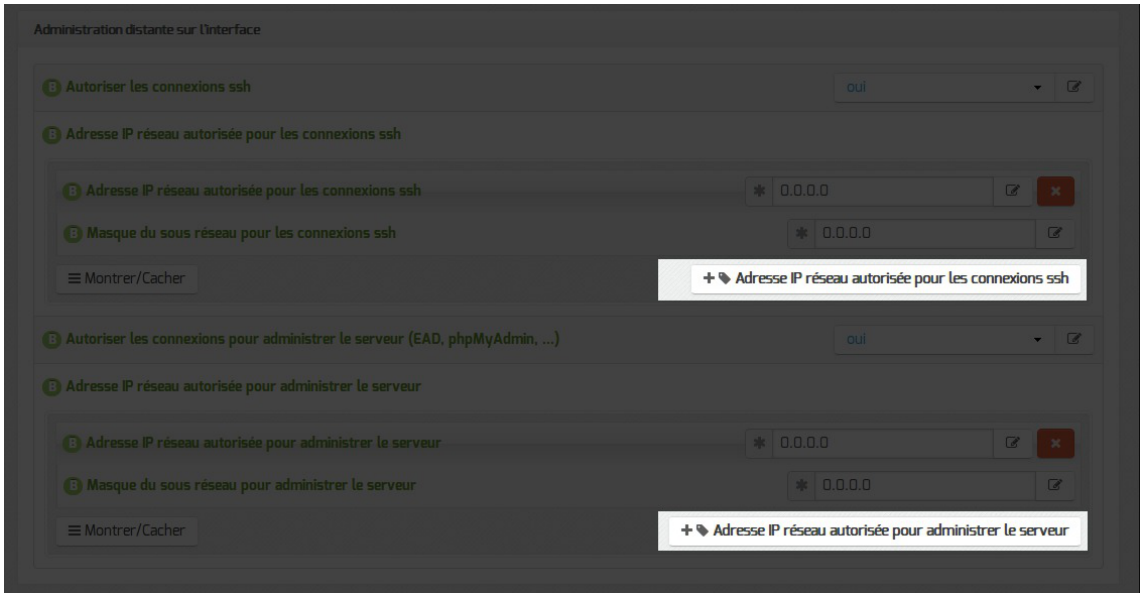


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.902] 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)

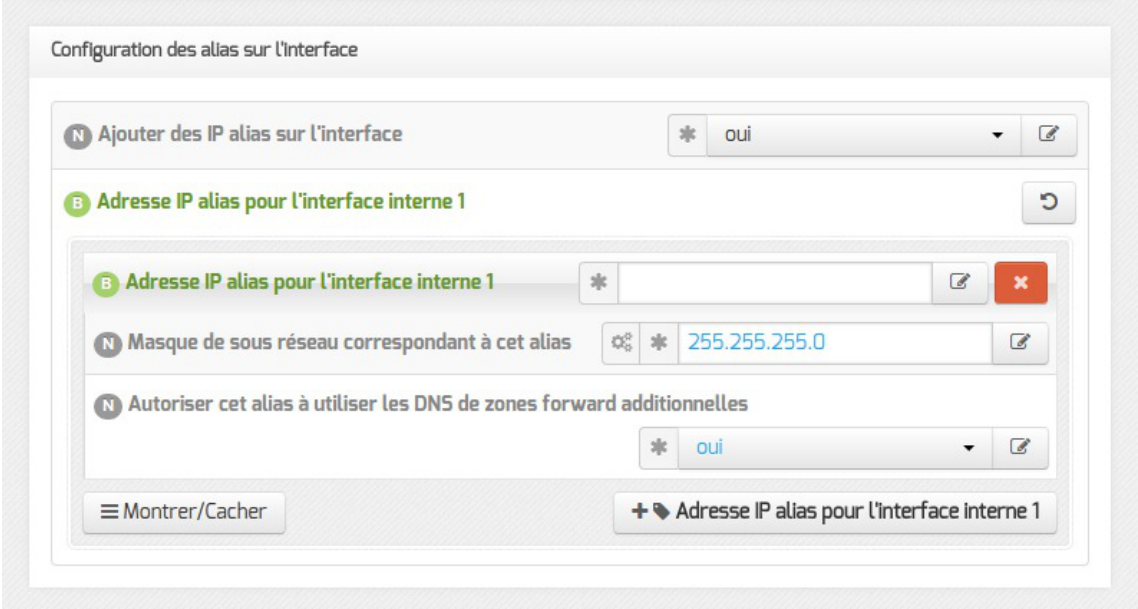
> `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

> 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.

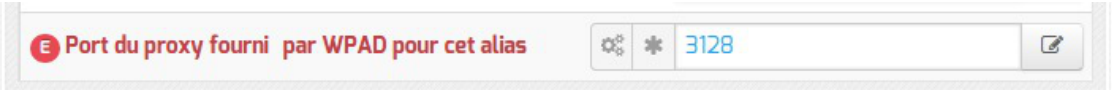


Pour cela, il faut activer son support (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous réseau.

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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

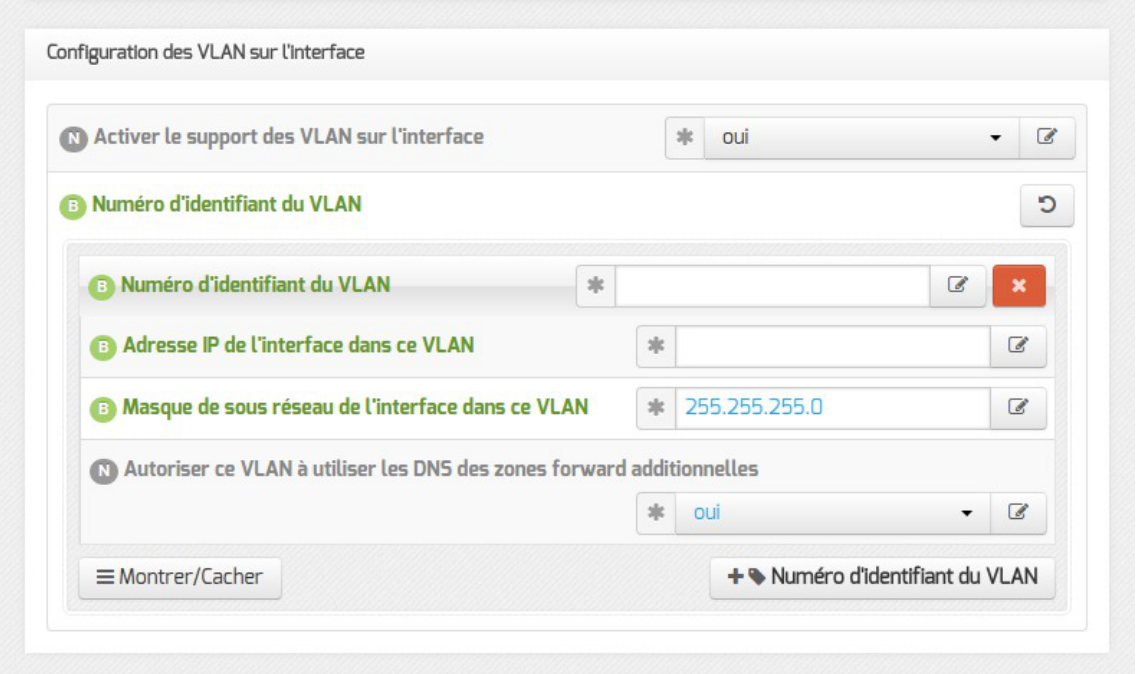


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration des VLAN sur l'interface

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



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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un VLAN donné.

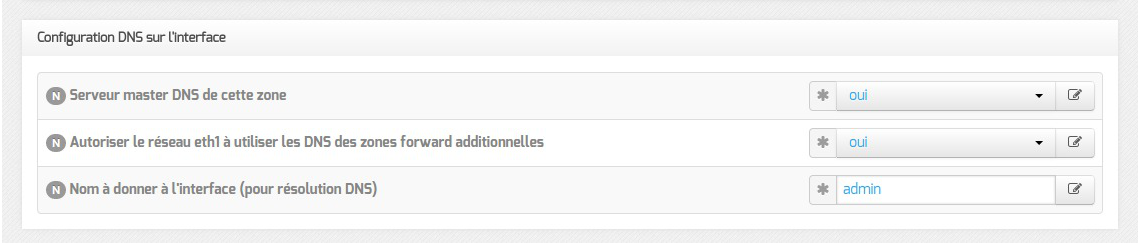


Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.

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



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.
- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

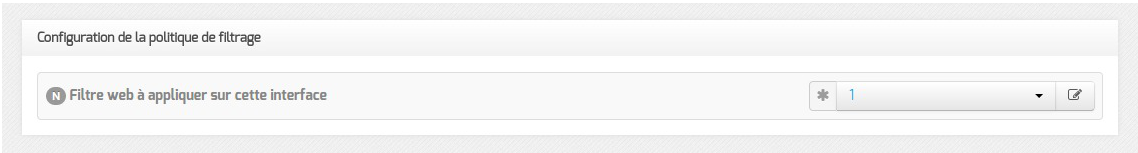
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de chaque interface (onglets : `Interface-1`, `Interface-2`, ...).



Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet `Filtrage web`.

Configuration de la détection automatique du proxy

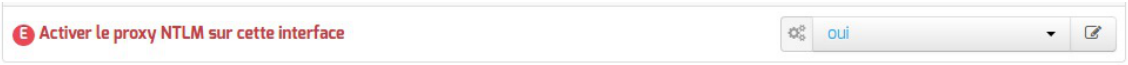
En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour l'interface.



Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Si le proxy NTLM est activé, la variable `Activer le proxy NTLM sur cette interface` permet de le désactiver pour cette interface de façon spécifique.

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



Voir aussi...

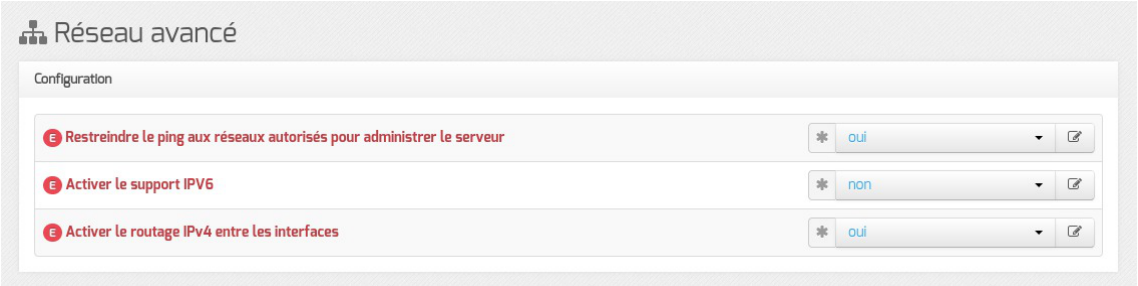
Onglet Filtrage web : Configuration du filtrage web [p.209]

Onglet Proxy authentifié : 5 méthodes d'authentification [p.95]

3.10. Onglet Réseau avancé

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

Configuration IP



Même si la fonctionnalité `Restreindre le ping aux réseaux autorisés pour administrer le serveur` apparaît dans l'onglet `Réseau avancé` du présent module, elle n'a aucun effet.

C'est dans les modèles ERA que sont décrites les restrictions liées au protocole ICMP[p.891].

À partir de la version 2.5.2, cette variable n'apparaît plus sur le présent module.

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.892] 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`.

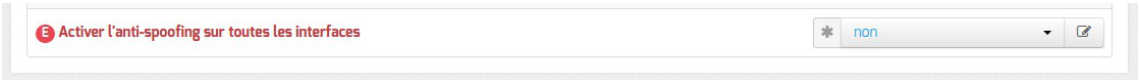
Si cette dernière est à `oui` le routage IPv6 est activé au niveau du noyau (`/proc/sys/net/ipv6/conf/all/forwarding` passe à `1`).

Sécurité

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



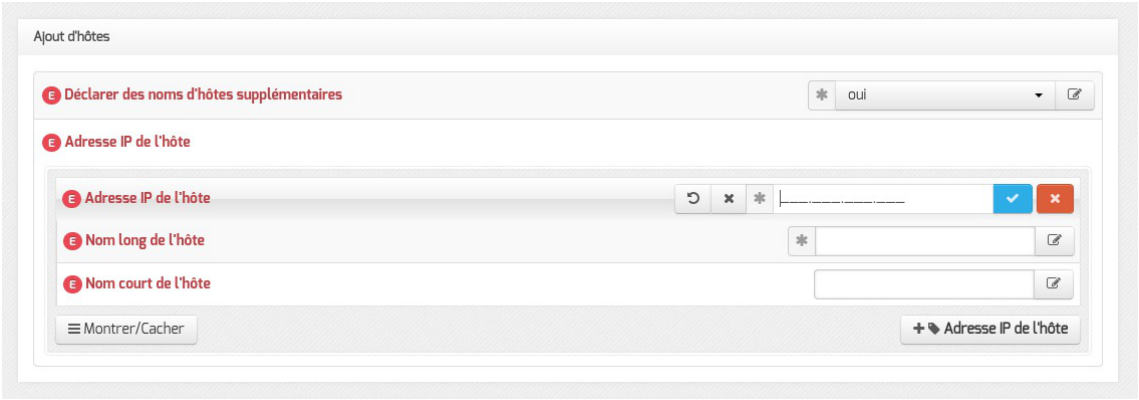
Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.883] est activé sur l'interface-0 des modules EOLE.

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

Ajout d'hôtes



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

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

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

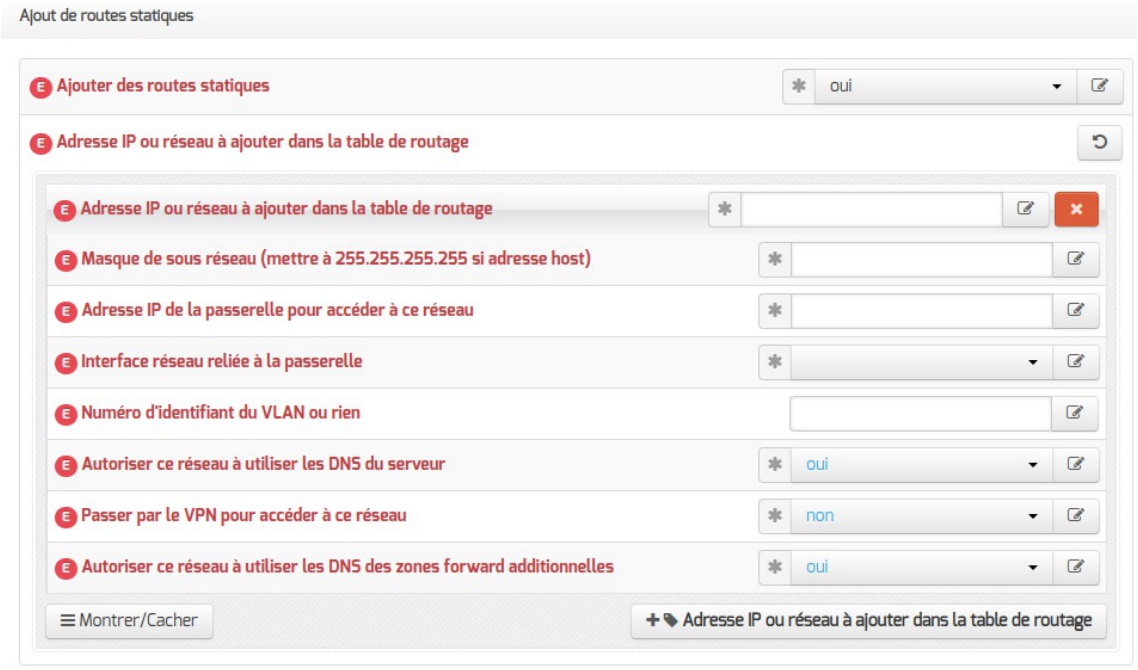


Sur les serveurs EOLE faisant office de serveur DNS, comme les modules Amon et AmonEcole, pour que le logiciel BIND[p.884] puisse résoudre un nom, il faut que le suffixe DNS de ce nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

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 ajouter les paramètres suivants :

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

Si le support du RVP est activé une option supplémentaire est disponible :



- `Autoriser ce réseau à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non les machines du réseau à résoudre les noms d'hôte de la zone AGRIATES.

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

Configuration du MTU



La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.893] (/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.891] 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.893] pour l'interface externe.

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

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

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

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

Configuration de la "neighbour table"



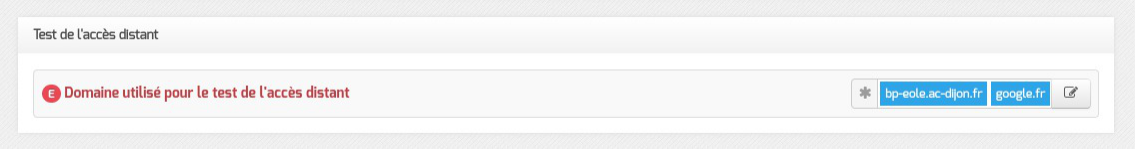
Les variables `ipv4 neigh default gc thresh1`, `ipv4 neigh default gc thresh2` et `ipv4 neigh default gc thresh3` servent à gérer la façon dont la table ARP évolue :

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;

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

- **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...

Onglet Zones-dns : Configuration du DNS [p.196]

Résoudre des dysfonctionnements liés au MTU [p.790]

3.11. Onglet Certificats ssl : gestion des certificats SSL

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

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

Certificats par défaut

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

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

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

- `ca_local.crt` ;
- `ACInfraEducation.pem` ;

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

- tout certificat présent dans le répertoire `/etc/ssl/local_ca/`

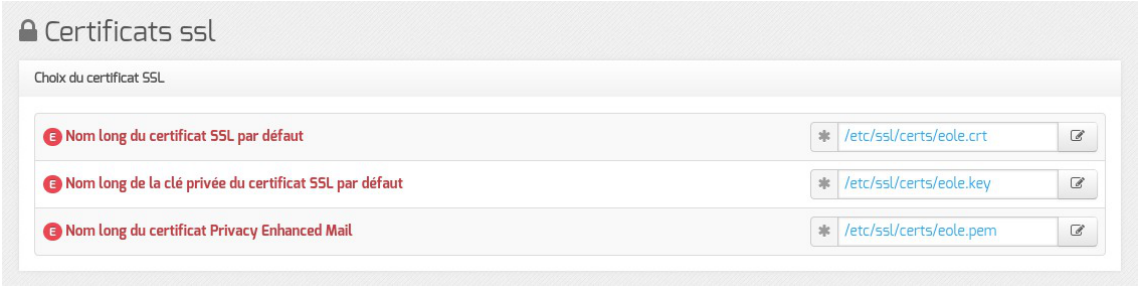
Détermination du nom de serveur (commonName) dans le certificat

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

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

Mise en place d'un certificat particulier

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



- `Nom long du certificat SSL par défaut` (server_cert) : chemin d'un certificat au format PEM à utiliser pour les services ;
- `Nom long de la clé privée du certificat SSL par défaut` (server_key) : chemin de la clé privée correspondante (éventuellement dans le même fichier).

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

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

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

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

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



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

Création de nouveaux certificats

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

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

Génération d'un certificat avec gen_certif.py

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

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

Étapes à suivre :

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

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

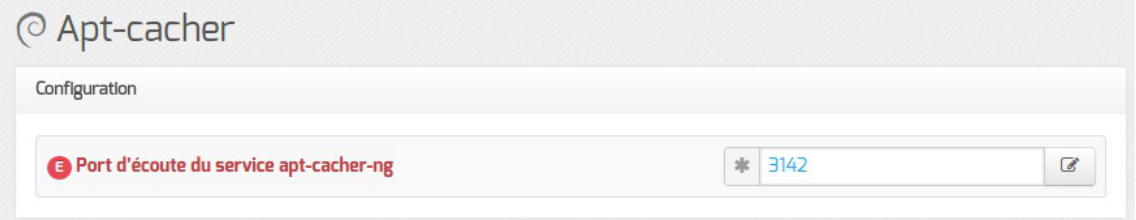
Certificats intermédiaires

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

3.12. Onglet Apt-cacher

Pour mettre en œuvre les services du module Amon et du module Scribe sur une même machine le module AmonEcole est en mode conteneur.

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



Il est possible dans cet onglet de changer le port d'écoute par défaut de ce service.

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

3.13. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité

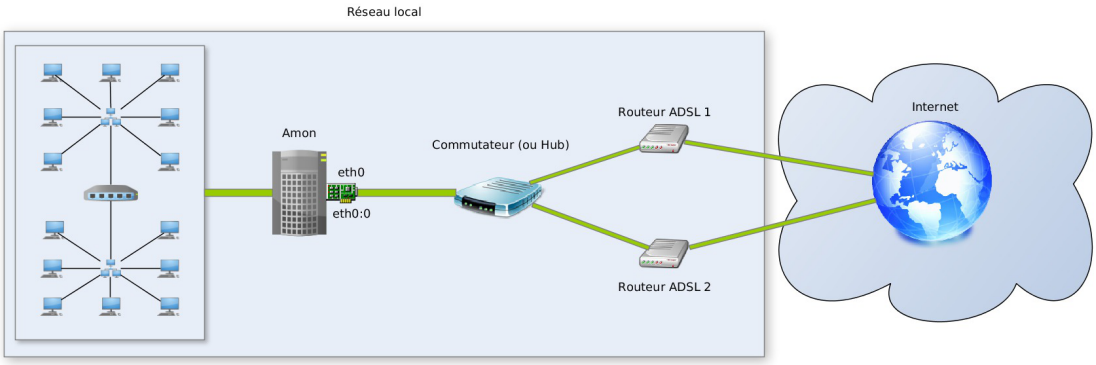
Présentation et mise en place de l'agrégation de liens

L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Les deux routeurs sont reliés entre eux par un commutateur (ou un Hub) à la carte eth0 du module Amon.

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP[p.899] et OSPF[p.896] ;
- il faut un service qui surveille l'état de chacun des liens.



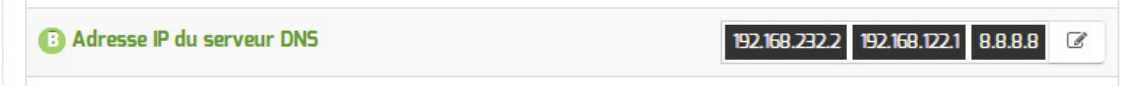
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie.

La première version a été réalisée par l'académie de Versailles, puis elle a été améliorée successivement par les académies de Nantes et de Lyon.

Onglet Général

Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



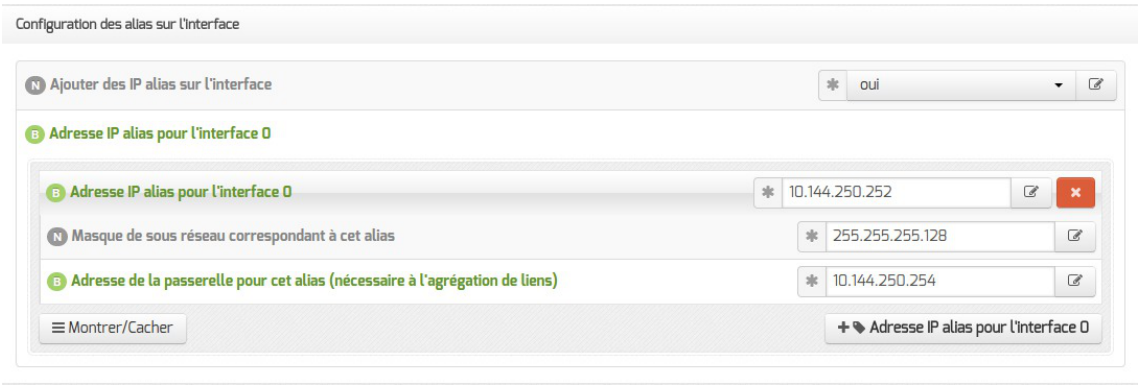
Onglet Interface-0

Il faut, en premier lieu, déclarer un alias sur l'interface eth0 dans la section `Configuration des alias sur l'interface`.

Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès

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

du second lien.



Création d'un alias sur eth0 pour l'agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.

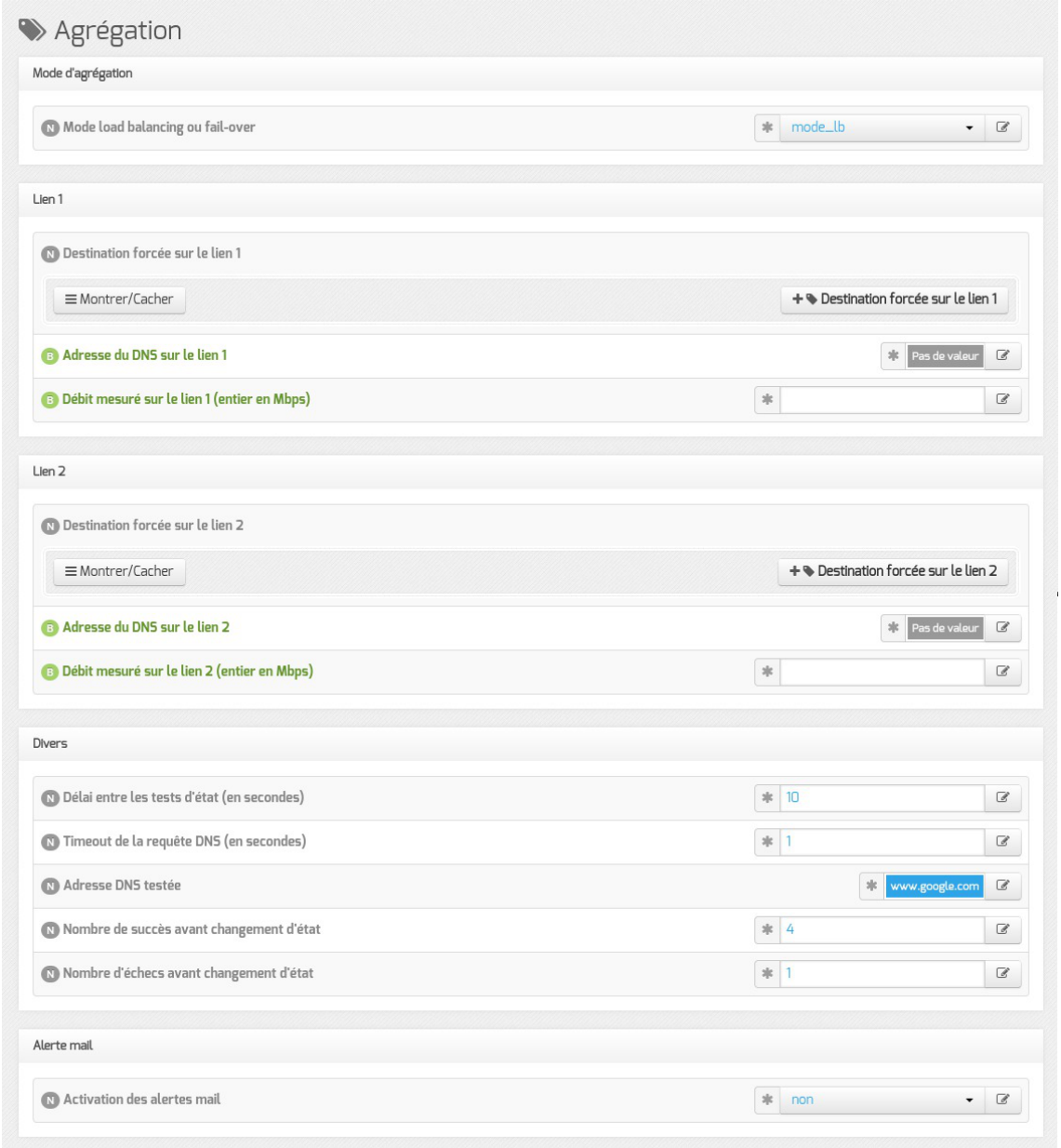


Un nouvel onglet, `Agrégation`, est disponible.

Onglet Agrégation : Configuration de l'agrégation de liens

Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.

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



Paramétrage de l'agrégation de liens

Modes d'agrégation



Il existe deux modes d'agrégation :

- le mode `mode-lb` (pour load balancing) correspond à la répartition de charge et fonctionne avec la notion de poids à utiliser sur les différentes passerelles ;
- le mode `mode-fo`, (pour fail-over) un seul lien est utilisé à la fois, il n'y a plus de notion de poids et il n'y a plus qu'une seule route par défaut.

Dans les deux modes il est possible de forcer des destinations IP ou réseau, et dans les deux cas si un lien tombe tous les flux (et également les destinations forcées) sont redirigés vers le second lien.

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

Quand les deux liens sont fonctionnels, on se retrouve dans la configuration de départ.



Le VPN, de par son mode de fonctionnement, ne peut pas être réparti entre plusieurs abonnements.

Tout le trafic devant passer par un seul lien, il est nécessaire d'utiliser le mécanisme de destination forcée.

Que le `Lien 1` ou le `Lien 2` soit choisi pour faire transiter le VPN, s'il devient indisponible, le VPN ne fonctionnera plus.

Adresse des DNS

Les champs `Adresse du DNS sur le lien 1` et `Adresse du DNS sur le lien 2` sont des champs obligatoires pour le bon fonctionnement de l'agrégation.



Les adresses DOIVENT être différentes sur chaque lien car c'est avec ces DNS que se font les tests d'état des liens.

Adresse DNS testée

Il est possible de spécifier plusieurs mires de tests qui seront testées afin de déterminer l'état des liens (résolution DNS avec le serveur DNS de chacun des liens).



L'ensemble des DNS doit être déclaré dans l'onglet `Général`.

Alerte mail



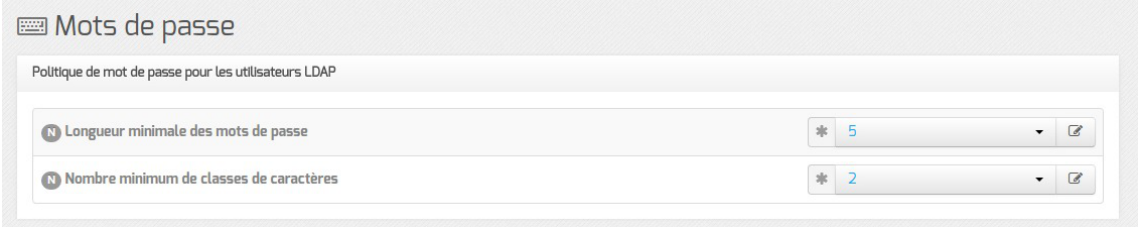
Lorsque l'un des liens est coupé, le message suivant est envoyé : `Seul le lien 2 est actif, redirection des flux sur ce lien`.

Quand les deux liens sont de nouveaux fonctionnels, le message suivant est envoyé : `Rechargement de la répartition sur les 2 liens`.

3.14. 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.

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 sera à terme propagée à toutes les interfaces fournissant cette fonctionnalité (EAD, portail...). 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.885] 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.

3.15. 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

L'onglet Clamav n'est accessible que si le service est activé dans l'onglet Services. Pour ce faire, passer la variable `Activer l'anti-virus ClamAV` à `oui`.

Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.

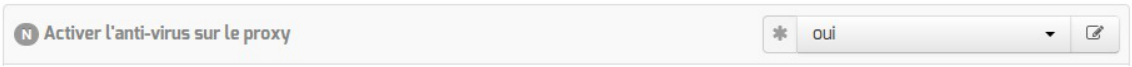


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 le proxy

Pour activer l'anti-virus en temps réel sur les fichiers filtrés par le proxy Internet, il faut passer la variable Activer l'anti-virus sur le proxy à oui dans l'onglet Clamav.

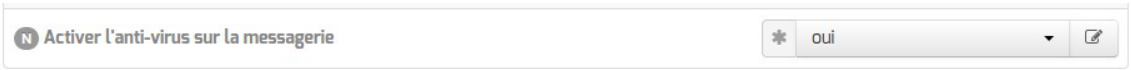


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.886]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

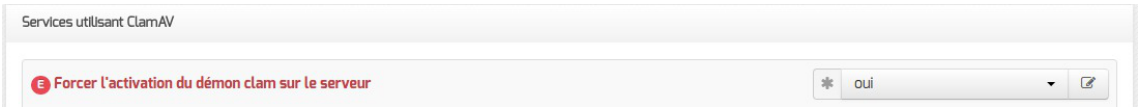
Pour activer l'anti-virus sur la messagerie il faut passer la variable Activer l'antivirus sur la messagerie à oui dans l'onglet Clamav.



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.

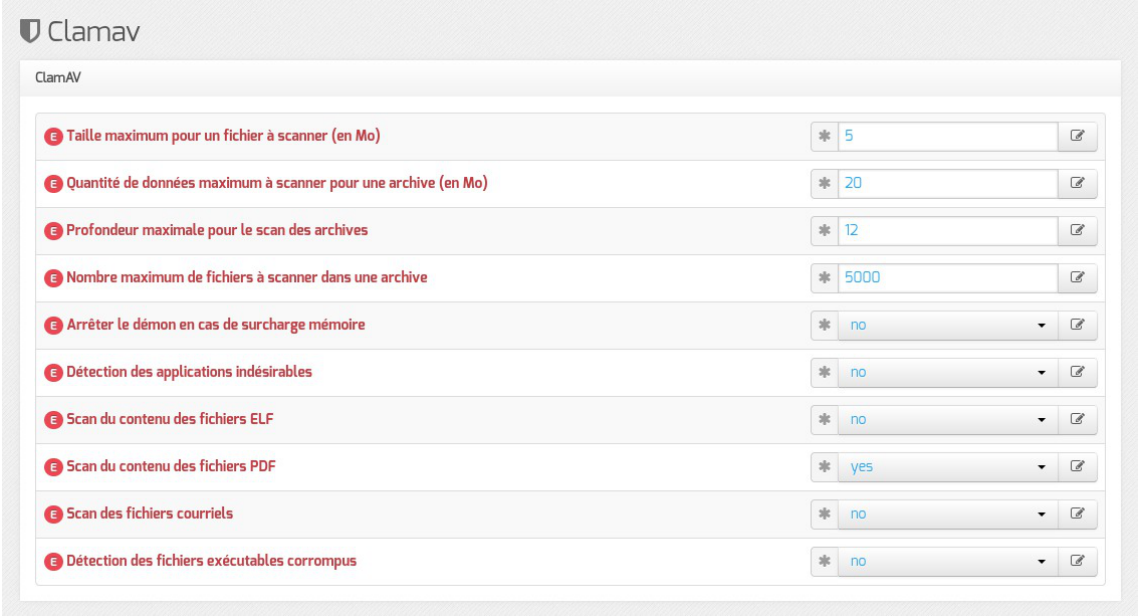
À partir de la version 2.5.2 d'EOLE, il est possible de forcer l'activation du service anti-virus (clamd) en passant la variable du mode expert Forcer l'activation du démon clam sur le serveur à oui dans l'onglet Clamav.



Configuration avancée

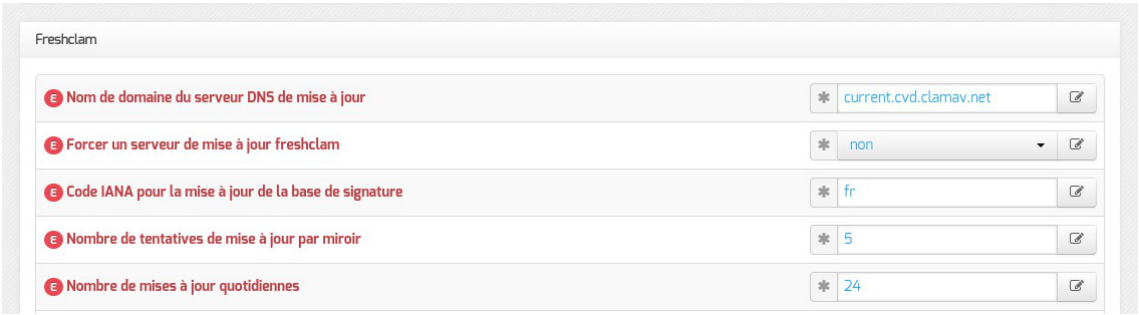
En mode expert, l'onglet Clamav comporte de nombreuses variables qui permettent d'affiner la configuration de ClamAV.

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



- `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` ;
- `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.888] ;
- `Scan du contenu des fichiers PDF` ;
- `Scan des fichiers courriels` ;
- `Détection des fichiers exécutables corrompus`.

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` ;
- `Nombre de tentatives de mise à jour par miroir` permet de réduire le nombre de

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

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.

Contribuer

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

Il est possible de faire des signalements :

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

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

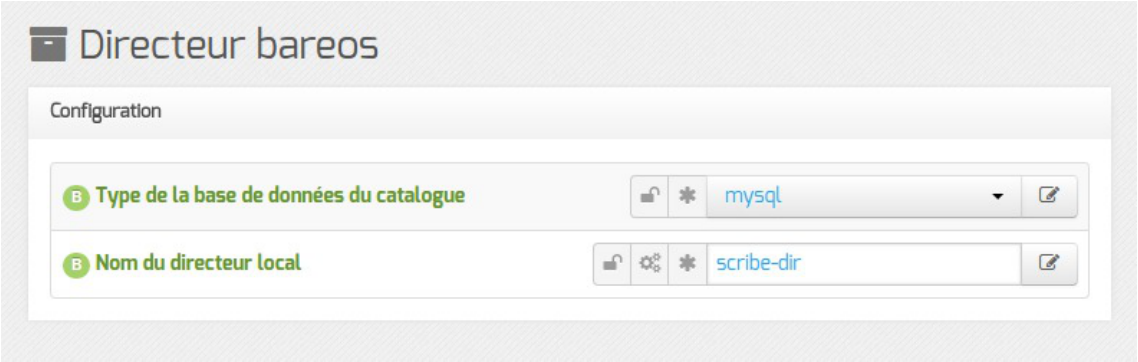
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

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



Il ne faut pas signaler des PUA[p.899] comme étant des faux positifs.

3.16. 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.

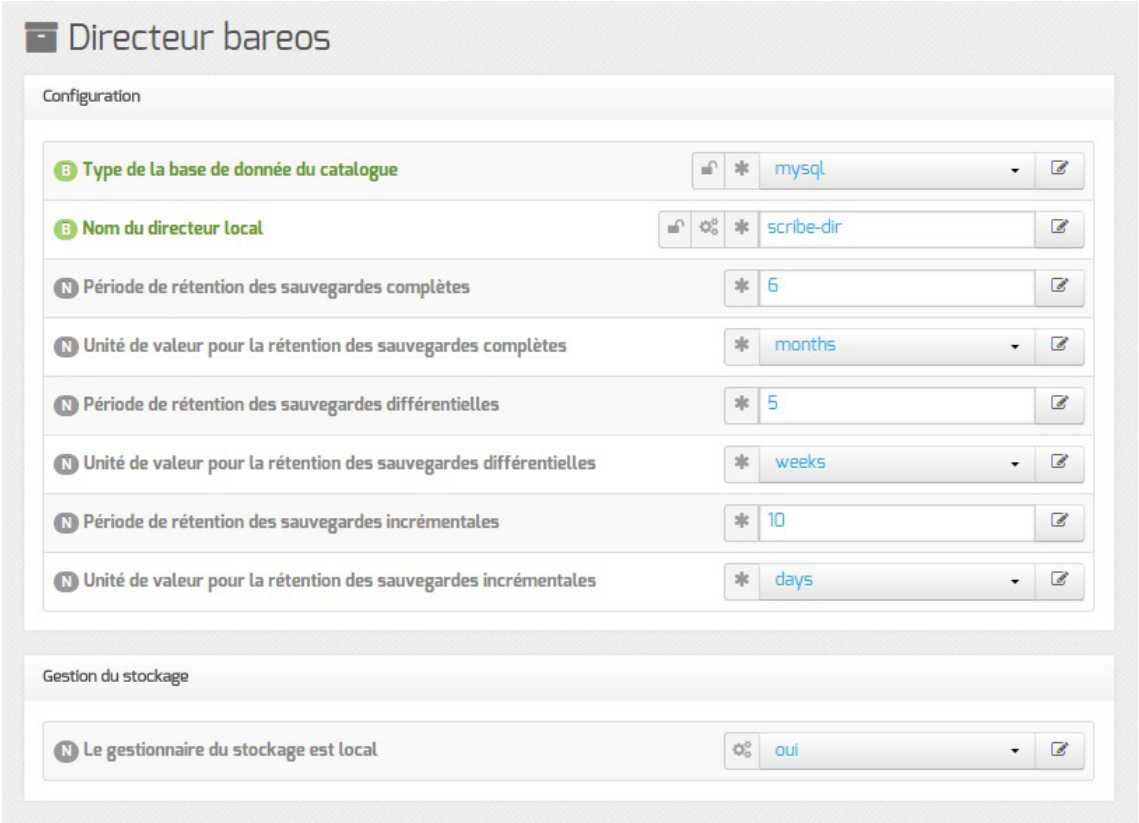


Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

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.888] 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.

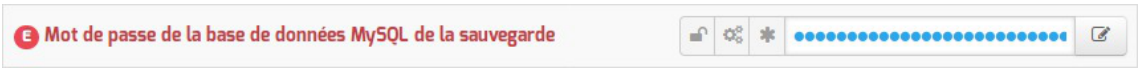
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

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.

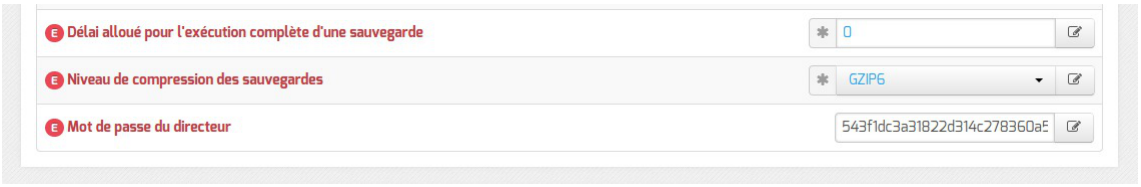
En mode expert, il est possible de définir manuellement le mot de passe de la base de donnée MySQL, le délai accordé à l'exécution de la sauvegarde ainsi que l'algorithme de compression utilisé pour le

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

stockage.



Vue de l'onglet Directeur Bareos



Type de compression et délai alloué

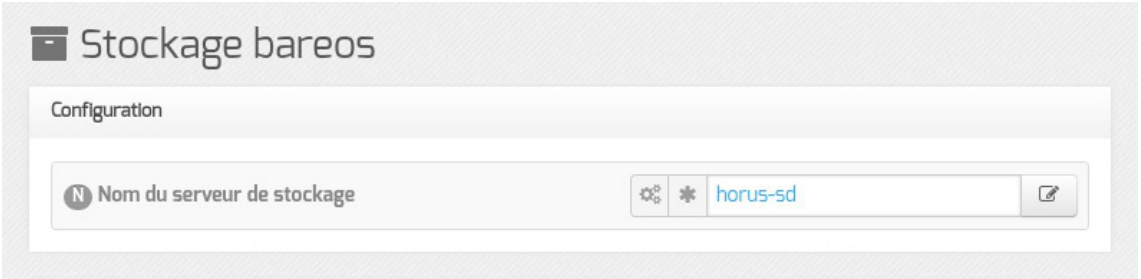
Le délai permet d'arrêter le job après un temps d'exécution fixé en seconde, par défaut le job n'a pas de limite de temps.

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.

3.17. 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.

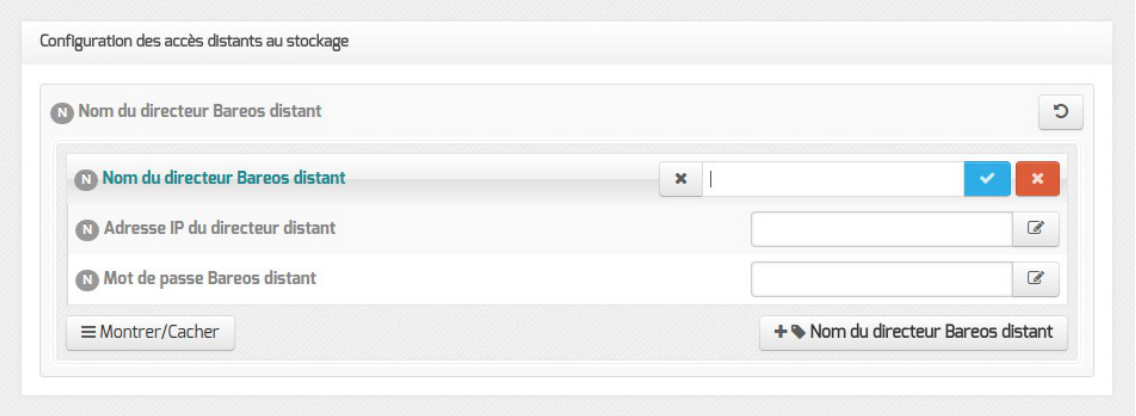


Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur `Nom du directeur Bareos distant`, le détail de l'autorisation s'affiche.

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

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

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



Autoriser des clients Bareos distants à se connecter au directeur

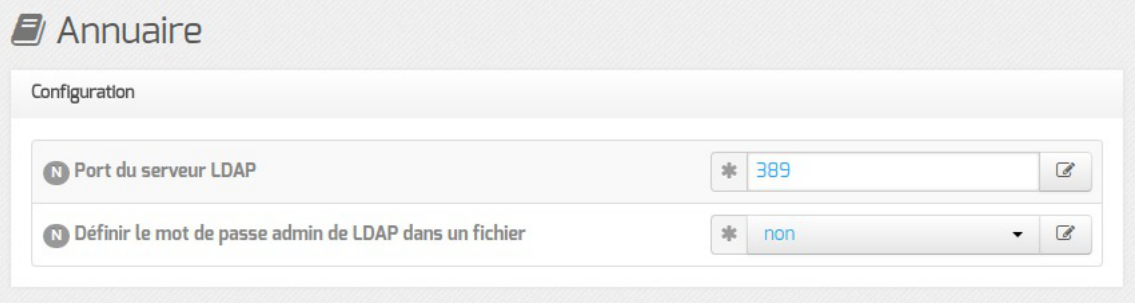
Les sauvegardes sont des informations sensibles. Il ne faut pas utiliser de mot de passe facilement déductible.

Voir aussi...

Les mots de passe

3.18. Onglet Annuaire

Sur le module Scribe l'annuaire OpenLDAP est local.



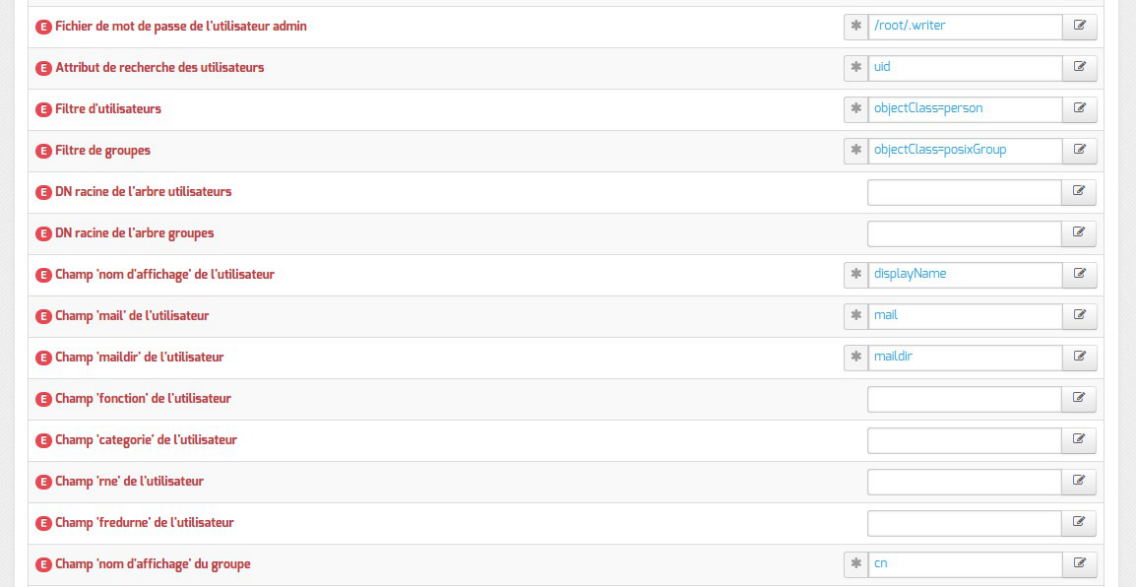
Lorsque l'annuaire est configuré comme étant local, l'onglet propose 2 paramètres :

- `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`.

Mode expert

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

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 se fait dans l'onglet `Openldap`.

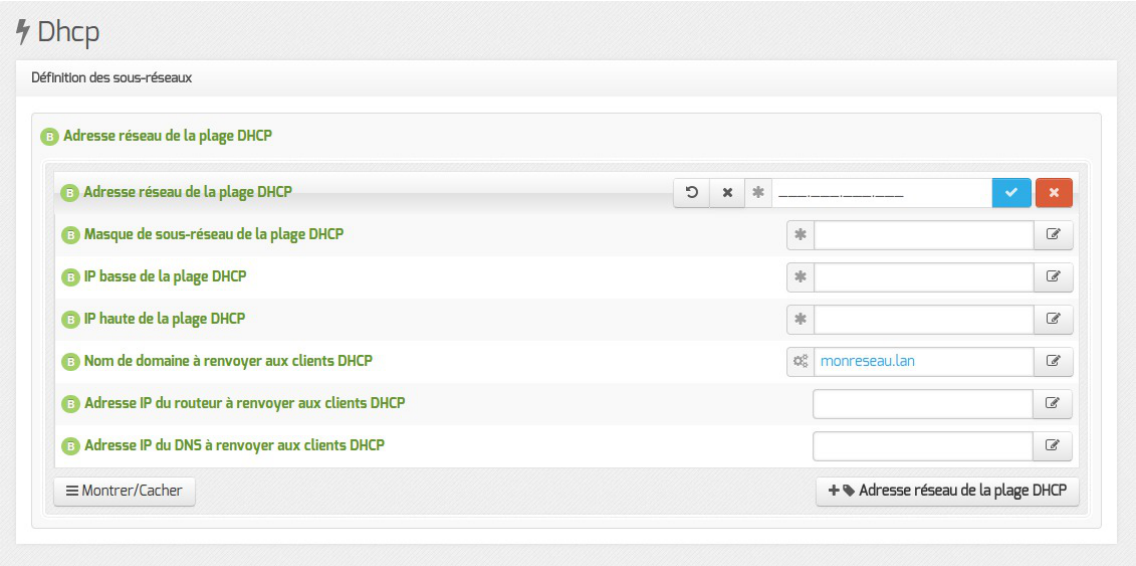
Voir aussi...

Onglet Openldap : Configuration du serveur LDAP local [p.206]

3.19. Onglet Dhcp : Configuration du serveur DHCP

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

L'onglet `Dhcp` apparaît uniquement s'il est activé.



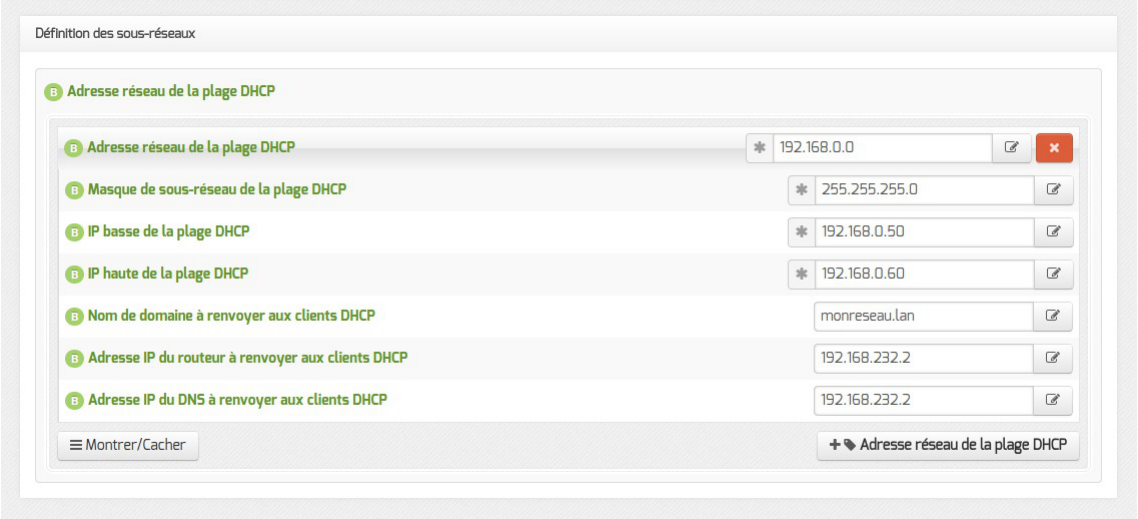
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sur les modules Scribe et Horus (mode une carte), les adresses servies doivent généralement être dans le même réseau que celui de l'Interface-0 (eth0).

Sur le module AmonEcole et ses dérivés, les adresses servies sont celles sur réseau interne (interface `eth1`).

Si le serveur est installé en DMZ, on pourra renseigner des adresses du réseau administratif/pédagogique mais dans ce cas, il faudra activer le relayage du DHCP sur le pare-feu.

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.

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.889] 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 préférable d'utiliser le module comme relais DNS[p.887], 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.

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 réseau spécifique.



Un certain nombre de paramètres peuvent être spécifiés ou modifiés dans le 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).

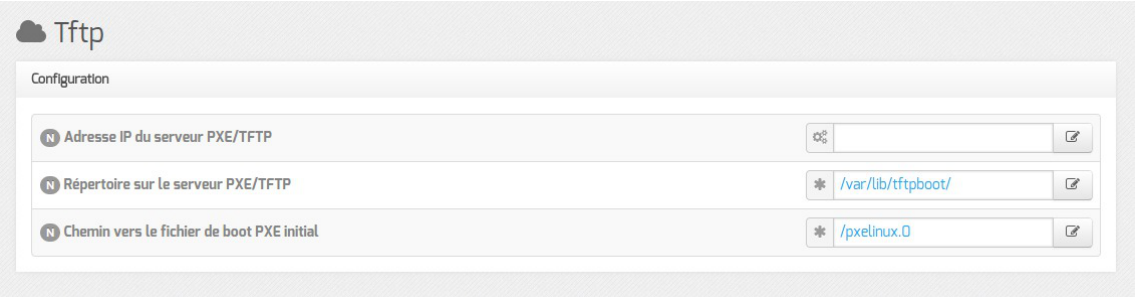
Il est possible de modifier les durée du bail DHCP : `Temps du bail par défaut (sec)` et `Temps maximum du bail (sec)`.

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

3.20. 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`.



Vue de l'onglet Tftp

L'adresse IP du serveur PXE/TFTP proposée par défaut est celle de l'interface `eth0` 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.896], outil de clonage édité par le CRDP de Lyon (http://oscar.crdp-lyon.fr) :

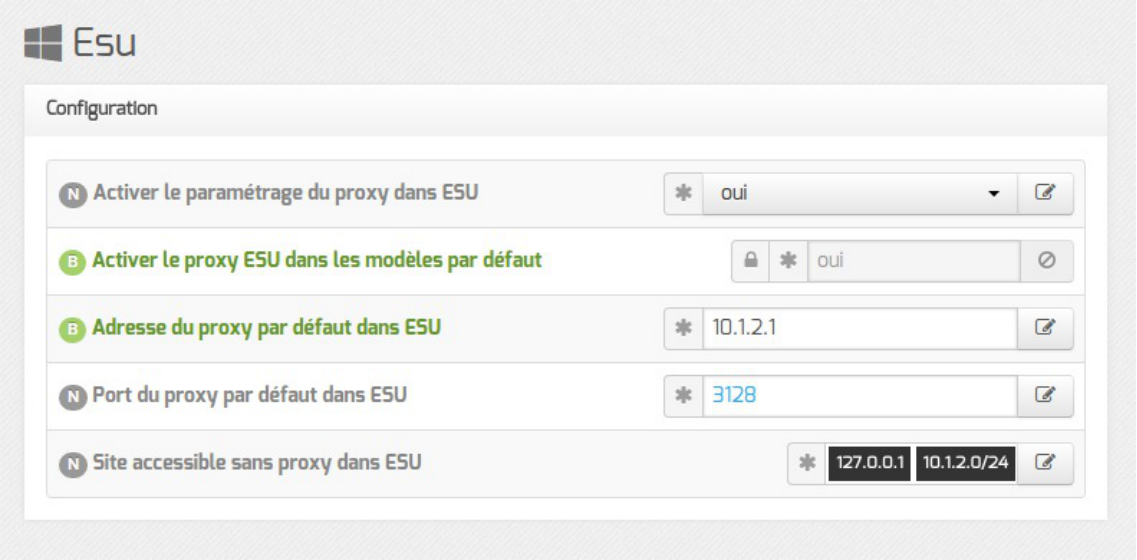
- Un procédure pour la mise en place d'OSCAR est disponible sur la forge EOLE à l'adresse : http://dev-eole.ac-dijon.fr/projects/oscar/wiki
- Une documentation sur l'utilisation d'OSCAR est disponible à l'adresse : http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/scribe/formationadminscribeoscar

3.21. 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 varibles 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`).

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.882] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG[p.882] tels que celui fourni par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

3.22. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC[p.898]) 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.).

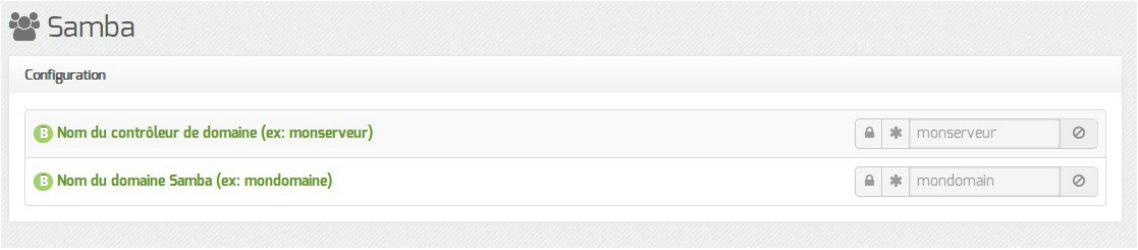
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

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.894]) 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`.

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

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.

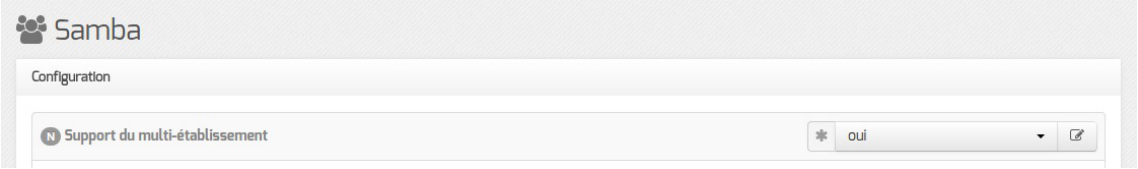
Dans la configuration de Samba, plusieurs types de fichiers ont été ajoutés pour les rendre invisibles des utilisateurs :

- 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`) ;
- .scanned:* : si l'anti-virus temps réel est activé, les fichier `.scanned:*` générés par Scannedonly[p.901] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

Mode multi-établissement

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

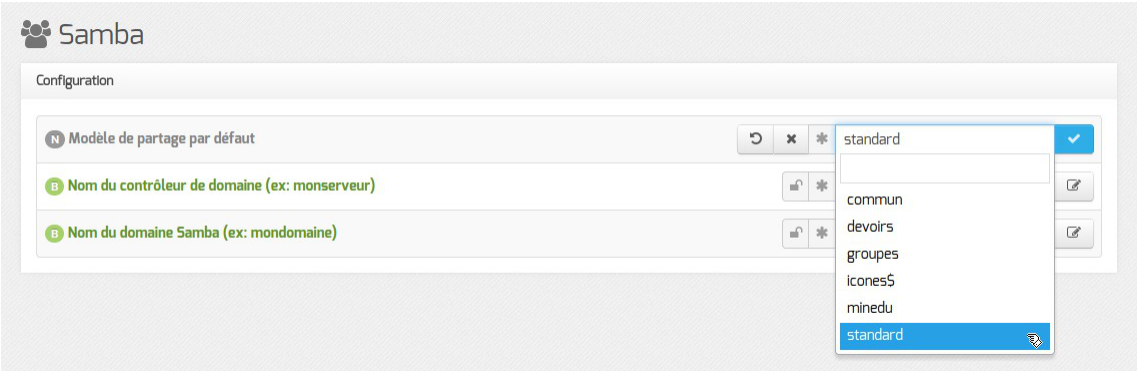
Pour certaines structures, une communauté de communes par exemple, il peut être intéressant de n'avoir qu'un seul module Scribe ou AmonEcole pour gérer plusieurs établissements.



Activation du mode multi-établissement dans l'interface de configuration du module

Pour activer le support du **mode multi-établissement** il faut passer la variable `Support du multi-établissement` à `oui`. Le paramétrage du mode multi-établissement se fait dans l'EAD.

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



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)

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

- `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.

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`

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

`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.

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.

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

Niveau de protocole maximum supporté par le serveur

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

Par défaut, la valeur sur un module EOLE 2.5.2 est `NT1`. Cette valeur **permettait** d'assurer la compatibilité avec Windows 10.

La valeur `default` 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 :

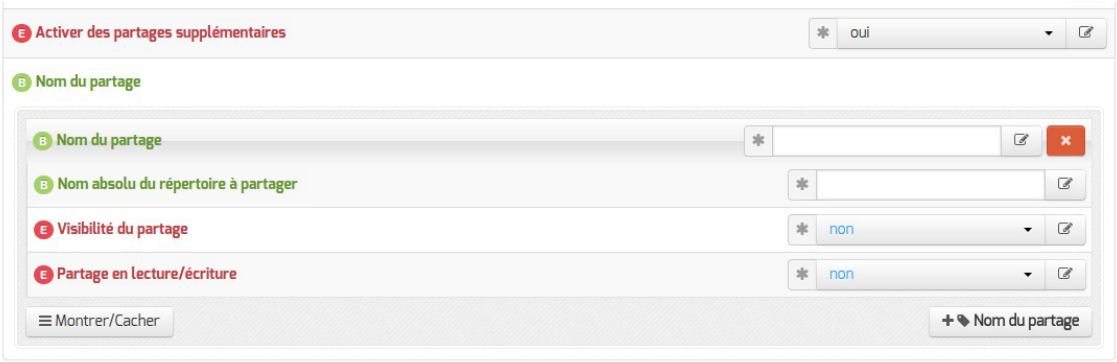
- de passer le niveau de protocole maximum à la valeur `default` sur le module gérant le domaine (Scribe, Horus ou AmonEcole) ;
- d'activer le support de partage de fichiers SMB 1.0/CIFS sur les postes clients.

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.

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



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 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/trusty/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`.

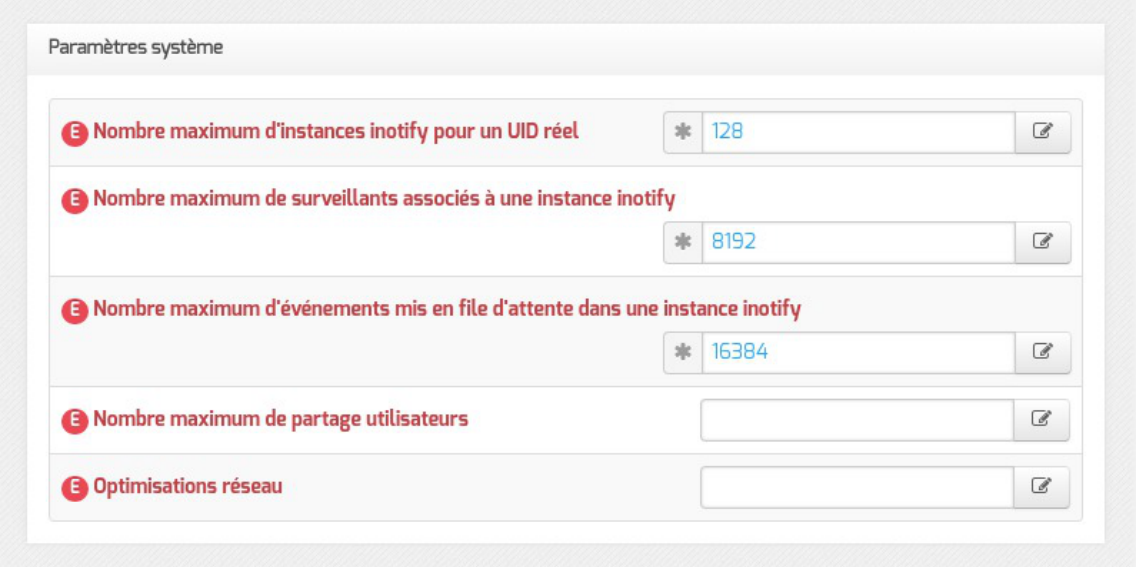
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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



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.

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

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

Anti-virus temps réel

Afin de limiter la propagation des virus à travers le réseau, une surveillance anti-virus temps réel est active sur les partages.

L'activation du service se gère en modifiant la variable `Activer l'anti-virus temps réel sur SMB` dans l'onglet `Clamav` de l'interface de configuration du module.

Attention cet onglet n'est visible que si le service ClamAV est lui même activé (`Activer l'anti-virus Clamav` à `oui`) dans l'onglet `Services`.

La durée de conservation des fichiers mis en quarantaine est paramétrable.

Lorsqu'un virus est détecté, il est renommé avec le préfixe `.virus:` et devient masqué pour l'utilisateur.



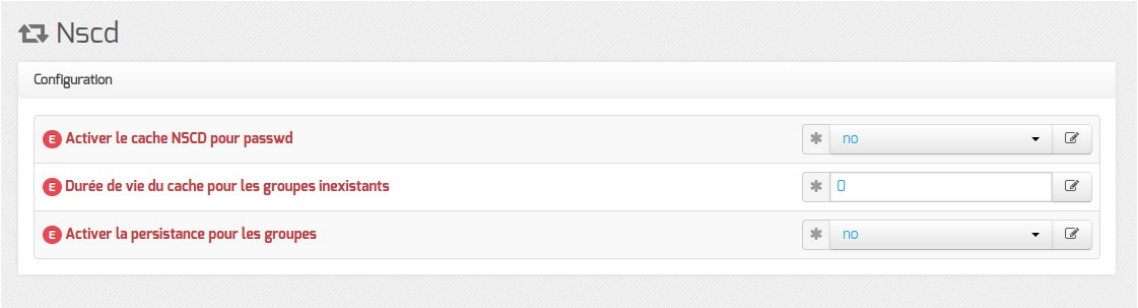
La consultation des fichiers infectés détectés et mis en quarantaine par le serveur peut se faire au travers de l'EAD.

Voir aussi...

- Onglet Clamav : Configuration de l'anti-virus
- Configuration du mode multi-établissement

3.23. Onglet Nscd

Nscd[p.895] est un démon qui fournit un cache pour limiter les requêtes vers 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 :

- `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

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

cache sera conservé lors du redémarrage du service nscd.

3.24. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.895]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

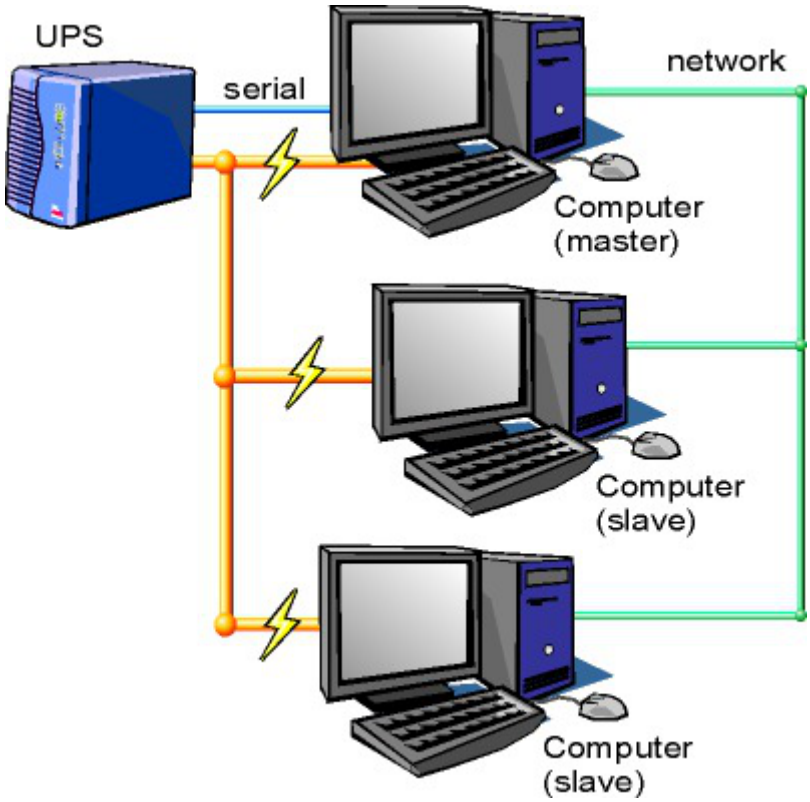


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

http://www.networkupstools.org/

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

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

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

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

ou encore :

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

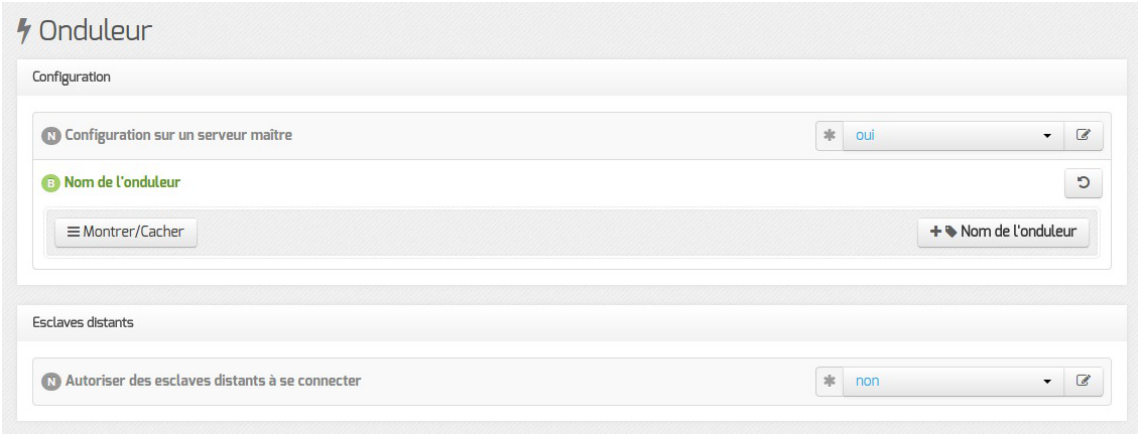
Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

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

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

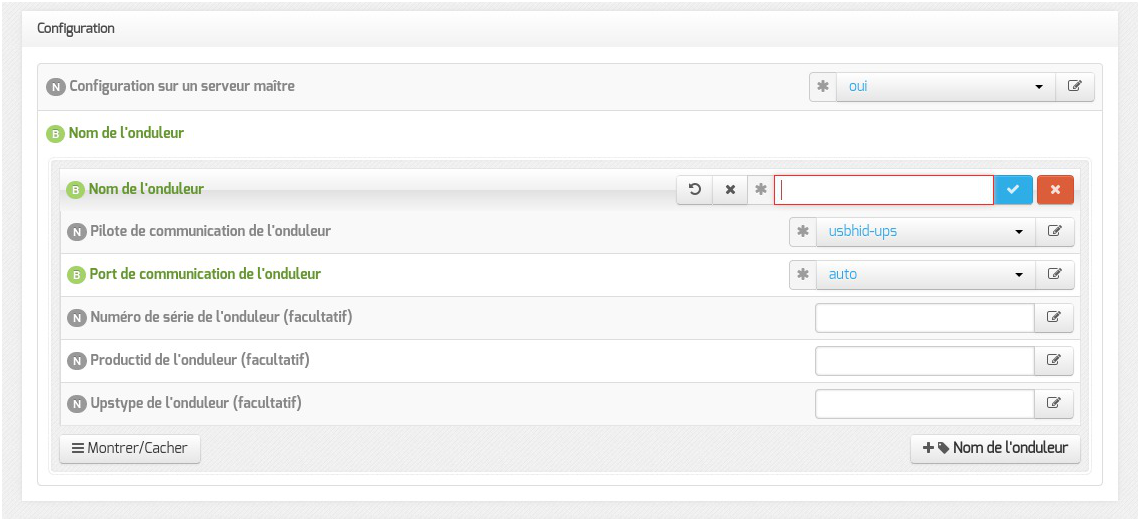
> Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :
>
> http://www.networkupstools.org/source/2.7/new-2.7.3.txt

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



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

La configuration sur un serveur maître



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

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

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

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

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

Configuration d'un second onduleur sur un serveur maître

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

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

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

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

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

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

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

Deux onduleurs de même marque

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

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

Deux onduleurs différents

Un onduleur sur port série :

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

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

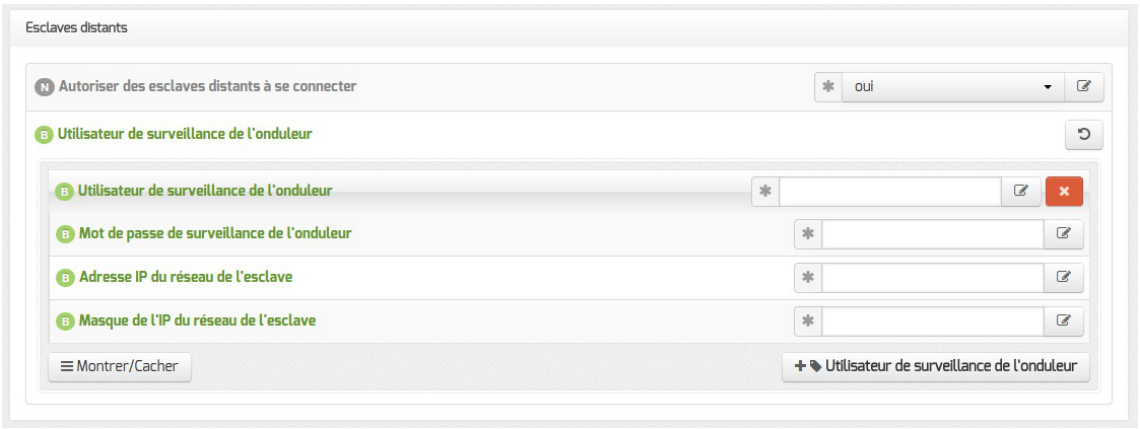
> Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.
>
> Cette adaptation est effectuée automatiquement lors de l'application de la configuration.
>
> Onduleur sur port USB :
>
> - Nom de l'onduleur : `eoleups` ;
> - Pilote de communication de l 'onduleur : `usbhid-ups` ;
> - Port de communication de l'onduleur : `auto`.
>
> La majorité des onduleurs USB sont détectés automatiquement.



Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

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



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

Pour chaque utilisateur, il faut saisir :

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

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

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

Chaque utilisateur doit avoir un nom différent.

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

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

Configurer un serveur esclave

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

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



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

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

Exemple de configuration

Sur le serveur maître :

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

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

- Masque de l'IP du réseau de l'esclave : `255.255.255.255`.

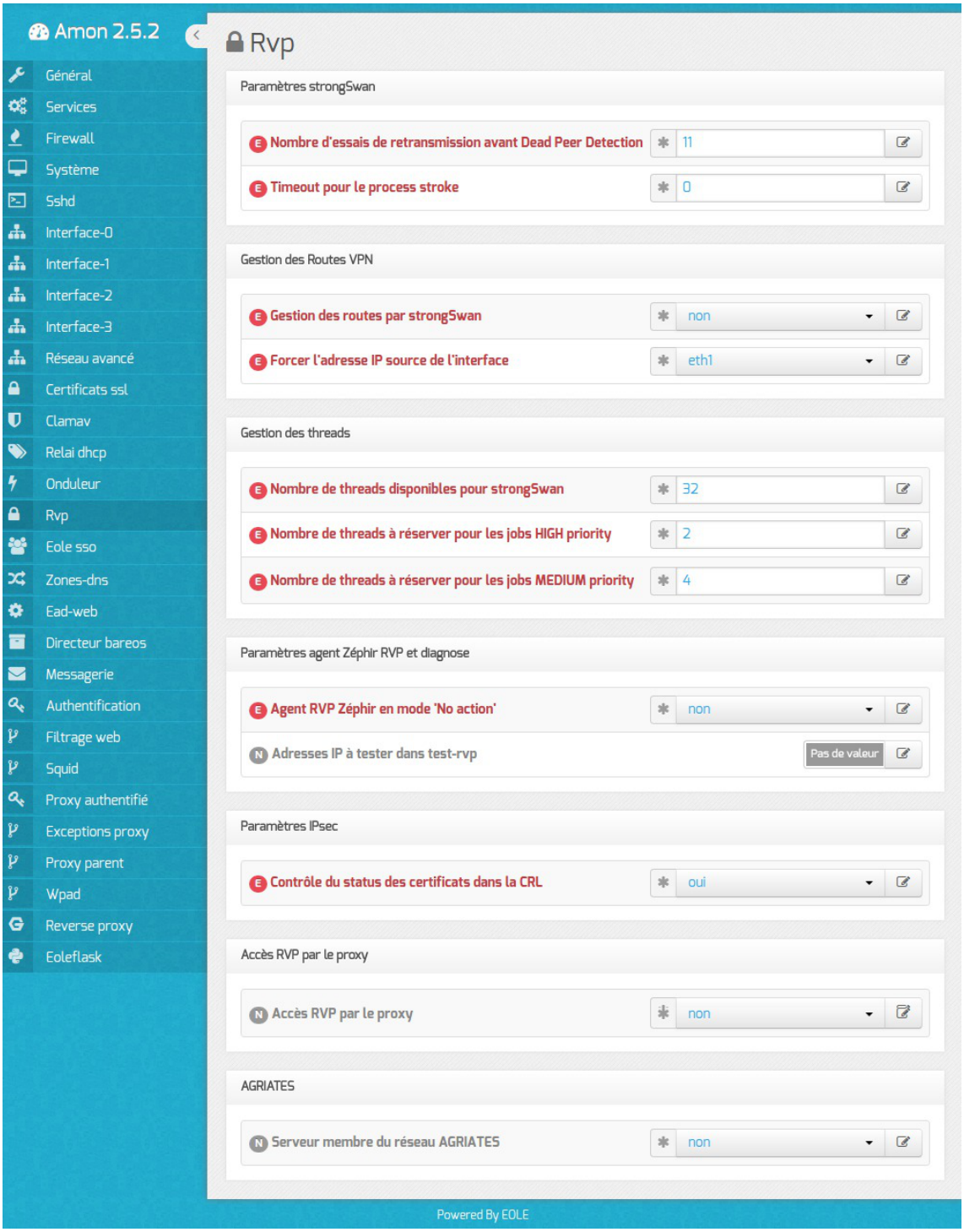


Sur le serveur esclave :

- 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`.

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

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



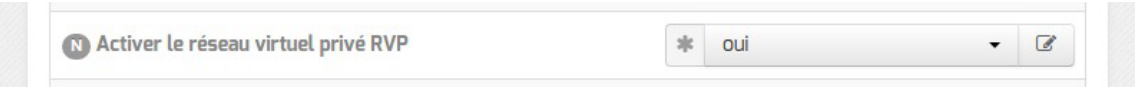
Onglet Rvp mode Expert

Le réseau virtuel privé[p.899] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

L'onglet `Rvp` apparaît après activation du service dans l'onglet `Services`.

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



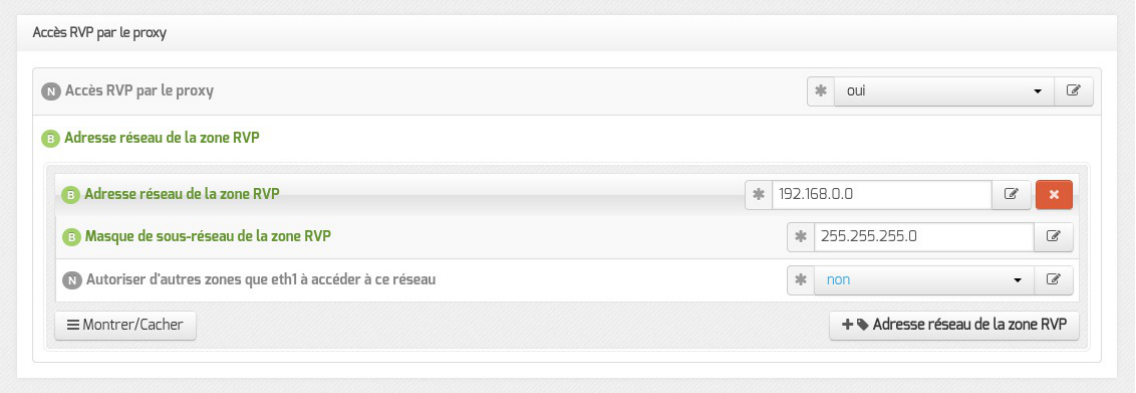
Configuration des tunnels

Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.1 du module Amon. La configuration des tunnels s'effectue d'office en mode fichier plat.

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

Accès RVP par le proxy

Pour paramétrer l'accès RVP par le proxy, il faut passer la variable `Accès RVP par le proxy` à `oui`.

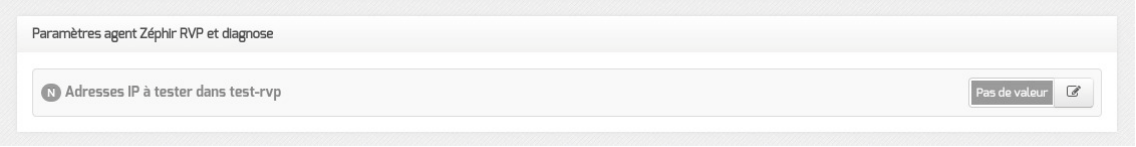


L'adresse réseau de la zone RVP permet la configuration du proxy Squid pour autoriser ou non, aux postes autres que sur l'interface eth1, l'accès via le VPN à un sous réseau.

Pour ajouter d'autres adresses réseau il faut cliquer sur le bouton `+Adresse réseau de la zone RVP`.

Paramètres agent Zéphir RVP et diagnose

Le champ `Adresses IP à tester dans test-rvp` permet de saisir une ou plusieurs adresses IP qui seront utilisées par le diagnose et par l'agent Zéphir pour tester des adresses IP à l'autre extrémité des tunnels.



AGRIATES

Si le serveur est membre d'AGRIATES il faut passer la variable `Serveur membre du réseau AGRIATES` à `oui`.

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



- `Adresse du DNS permettant de résoudre les in.ac-acad.fr` permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;
- `Nom DNS de la zone résolue par le DNS AGRIATES` : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

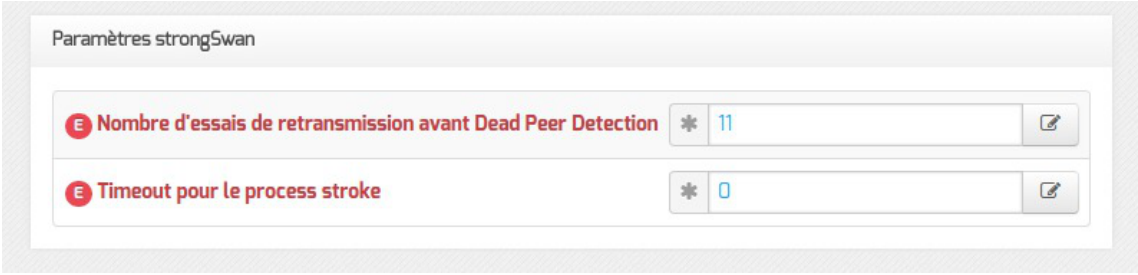
Paramètres propres au mode expert

Le mode Expert permet de personnaliser le fonctionnement de strongSwan.

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

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

Paramètres strongSwan



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

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

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

Gestion des Routes VPN

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



Onglet Rvp mode Expert

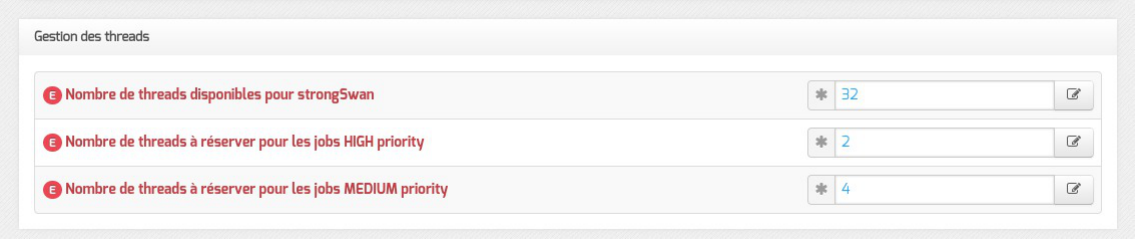
`Gestion des routes par strongSwan` permet si la valeur est passée à `non` de faire gérer la mise en place des routes concernant les tunnels par un script.

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

/etc/ipsec.d/ipsec_updown

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

Gestion des threads



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

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

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

Paramètres agent Zéphir RVP et diagnose



Onglet Rvp mode Expert

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

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

Cette variable est sans effet depuis la version EOLE 2.4.2.

Paramètres IPsec



Onglet Rvp mode Expert

Active ou non la vérification de la validité d'un certificat dans la liste de révocation (CRL[p.887]).

Application de la configuration et gestion du RVP

Activation du RVP au moment de l'instanciation du serveur Amon

Au lancement de l'instanciation, la question suivante vous est posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Deux choix sont alors proposés :

`1.Manuel` permet de prendre en compte la configuration RVP présente sur une clé USB ;

`2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

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

Lors de cette phase de configuration du VPN sur Amon, les tunnels peuvent se couper dans les secondes qui suivent et dans certaines circonstances uniquement. Le problème est corrigé à partir de la version strongSwan 5.5.0 qui n'est pas disponible sur cette version d'EOLE.

Toutefois, le problème est très ponctuel et les tunnels seront relancés automatiquement par l'agent Zéphir assez rapidement.

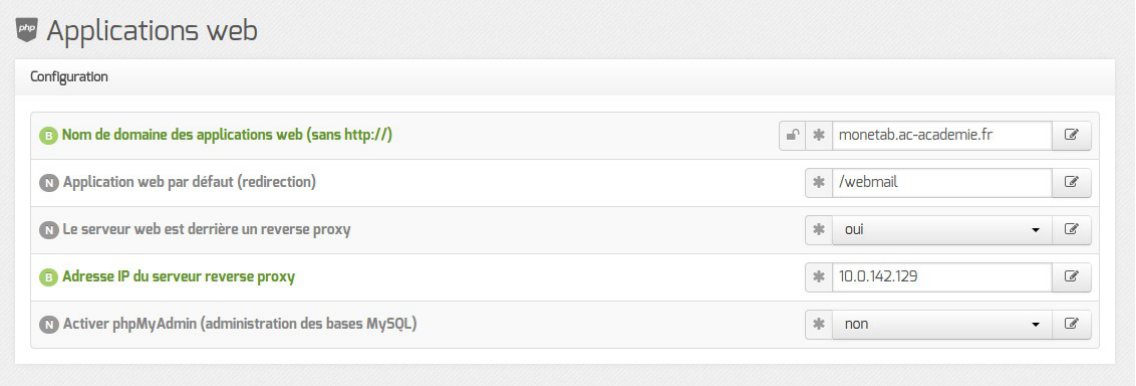
Suppression du RVP

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

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

3.26. 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.

Bien que l'utilisation de l'adresse IP de la carte eth0 soit possible pour une utilisation des applications sur le réseau local du module, il est fortement recommandé d'utiliser un nom de domaine.

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 sur le module Scribe 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`. Déclarer le proxy inverser permet également de mettre en place correctement certaines restrictions sur les applications web

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 par contre une entête qui contient une adresse IP qui peut être falsifiée depuis la machine source.



> Cette fonctionnalité était implémentée via le module Apache additionnel RPAF : https://github.com/gnif/mod_rpaf.

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`.

Activer EOE

Cette variable permet d'activer/désactiver l'application web EOE sur le module.

EOE propose une interface simple contenant un ensemble d'outils à destination des élèves.

Activer EOP

Cette variable permet d'activer/désactiver l'application web EOP sur le module.

EOP propose une interface simple contenant un ensemble d'outils à destination des enseignants.

Activer Roundcube (webmail)

Cette variable permet d'activer/désactiver l'application web Rouncube sur le module.

Roundcube est une application web qui permet à l'utilisateur de gérer ses courriers électroniques au travers d'un navigateur.

Permettre aux utilisateurs d'ajouter des comptes de courrier électronique personnels

`Permettre aux utilisateurs de paramétrer leurs propres mails via serveur pop` permet aux utilisateurs d'ajouter des comptes de courrier électronique autres que ceux géres par l'annuaire du module.

Activer Pydio (gestionnaire de fichiers)

Cette variable permet d'activer/désactiver l'application web Pydio (anciennement Ajaxplorer) sur le module.

Pydio est une application web qui permet à l'utilisateur de gérer ses fichiers au travers d'un navigateur.

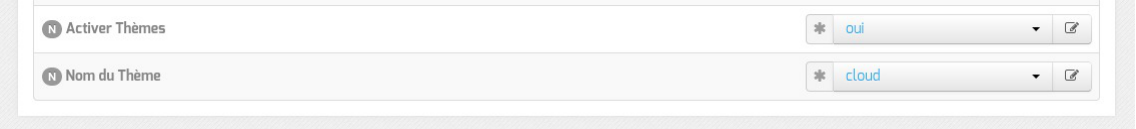


> Toutes les applications web pré-packagées installées manuellement apparaissent dans cet onglet pour éventuellement être désactivées.

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

Envole

L'installation d'Envole[p.888] fait apparaître des variables supplémentaires dans cet onglet et un onglet `Envole`.



La gestion des thèmes pour Envole et les applications web est désactivable. Il est également possible de choisir le thème à utiliser parmi une liste.

Beaucoup d'applications web seront impactées : portail Envole, Dokuwiki, EAD, edispatcher, EoleSSO, Moodle, OpenSondage, WordPress, ...

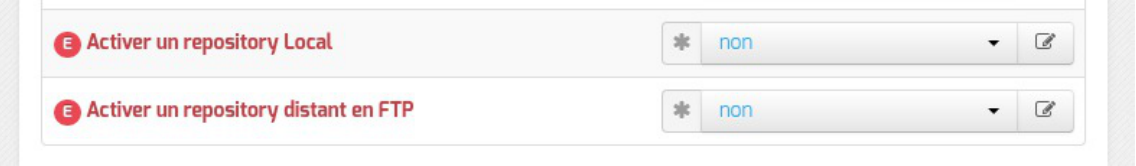
Mode expert

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.

Pydio



Lorsque l'application Pydio est activée, les variables `Activer un repository Local` et `Activer un repository distant en FTP` sont disponibles :

- `Activer un repository local` permet d'activer un espace commun en lecture/écriture sur le serveur à tous les utilisateurs ;
- `Activer un repository distant en FTP` permet de faire un serveur de fichiers avec Pydio qui pointe sur un contrôleur de domaine distant via le protocole FTP.

> Le répertoire utilisé pour le `repository local` est par défaut : `/home/www-data/var/www/html/pydio`.

Voir aussi...

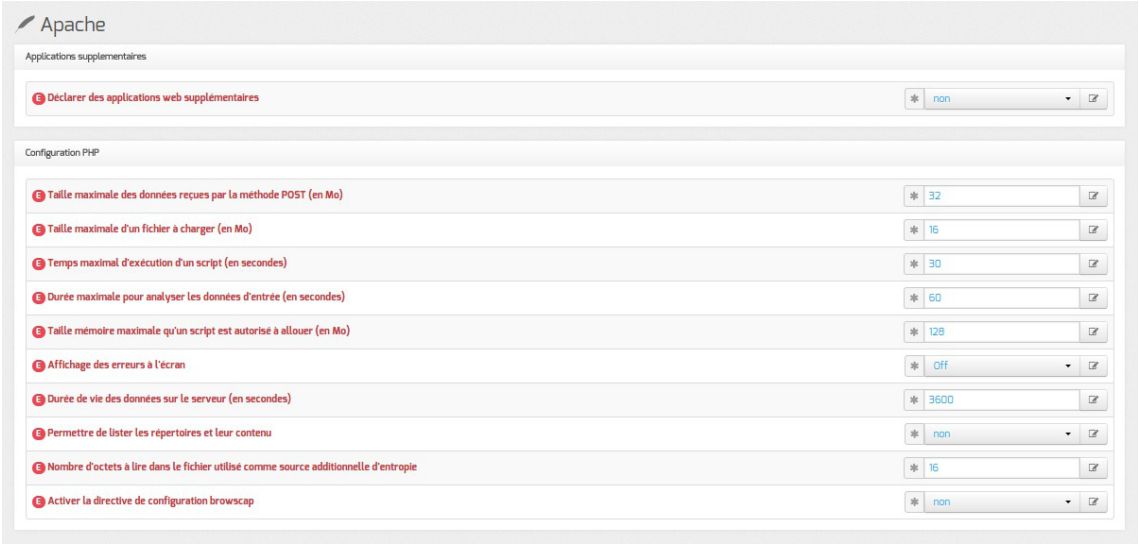
> Les applications web sur le module Scribe

> Espace Numérique Personnel pour l'Éducation avec Envole [p.649]

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

3.27. 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`.

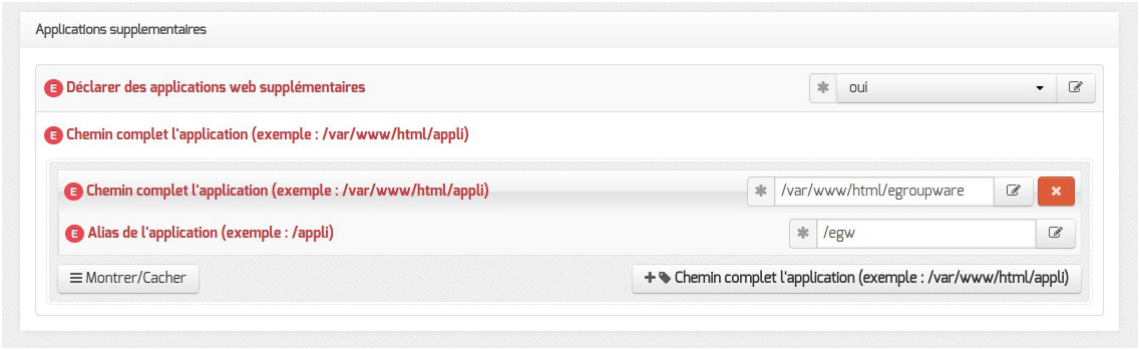


Vue de l'onglet Apache de l'interface de configuration du module

L'onglet expert `Apache` permet de déclarer des applications web supplémentaires et d'affiner la configuration du serveur web.

Applications supplémentaires

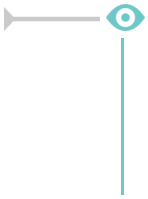
Pour déclarer de nouvelles applications web, il faut tout d'abord passer la variable `Déclarer des applications web supplémentaires` à `oui`.



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)`.



- `Chemin complet l'application (exemple : /var/www/html/appli)` : /var/www/html/egroupware
- `Alias de l'application (exemple : /appli)` : /egw

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

> 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 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. 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

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

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.
- `Permettre de lister les répertoires et leur contenu` : Impacte le fichier `/etc/apache2/sites-available/default` en ajoutant la directive `Options -Indexes`.
- `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`

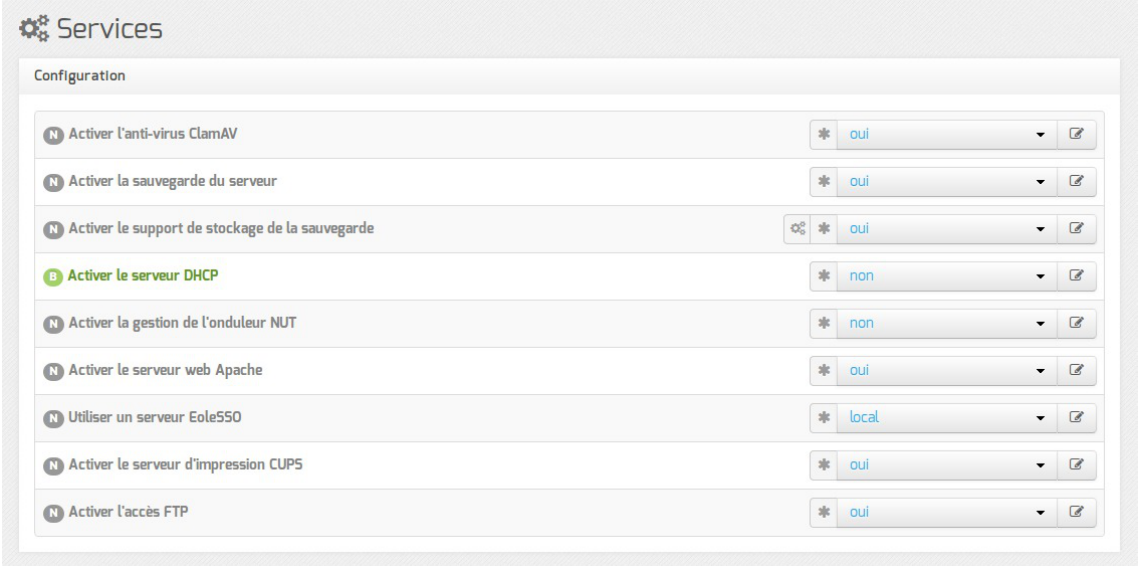
ou consulter la liste des directives du fichier `php.ini` : http://www.php.net/manual/fr/ini.list.php

Voir aussi...

Prise en charge d'applications supplémentaires [p.783]

3.28. Onglet Envole : Espace Numérique Personnel pour l'Éducation

En mode normal la liste des services activables ou désactivables est beaucoup plus conséquente.



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

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

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

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

- l'anti-virus ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le serveurs web ;
- l'authentification unique SSO[p.902] ;
- le serveur d'impression avec CUPS ;
- l'accès FTP.

Voir aussi...

> Espace Numérique Personnel pour l'Éducation avec Envole

> Les applications web sur le module Scribe

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

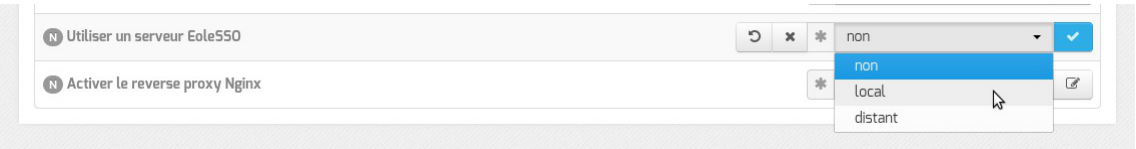
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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

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

Serveur local ou distant

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



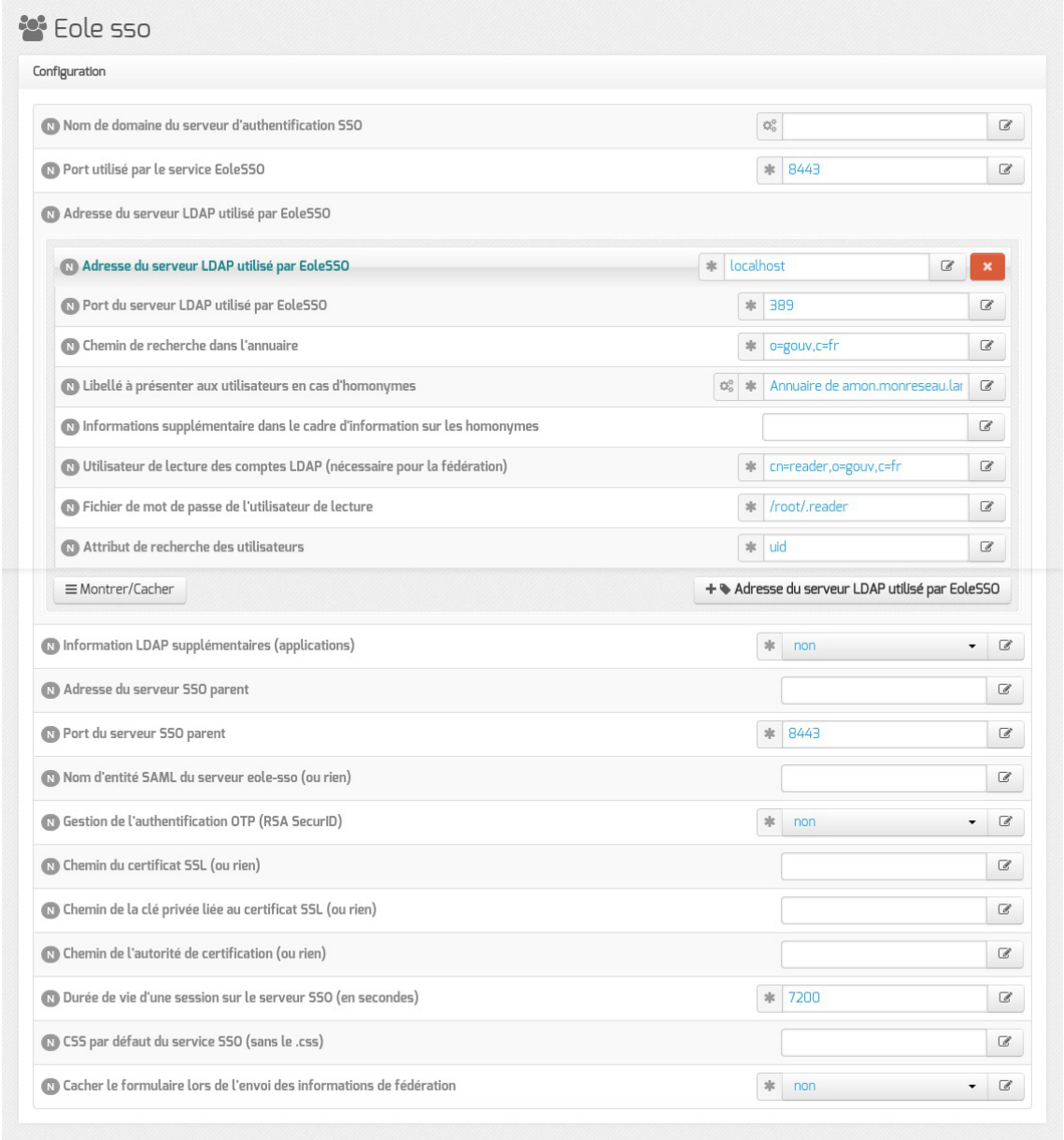
La variable `Utiliser un serveur EoleSSO` permet :

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

Adresse et port d'écoute

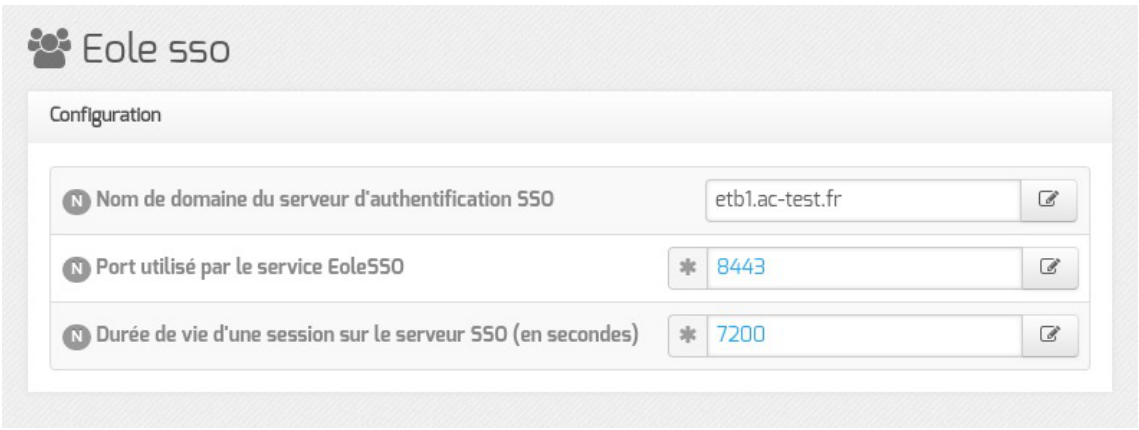
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

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



Configuration d'un serveur EoleSSO local

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



Configuration d'un serveur EoleSSO distant

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.

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

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

Configuration LDAP

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

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.897] si disponible *(voir plus loin)*.



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

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

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

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

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

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

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

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

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

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.906] 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.901] 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

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

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.891] 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.901] (version 2).

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

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

Autres options

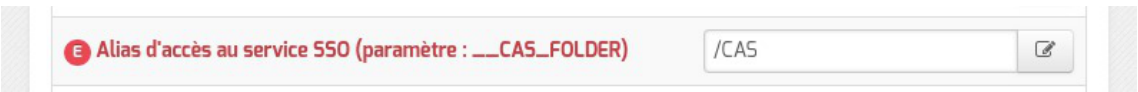
`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra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

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

Configuration en mode expert

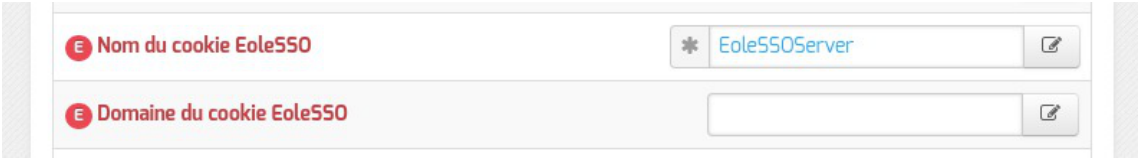
Options générales

En mode expert plusieurs nouvelles variables sont disponibles :

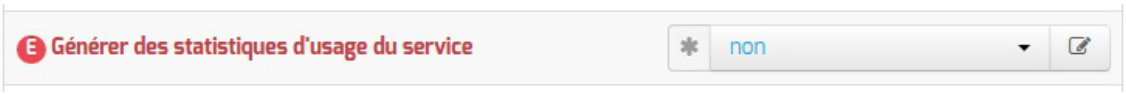


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP ou keycloak.

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



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

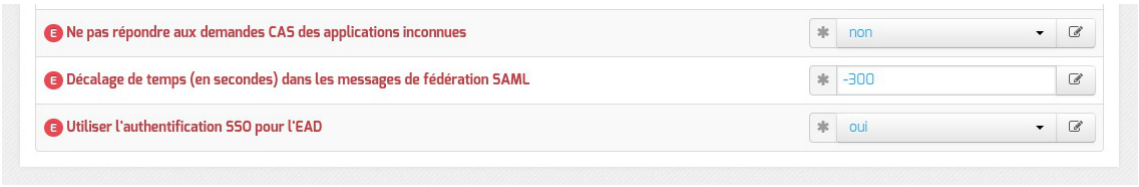


- `Générer des statistiques d'usage du service` est à `non` par défaut.

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



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



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

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

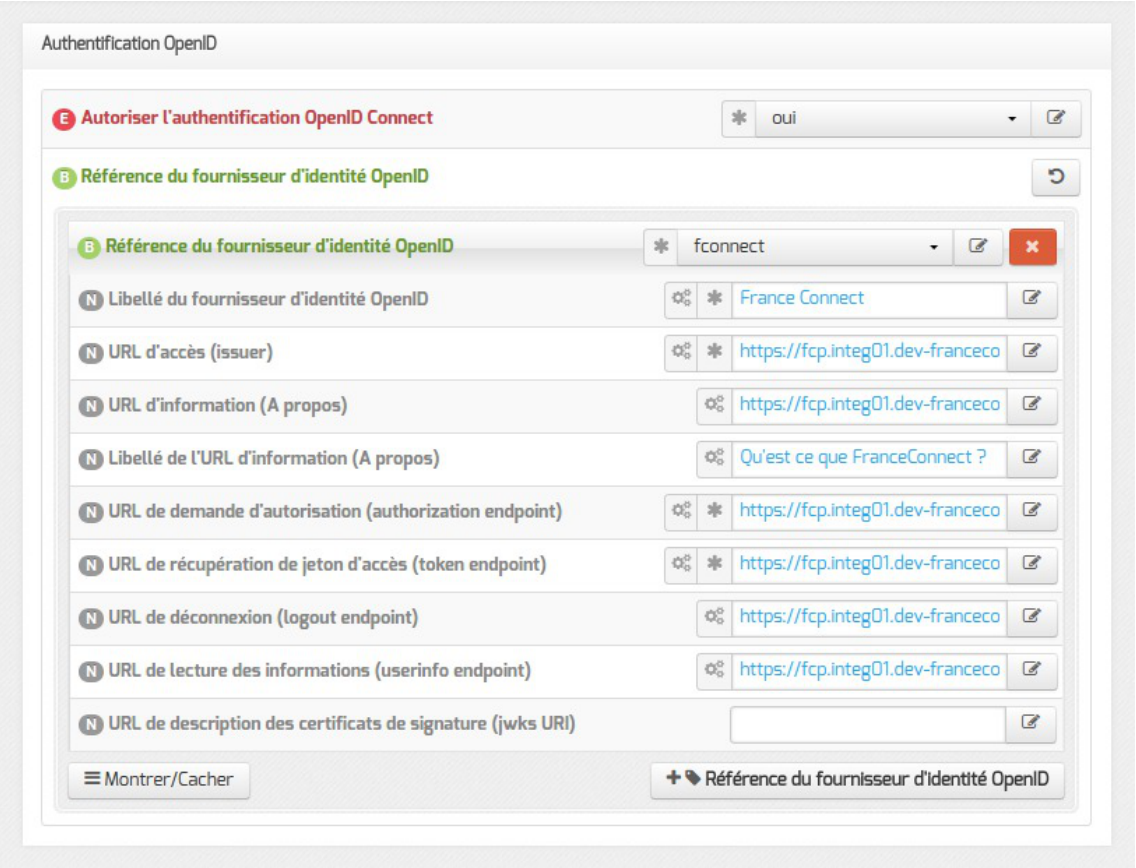
- `Décalage de temps (en secondes) dans les messages de fédération SAML` est à `-300` secondes par défaut

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

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

Configuration d'authentification OpenID Connect

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



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

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

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

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.286]

Compatibilité OpenID Connnect [p.265]

3.30. Onglet Zones-dns : Configuration du DNS

EOLE propose un serveur DNS[p.887] local qui a pour rôles principaux de servir de cache afin d'accélérer les requêtes et de résoudre certains noms de domaines locaux.

Dans le cadre du module Amon, il est en mesure de gérer les différentes zones du réseau établissement.

La génération des différents fichiers de configuration (fichiers de zones) est effectuée par un programme appelé `h2n`.

Il est possible, depuis l'interface de configuration du module, d'activer ou non certaines fonctionnalités et d'ajouter des valeurs au niveau du DNS.

Configuration DNS sur l'interface-0

Sur une installation en mode une carte (exemple : EoleBase + `eole-dns`), le DNS est activable ou désactivable dans l'onglet `Interface-0` avec la variable : `Activer le serveur DNS sur cette zone`.



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

Sur le module Amon et ses variantes (AmonEcole, AmonEcole+), cette question est également présente dans l'onglet `Interface-0`.

Pour chacune des interfaces configurées, il est possible de préciser si le DNS est maître de la zone en passant la variable `Serveur master DNS sur cette zone` à `oui`.



Au moins une des zones doit être configurée en maître de la zone.

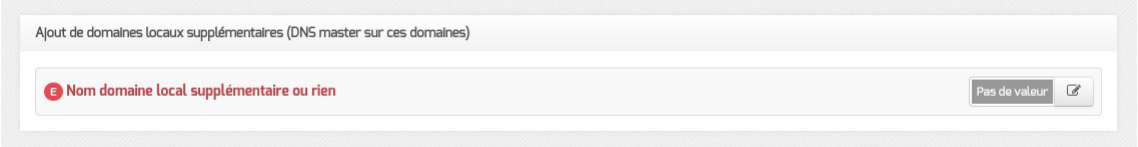
Personnalisation des zones DNS

L'onglet expert `Zones-dns` comporte plusieurs variables directement liées au DNS.

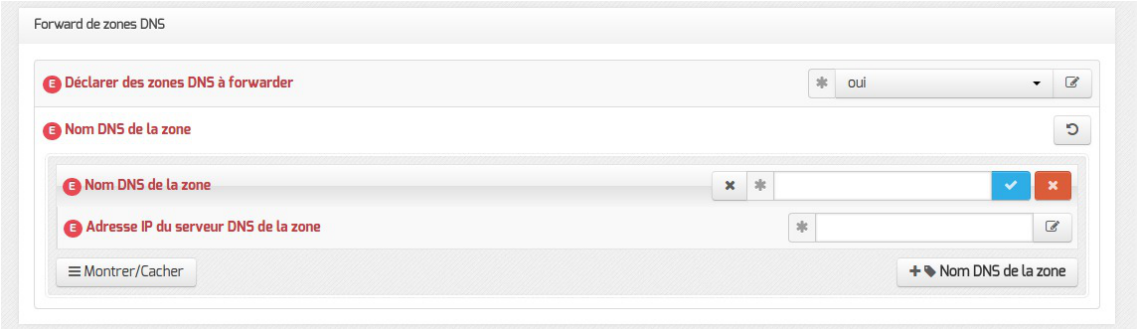


L'onglet Zones-dns

Le champs `Nom de domaine local supplémentaire ou rien` permet au serveur DNS de résoudre les noms de ce domaine.



Si un nom d'hôte avec un suffixe DNS différent du nom de domaine privé du réseau local est déclaré, il est nécessaire de renseigner ce suffixe ici pour que le serveur DNS puisse résoudre ce nom.



Certaines zones nécessitent l'utilisation d'un serveur DNS particulier.

En passant la variable `Déclarer des zones DNS à forwarder` à `oui`, il est possible de saisir le nom d'une zone et l'adresse IP de son DNS de forward dans les champs `Nom DNS de la zone` et `Adresse IP du serveur DNS de la zone`.

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

La déclaration de serveurs locaux (`Ajouts d'hôtes dans le DNS`) ne se fait plus dans l'onglet `Zones-dns` mais dans l'onglet `Réseau avancé` .

DNS et RVP

Si le réseau privé virtuel (RVP[p.899]) est activé et configuré sur le serveur et que le serveur est membre du réseau privé de l'Éducation nationale (AGRIATES[p.882]), il devient possible de déclarer, dans l'onglet `Rvp` , le DNS interne à utiliser pour résoudre les noms de domaines.



L'onglet Rvp

Il est possible de renseigner un ou plusieurs serveurs DNS AGRIATES dans le champs `Adresse du DNS permettant de resoudre les in.ac-acad.fr` . Des relais de zones "AGRIATES" sont prédéfinis et correspondent aux zones *in* du domaine académique. D'autres relais de zone pour le DNS AGRIATES peuvent être ajoutés dans le champs `Nom DNS de la zone resolue par le DNS AGRIATES` .

La configuration des zones DNS AGRIATES est enregistrée dans le fichier templatisé : `/etc/bind/agriates.zones` .

3.31. Onglet Ead-web : EAD et proxy inverse

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



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

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

Voir aussi...

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

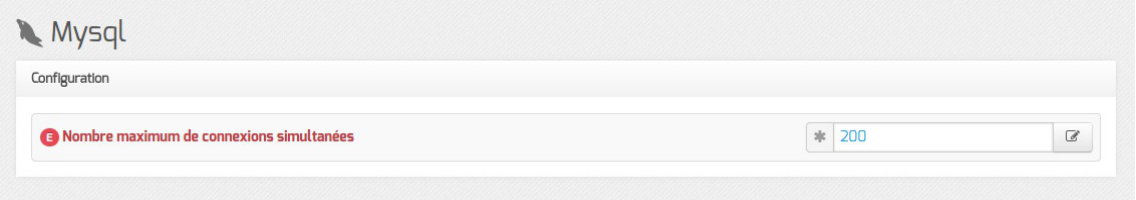
Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur

3.32. Onglet Mysql : Configuration du serveur MySQL

Sur les modules Scribe, AmonEcole 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, qui est pour l'instant le seul disponible, 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 qui engendrerait l'erreur MySQL : `Too many connections`.

Pour plus d'informations, vous pouvez consulter les exemples de configuration fournis dans : /usr/share/doc/mysql-server-5.5/examples/

ou consulter :

http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html

3.33. Onglet Messagerie

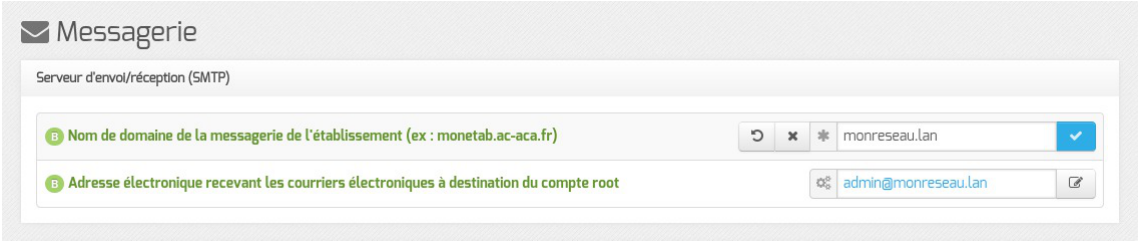
Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

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

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

Configuration basique de la messagerie

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>.*` soient considérés comme des courriers électroniques systèmes.



Tous les noms de conteneur utilisés sur un serveur EOLE peuvent être récupérés grâce à la commande `CreoleGet --groups`. Attention de ne pas oublier de prendre en compte le nom de machine.



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`

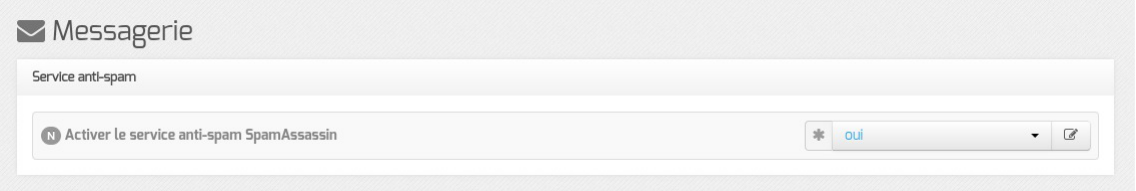
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

En mode normal

En mode normal il est possible de désactiver plusieurs services et d'affiner les réglages de la messagerie.

Anti-spam



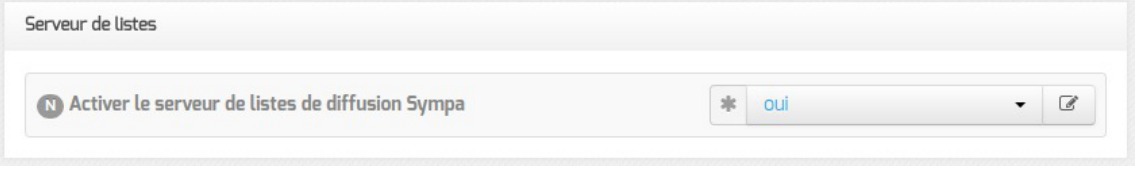
Le service anti-spam peut être désactivé en passant `Activer le service anti-spam SpamAssassin` à `non`.

Service d'échange de courrier



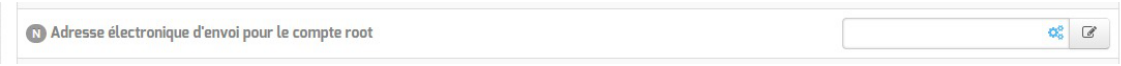
`Activer le serveur de courrier` permet de désactiver le service d'échange de courrier ou de choisir le ou les protocoles supportés : POP, IMAP ou POP -IMAP.

Serveur de listes



`Activer le serveur de listes de diffusion Sympa` permet de désactiver le gestionnaire de publipostage.

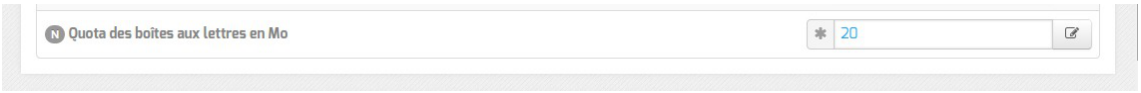
Serveur d'envoi/réception



Il est possible de configurer l'adresse d'expédition des messages du compte `root`.

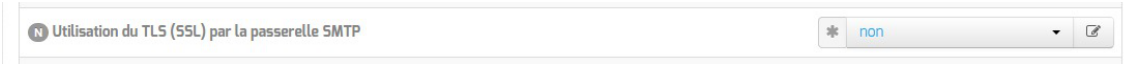
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

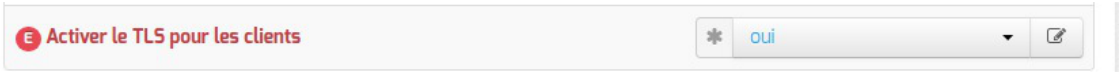


Il est possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

Relai des messages



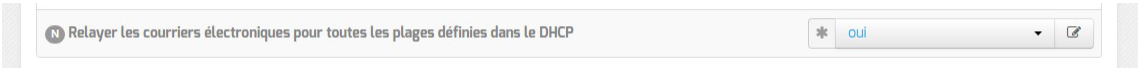
`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS[p.903] pour l'envoi de message. Si la passerelle SMTP[p.901] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS[p.902] (port 25) ou non (port 465).



Le support du TLS[p.903] pour l'envoi de message est activé par défaut. La commande StartTLS[p.902] est supportée sur le port 25 (la connexion est initiée en mode non chiffré) et permet de basculer en TLS sur le port 465.

Le client de courrier qui le supporte (comme par exemple Thunderbird) pourra chiffrer le dialogue avec le serveur SMTP.

Si le client ne supporte pas le chiffrement, le courrier sera envoyé mais sans chiffrement.



Si le service DHCP est activé dans l'onglet `Services`, la variable `Relayer les courriers électroniques pour toutes les plages définies dans le DHCP` apparaît et est à `oui` par défaut.

Dans cette configuration, le relai des courriers électroniques est activé pour les plages d'adresses définies dans la configuration DHCP.

Si toutes les plages d'adresses ne sont pas autorisées à utiliser ce serveur comme relai de messagerie, vous devez passer cette variable à `non` et paramétrer les variables expertes de la même section (`Relayer les courriers électroniques pour des plages d'adresses IPv4` et `Relayer les courriers électroniques pour des nom de domaines`).

> Contrairement à ce qui est marqué dans l'aide, `Activer le relai des messages` est déjà forcé à `oui` et la variable n'apparaît pas dans l'interface de configuration du module.

En mode expert

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

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

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

- `user@%%domaine_messagerie_etab` si l'expéditeur ne précise pas le nom de domaine, par exemple : `root@internet:~# echo "Test" | mail -s "Test mail from shell" -r root root`
- `user@%%nom_machine.%%domaine_messagerie_etab` pour le maître si l'expéditeur utilise la configuration définie dans `/etc/mailname`
- `user@%%conteneur.%%nom_machine.%%domaine_messagerie_etab` pour les conteneurs[p. 886] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

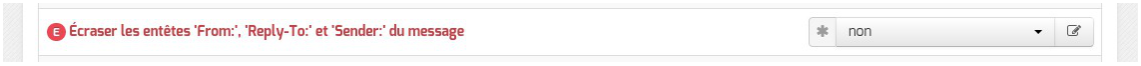
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

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

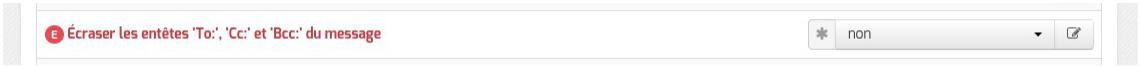
Les adresses destinataires `root@%%nom_domaine_local` et `root@%%domaine_messagerie_etab` sont remplacées par `%%system_mail_to` si cette dernière est définie.

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

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



- `system_mail_to_for_headers` : écraser les entêtes « 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

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

Cc :	user@conteneur.machine.domaine	system_mail_to
Bcc :	user@conteneur.machine.domaine	system_mail_to

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



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



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



Le TLS est activé par défaut pour les clients.



Dans la rubrique Configuration experte plusieurs paramètres peuvent être modifiés :

- `FQDN utilisé par Exim`

  Personnalisation du nom de domaine complètement qualifié utilisé par Exim dans le protocole SMTP. C'est utile pour les vérifications anti-spam des MX externes

  Les valeurs possibles sont :

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

- `Domaine utilisé pour qualifier les adresses`

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

Nom de domaine ajouté aux adresses :

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

- `Envoyer les logs à rsyslog`

  Permet de désactiver l'envoi des logs.

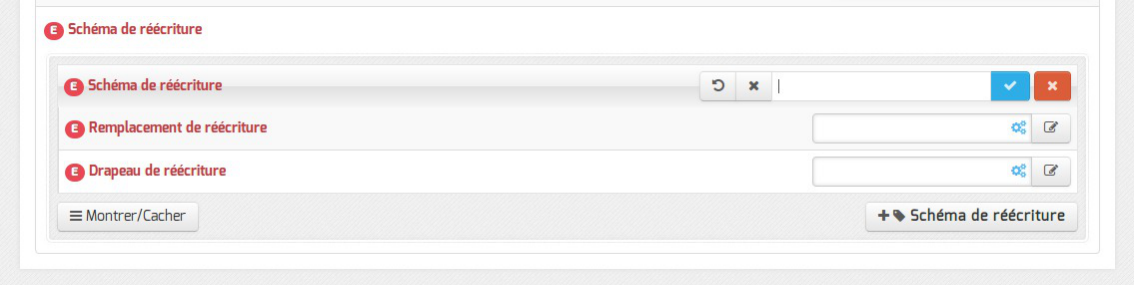
- `Dupliquer les logs dans des fichiers`

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

- `Activer les règles de réécriture étendue`

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

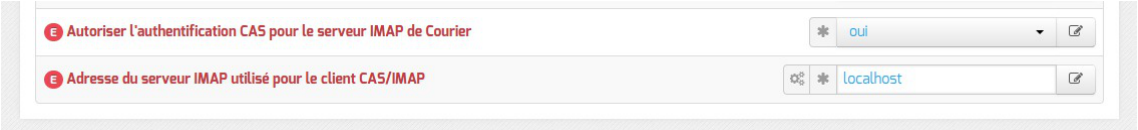
  http://exim.org/exim-html-current/doc/html/spec_html/ch31.html.



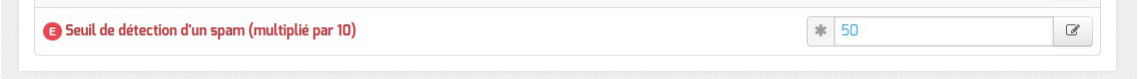
Les trois variables à saisir sont :

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

En ce qui concerne le serveur de récupération de courrier électronique, il est possible de changer l'adresse du serveur IMAP utilisé pour le client CAS/IMAP et de désactiver l'autorisation de l'authentification CAS sur le serveur IMAP de Courier.



Si le service anti-spam est activé, il est possible de modifier le seuil à partir duquel un courrier électronique est considéré en tant que spam. La valeur attendue par SpamAssassin doit être multipliée par 10 dans le champ `Seuil de détection d'un spam (multiplié par 10)` afin de faire des comparaisons sur des entiers.

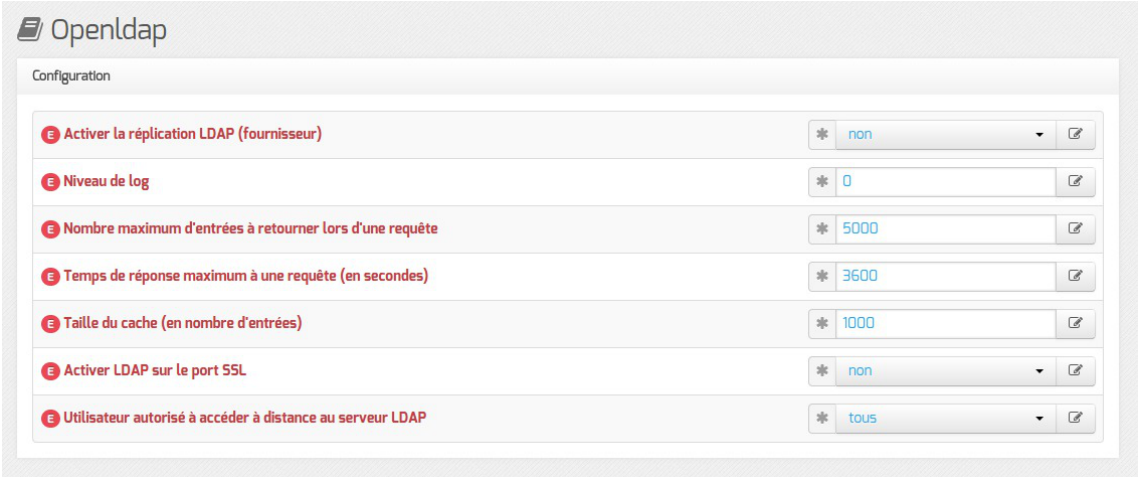


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3.34. Onglet Openldap : Configuration du serveur LDAP local

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

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



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

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

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

Activer la réplication LDAP (fournisseur)

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

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

Niveau de log

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

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

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

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

La valeur par défaut est de `5000` entrées.

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

Temps de réponse maximum à une requête (en secondes)

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

La valeur par défaut est de `3600` secondes.

Taille du cache (en nombre d'entrées)

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

La valeur par défaut est de `1000` entrées.

Activer LDAP sur le port SSL

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



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

Utilisateur autorisé à accéder à distance au serveur LDAP

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

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



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

```
# man slapd.conf
```

ou

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

3.35. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

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

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.



Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Activer une deuxième instance de Squid

Activer une deuxième instance de Squid permet une double authentification, c'est à dire la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Pour profiter de cette fonctionnalité, il faut passer `Activer une deuxième instance de Squid` à `oui`.



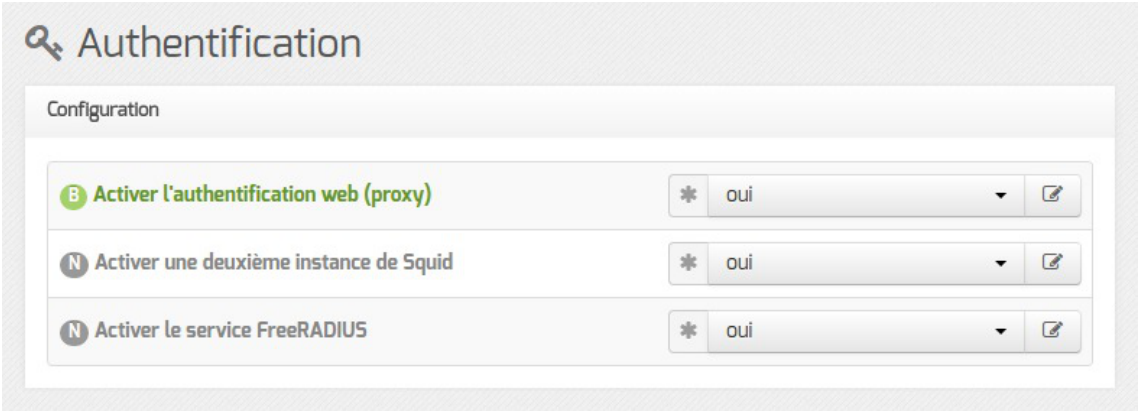
Cela fera apparaître l'onglet `Proxy authentifié 2`.

En mode expert cela fera apparaître également l'onglet `Squid2`.

Activer le service FreeRADIUS

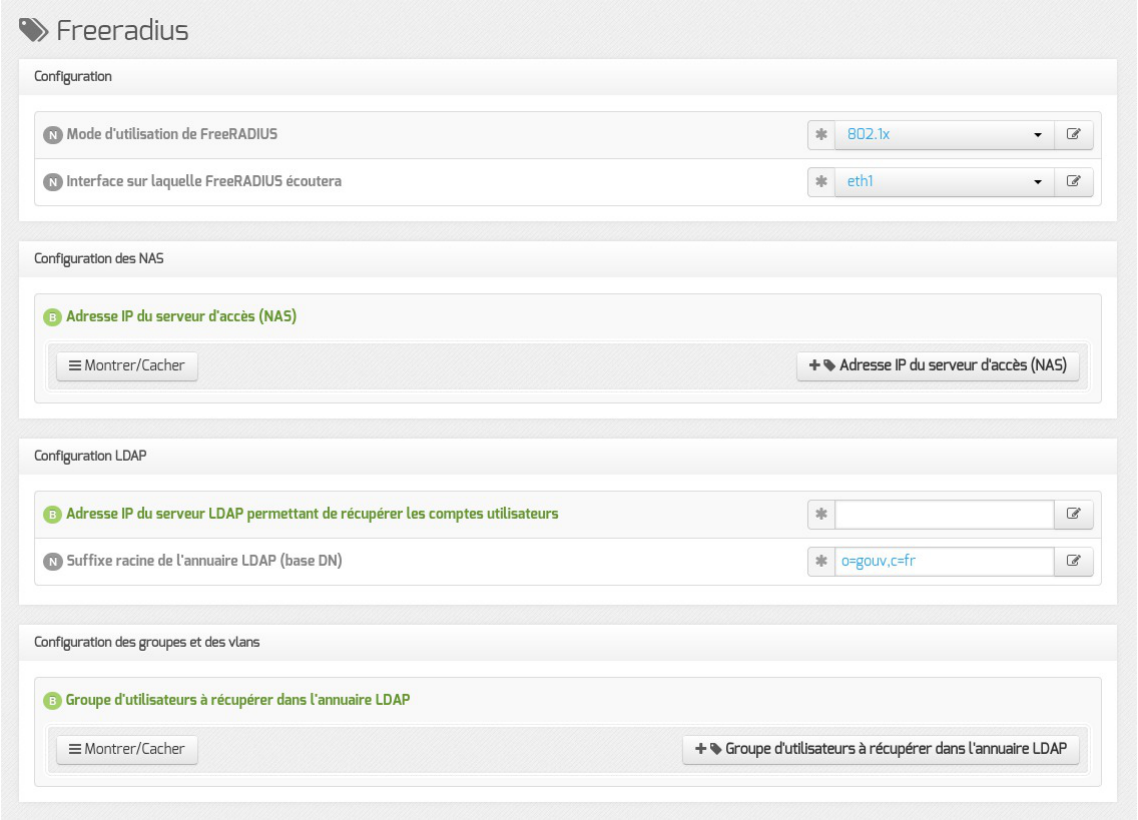
EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.899].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui`.



Cela fera apparaître l'onglet `Freeradius`.

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



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

Voir aussi...

Onglet Proxy authentifié : 5 méthodes d'authentification [p.95]

Onglets Squid2 et Proxy authentifié 2 : Double authentification [p.224]

Onglet Freeradius : Configuration de l'authentification Radius [p.105]

3.36. Onglet Filtrage web : Configuration du filtrage web

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour `Filtre Web à appliquer à cette interface` dans la configuration de l'interface (onglets : `Interface-1`, `Interface-2`, ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage.

Le module Amon intègre le logiciel libre e2guardian[p.888] pour réaliser le filtrage web.

Le paramétrage par défaut de e2guardian convient à un établissement de taille moyenne sans modification particulière.

Il peut être néanmoins intéressant de modifier ce paramétrage pour satisfaire les besoins de l'établissement (notamment dans le cas où le serveur ne peut plus répondre aux requêtes, la fenêtre

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

d'authentification apparaît de façon intempestive, ...).

Sur un petit établissement, il sera possible d'économiser des ressources.

Sur un gros établissement, il pourra répondre à un plus grand nombre de requêtes.

Un certain nombre de paramétrages sont proposés pour contrôler les ressources de e2guardian.

Il est possible d'affecter une politique spécifique aux machines du foyer (politique plus laxiste) et une autre aux machines du CDI (politique moins permissive).

Politiques de filtrage optionnelles

Une politique de filtrage correspond à un ensemble d'autorisations ou interdictions d'accès à des sites, suivant différents critères.

Il existe par défaut 4 politiques obligatoires :

- une politique de filtrage par défaut ;
- une politique « modérateur » (permet d'outrepasser les interdictions) ;
- une politique « interdits » (permet d'interdire toute navigation) ;
- une politique « liste blanche » (navigation limitée aux sites de cette même liste).

Seule la politique de filtrage par défaut est modifiable via l'EAD.

En plus de ces politiques, il est possible d'ajouter de 1 à 4 autres politiques de filtrage optionnelles (il y en a 3 par défaut).

Ces politiques de filtrage optionnelles seront alors paramétrables dans l'EAD.



Pour modifier le nombre de politiques de filtrage par zone, il faut utiliser le paramètre :

`Nombre de politiques optionnelles de filtrage par zone`.

La valeur 0 revient à n'utiliser que les 4 politiques par défaut proposées ci-dessus.

L'ajout de politiques optionnelles (valeur 1,2,3,4) permet d'ajouter des filtres supplémentaires, associables à des groupes de machines ou des comptes utilisateur.

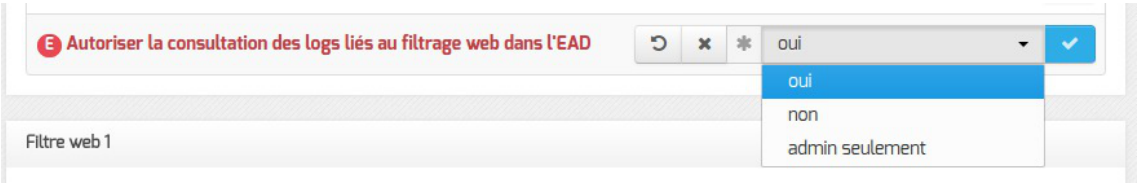
Plus vous définissez de politiques, plus e2guardian utilisera de ressources.

Adaptez le nombre de politiques activées en fonction de vos besoins.

L'observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.888].

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



La question `Autoriser la consultation des logs liés au filtrage web dans l'EAD` propose plusieurs options :

- `oui` : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` ;
- `non` : accès interdit pour tout le monde, personne ne voit le lien `Visites des sites` (configuration par défaut) ;
- `admin seulement` : accès autorisé uniquement pour le rôle `admin`.

La consultation des visites de sites se fait au travers de l'EAD, menu : `Filtre web X/visites des sites`.

Paramétrage de e2guardian

Le logiciel e2guardian offre de nombreuses options de configuration.

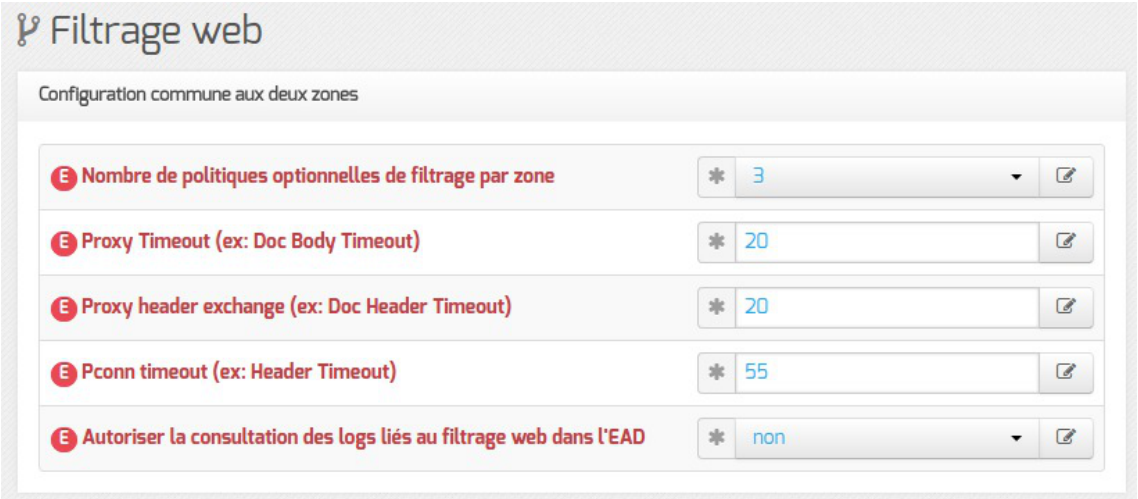
Plusieurs sont paramétrables dans l'interface de configuration du module.

Seule l'expérience «à tâtons»[p.892] permet de définir les valeurs adéquates à votre installation.

L'objectif est d'utiliser le plus de mémoire possible sans que le serveur n'utilise la partition d'échange (swap[p.902]) .

La commande `top` en console permet d'observer l'évolution de l'utilisation de la partition d'échange de façon dynamique.

Les options de configuration proposées dans la première partie de l'interface de configuration sont communes aux deux zones configurables :



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

Proxy Timeout (ex: Doc Body Timeout)

Délai d'attente TCP entre le proxy et e2guardian (en secondes).

Proxy header exchange (ex: Doc Header Timeout)

Délai d'attente entre le proxy et e2guardian (en secondes).

Pconn timeout (ex: Header Timeout)

Délai pendant lequel une connexion persistante attend de nouvelles requêtes (en secondes).

Les options de configuration proposées dans les sections suivantes permettent de personnaliser la configuration de chacune des zones configurables.



Nombre maximum de processus

Nombre maximum de processus disponibles pour traiter les nouvelles connexions (paramètre maxchildren).

Sa valeur par défaut est fixée à 256. Elle peut être modifiée en respectant les contraintes suivantes :

- sa valeur minimum est de 80 ;
- sa valeur maximum théorique est de 8192 mais, dans les faits, elle est proche de 8192 moins deux fois la valeur du paramètre preforkchildren (`Nombre de processus démarré s'il en manque`) qui est de 6 par défaut.



Si la valeur maximum est dépassée, le service refusera de démarrer.

Nombre minimum de processus

Le nombre de processus minimal pour traiter les nouvelles connexions.

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

Nombre minimum de processus en attente

Le nombre minimum de processus prêts à recevoir de nouvelles connexions.

Nombre maximum de processus en attente

Le nombre maximum de processus attendant de nouvelles connexions.

Nombre de processus démarré s'il en manque

Le nombre minimum de processus disponibles lorsqu'ils viennent à manquer.

Durée de vie maximum d'un processus avant de se terminer

Les processus enfant, comme tout processus, peuvent succomber à des variables parasites. Ce paramètre définit l'âge maximal de connexions qu'un processus enfant traite avant de quitter. La valeur par défaut est de traiter 500 demandes de connexion avant de quitter.

Augmenter ce paramètre peut aider à soulager les problèmes de performance liés à la rotation des processus, mais peut créer un problème de performance si un processus s'emballe pour une raison quelconque.

Sur les grands sites vous pourriez vouloir essayer de passer cette valeur à 10000.

Répertoire de cache

Permet de choisir le chemin du répertoire de cache, par défaut `/tmp`.

La taille maximum de fichier conservé en mémoire

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes[p.898] que e2guardian va télécharger et mettre en cache dans la RAM. Après que cette limite soit atteinte, e2guardian met en cache sur le disque.

Cette valeur doit être inférieure ou égale à la valeur de `La taille maximum de fichier conservé sur le disque`.

Utiliser la valeur 0 permet de définir le même réglage que `La taille maximum de fichier conservé sur le disque`.

La taille maximum de fichier conservé sur le disque

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes[p.898] que e2guardian va télécharger de sorte qu'ils soient vérifiés par l'anti-virus.

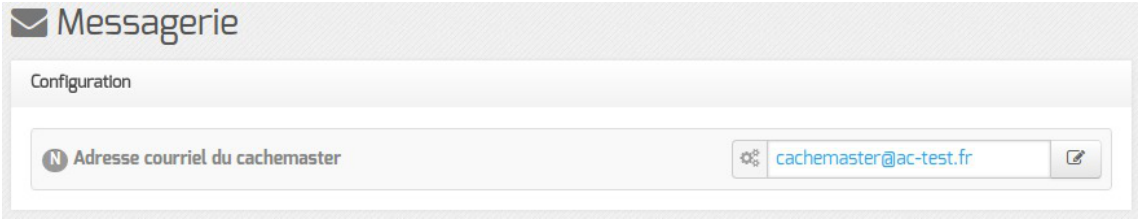
Cette valeur doit être supérieure ou égale à `La taille maximum de fichier conservé en mémoire`.

Adresse électronique à utiliser en cas de réclamation

Lorsque la consultation d'une page est refusée à l'utilisateur, une page d'erreur affichant les détails de l'interdiction apparaît.

Celle-ci propose également une adresse électronique à utiliser pour signaler les interdictions injustifiées.

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



Cette adresse se configure par l'intermédiaire de la variable `Adresse courriel du cachemaster` disponible dans l'onglet `Messagerie`.

Désactivation du filtrage web

Dans certaines configurations (utilisation d'un proxy académique, ...), il peut s'avérer utile de désactiver complétement le filtrage web.



Cela est possible en allant dans l'interface de configuration du module en mode expert et en répondant `non` à la question de l'onglet `Services`, `Activer le filtrage sur le proxy`.



Dans cette configuration, le proxy Squid écoute sur le **port 3128** en lieu et place du logiciel de filtrage e2guardian.

Voir aussi...

Observatoire des navigations [p.417]

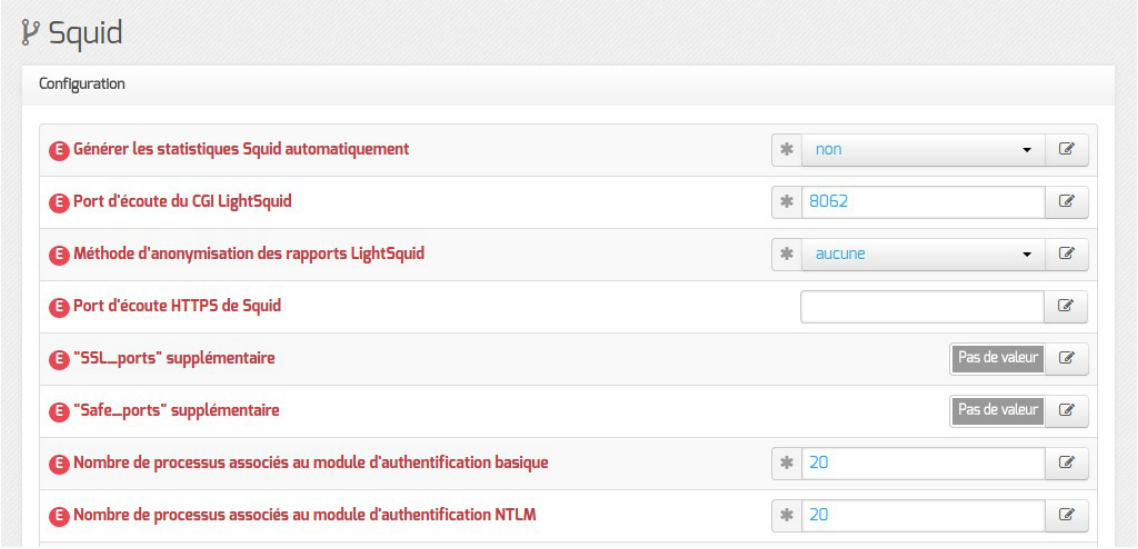
3.37. Onglet Squid : Configuration du proxy

Le service proxy Squid n'étant pas désactivable, l'onglet `Squid` est toujours accessible en mode expert.

L'onglet expert `Squid` permet de modifier et de fixer une sélection des principaux paramètres du fichier de configuration : `/etc/squid3/squid.conf`.

Les paramètres de ce fichier de configuration se retrouvent explicitement dans le nom des variables Creole (mode Debug de l'interface de configuration du module).

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



Paramétrer l'analyse de logs LightSquid

Les options `Générer les statistiques Squid automatiquement`, `Port d'écoute du CGI LightSquid` et `Méthode d'anonymisation des rapports LightSquid` servent à configurer l'outil d'analyse de logs LightSquid permettant d'afficher sous forme de pages web l'utilisation du proxy. Sa configuration fait l'objet d'une section dédiée.

Paramétrer les ports de Squid

Ports d'écoute

Si le filtrage web est activé, le service Squid écoute sur le port `8080` de la boucle locale.

Si le filtrage web est désactivé, le service Squid écoute sur le port par défaut de e2guardian : `3128`.

Il est possible de paramétrer Squid pour qu'il écoute les requêtes HTTPS des clients.

Ceci est particulièrement utile dans les situations où Squid est utilisé comme accélérateur des requêtes. Il faut alors saisir le numéro de port choisi dans le champ `Port d'écoute HTTPS de Squid`.

SSL_ports

Par défaut, seuls les ports de destination (sortants) des connexions SSL 443, 563, 631, 4000-5000, 6080, 8062, 8070, 8090, 8443, 8753 et 7070 sont autorisés.

Il est possible d'en ajouter autant que souhaité dans le champ `"SSL ports" supplémentaire`.

Safe_ports

De même, seuls les ports de destination (sortants) non SSL 80, 21, 443, 563, 70, 210, 631 et 1025-65535 sont autorisés.

Il est possible d'en ajouter autant que souhaité dans le champ `"Safe ports" supplémentaire`.

Personnaliser la durée des caches

L'option `Personnaliser sélectivement la durée des caches`, présente à partir de la version 2.5.2 d'EOLE, permet de personnaliser l'algorithme de gestion du rafraîchissement du cache par

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

site.

La gestion du cache de Squid peut ne pas correspondre à tous les sites. Par exemple, pour les sites antiviraux, il vaut mieux augmenter la durée de conservation du cache des fichiers téléchargés par les postes clients.

Voici un exemple la configuration à mettre en place pour conserver en cache les signatures de l'anti-virus Trend :



L'expression rationnelle décrit la chaîne de caractères et les règles qui permettent de construire l'URL :

- **^** marque le début d'une chaîne ;
- **$** marque la fin d'une chaîne ;
- | marque l'alternative ;
- **.** indique n'importe quel caractère ;
- * aucune, une ou plusieurs occurrences du caractère.

Les variables qui permettent de régler le comportement du cache de Squid sont :

- `Temps maximum de cache` ;
- `Rapport entre l'âge de l'objet dans le cache et son âge sur le site` ;
- `Temps minimum de cache`.

Cette configuration générera la ligne de configuration suivante :

- `refresh pattern -i <url regexp> "Temps maximum de cache" "Rapport entre l'âge de l'objet dans le cache et son âge sur le site" "Temps minimum de cache" <options>`
- `refresh pattern -i /.*\.trendmicro\.com/.* 180 100% 300 reload-into-ims ignore-reload`

L'option **-i** permet de ne pas tenir compte de la casse des caractères dans l'expression régulière.

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



La personnalisation sélective de la durée du cache est basée sur la directive `refresh pattern` de Squid. Cette directive permet un contrôle très fin de la validité des objets mis en cache.

Lors d'une requête, Squid décide du comportement à adopter en fonction de l'état de l'objet dans son cache :

- si l'objet n'est pas dans le cache, Squid le demande au serveur qui héberge l'objet, le met en cache et le fournit au client ;
- si l'objet est dans le cache et qu'il est considéré comme étant encore à jour, Squid le fournit directement au client ;
- s'il n'est plus considéré comme à jour, alors une requête `If-modified-since` est envoyée au serveur qui héberge l'objet.

Pour déterminer si un objet est à jour, Squid utilise plusieurs paramètres :

- la valeur liée à l'objet enregistré :
  - **age** correspond au temps en seconde écoulé depuis l'entrée de l'objet dans le cache (objet_age = maintenant - objet_date)
  - **lm_age** correspond à l'age de l'objet au moment de l'entrée dans le cache, temps, en secondes, écoulé entre la dernière modification de l'objet sur le serveur hébergeur et son entrée dans le cache. (lm_age = objet_date - objet_lastmod)
  - **expires** est la date d'expiration de l'objet éventuellement fournie par le serveur hébergeur au moment de l'entrée de l'objet dans le cache. Si elle est renseignée, la valeur de `Temps minimum de cache` prend le pas sur cette valeur.
- la valeur fournie par le client ;

  Squid tient compte de la variable **client_max_age** éventuellement fournie par le client, elle indique l'âge maximal de l'objet accepté par le client. Si cette valeur est fournie par le client elle prend le pas sur la valeur `Temps maximum de cache` du fichier de configuration de Squid.
- les valeurs du fichier de configuration de Squid :
  - temps écoulé depuis le téléchargement (**age**), temps maximum et minimum de cache :
    - si `Temps maximum de cache` est défini et que le temps écoulé depuis le téléchargement est supérieur, l'objet est périmé et devra être mis à jour ;
    - si le temps écoulé depuis le téléchargement est inférieur ou égal au `Temps minimum de cache`, l'objet est considéré comme étant à jour.
  - date d'expiration de l'objet fournie par le serveur hébergeur :
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur et qu'elle est dépassée, l'objet est périmé et devra être mis à jour ;
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur mais qu'elle n'est pas encore dépassée, l'objet est considéré comme étant à jour.
  - rapport (**lm_factor**) entre le temps, en secondes, écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache :

    Plus le score du rapport entre le temps écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache (**age**/**lm_age**) est élevé plus l'objet risque

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

d'être périmé :

- peu de temps écoulé (10) / objet vieux (1000) = rapport faible (0.01) → objet probablement à jour
- beaucoup de temps écoulé (1000) / objet vieux (1000) = rapport élevé (1) → objet probablement périmé
- peu de temps écoulé (10) / objet jeune (10) = rapport élevé (1) → objet probablement périmé
- beaucoup de temps écoulé (1000) / objet jeune (10) = ce cas de figure n'arrive pas car géré par des règles en amont.

Si le rapport est inférieur au pourcentage (**percent**) saisi dans `Rapport entre l'âge de l'objet dans le cache et son âge sur le site`, l'objet est considéré comme à jour. Diminuer la valeur du pourcentage diminue la probabilité (rapport faible) qu'un objet soit périmé.

Enfin, si aucune règle n'aboutit à considérer l'objet comme étant à jour, celui-ci est considéré comme périmé et devra être mis à jour.

Augmenter le nombre de redirections

Certains sites ont besoin de faire un grand nombres de redirections avant de fournir le contenu souhaité à l'utilisateur.

Par défaut, Squid n'accepte que 10 redirections (variable `forward max tries` du fichier de configuration de Squid) ce qui peut entraîner l'abandon des redirections et donc bloquer l'accès au site.

Il est possible à partir de la version 2.5.2 d'EOLE d'augmenter cette valeur en modifiant la variable `Nombre maximum de redirections testées` de l'onglet.

Paramètre Half_closed_clients

Certains clients peuvent arrêter leur connexion TCP d'envoi tout en laissant leur connexion de réception ouverte. Parfois,Squid ne peut pas faire la différence entre une connexion à demi-fermée et une connexion entièrement fermée :

- si le paramètre `Half_closed_clients` est à `On`, les connexions demi-fermée sont maintenues ouvertes jusqu'à ce qu'une erreur de lecture ou d'écriture apparaisse ;
- si le paramètre `Half_closed_clients` est à `Off`, les connexions sont fermées dès qu'il n'y a plus de données à lire (valeur recommandée sur Squid >= 3.0).

Historiquement paramétrée à `On` sur les modules EOLE, sa valeur par défaut a été passée à `Off` sur les versions d'EOLE >= 2.5.1 depuis avril 2016.

Autres paramètres

L'onglet expert Squid permet de modifier et de fixer un nombre conséquent de paramètres optionnels du fichier de configuration : `/etc/squid3/squid.conf`.

Pour plus d'informations sur la modification de ces paramètres, vous pouvez consulter :

- les exemples de configuration dans le fichier de documentation de Squid :

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

`/usr/share/doc/squid3-common/squid.conf.documented.gz`

- la documentation en ligne des différents paramètres : http://www.squid-cache.org/Doc/config/

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.209]

Outil d'analyse de logs LightSquid [p.418]

3.38. Onglet Proxy authentifié : 5 méthodes d'authentification

EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

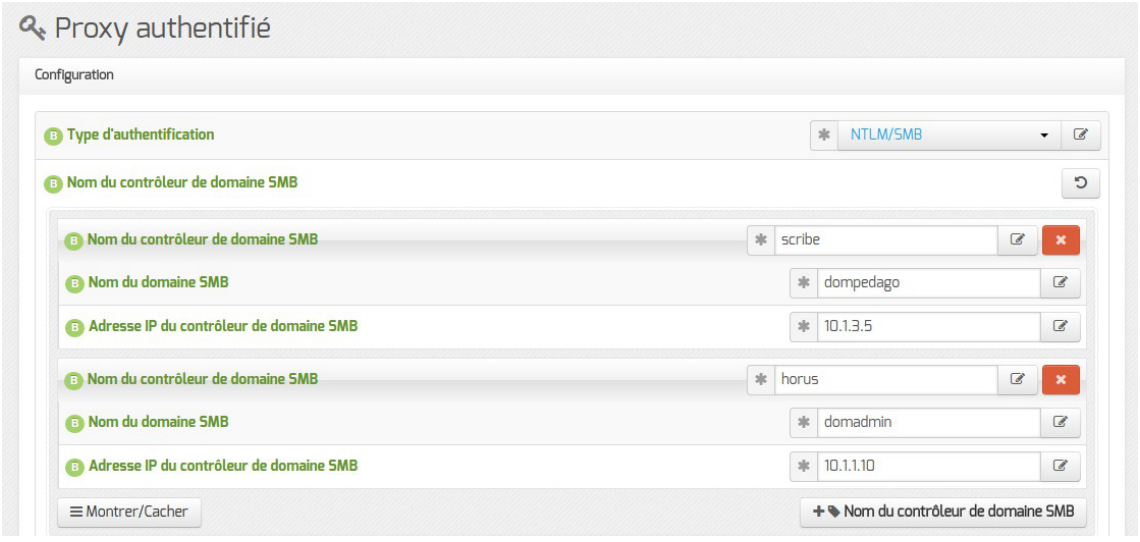
Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet `Authentification` : `Activer l'authentification web (proxy)`.



Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.



Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

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

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

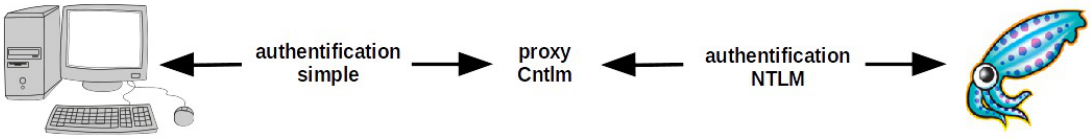
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : http://technet.microsoft.com/en-us/library/cc960646

Authentification NTLM/SMB poste hors domaine

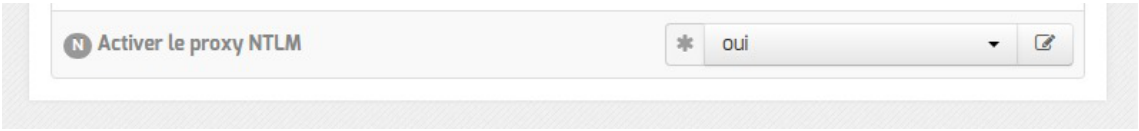
En mode normal, l'authentification NTLM[p.895] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.886].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

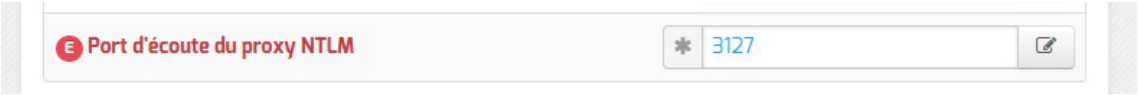
Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

C'est le premier domaine spécifié qui sera utilisé par Cntlm.

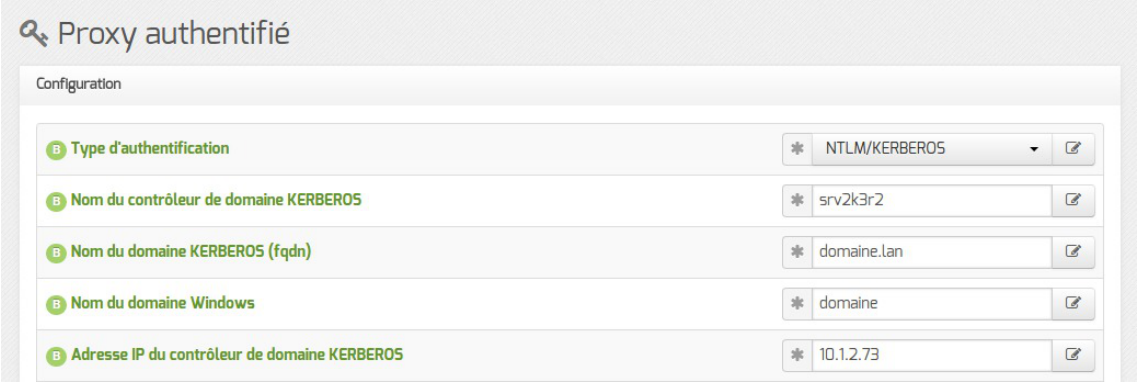
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.



Une fois activé, le choix peut être fait de désactiver le proxy NTLM sur une interface donnée, pour cela il faut se rendre en mode expert dans l'onglet de l'interface à paramétrer.

Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

L'intégration peut être réalisée lors de l'instanciation du module en répondant `oui` à la question suivante :

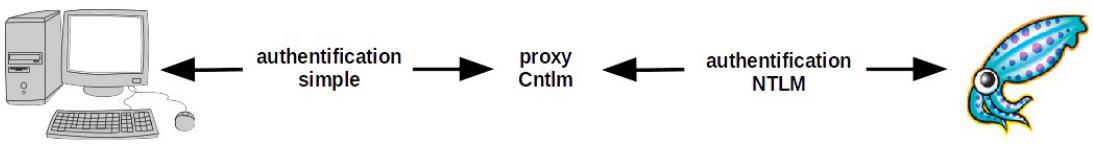
```
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?
```

Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification NTLM/KERBEROS poste hors domaine

En mode normal, l'authentification NTLM[p.895] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm[p.886].

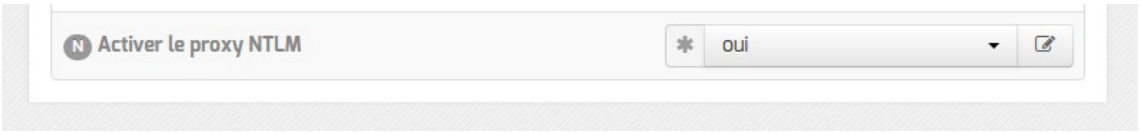
Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

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

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



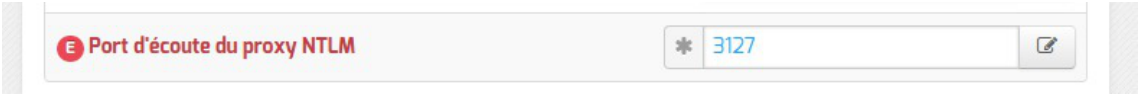
Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

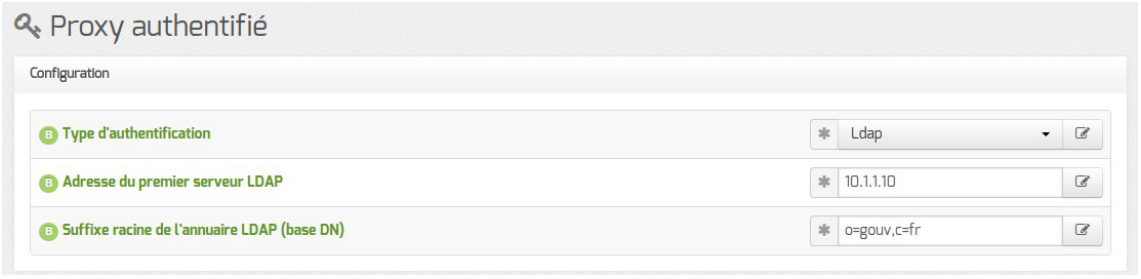
En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.



Une fois activé, le choix peut être fait de désactiver le proxy NTLM sur une interface donnée, pour cela il faut se rendre en mode expert dans l'onglet de l'interface à paramétrer.

Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.



Ce type d'authentification est recommandé pour les postes hors domaine.

En mode normal, il est possible de déclarer un annuaire de secours.

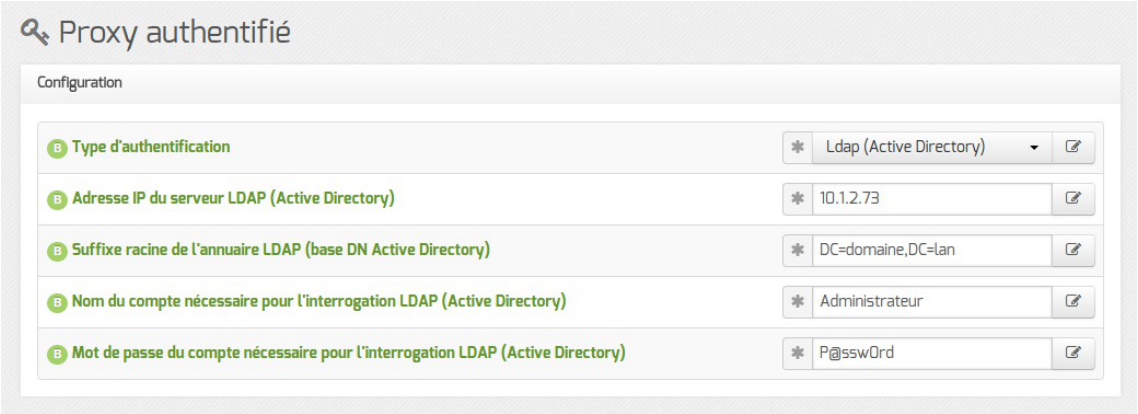


Cet annuaire est interrogé uniquement si le premier ne répond pas.

Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

Authentification LDAP (Active Directory)

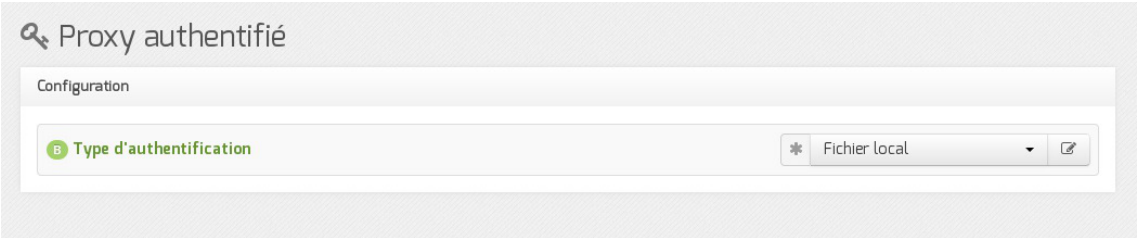
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory.

Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local



Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux.

Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format *htpasswd* et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```



En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors eth0 si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette`

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

`interface (s'applique aussi aux VLAN)`.

3.39. Onglets Squid2 et Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

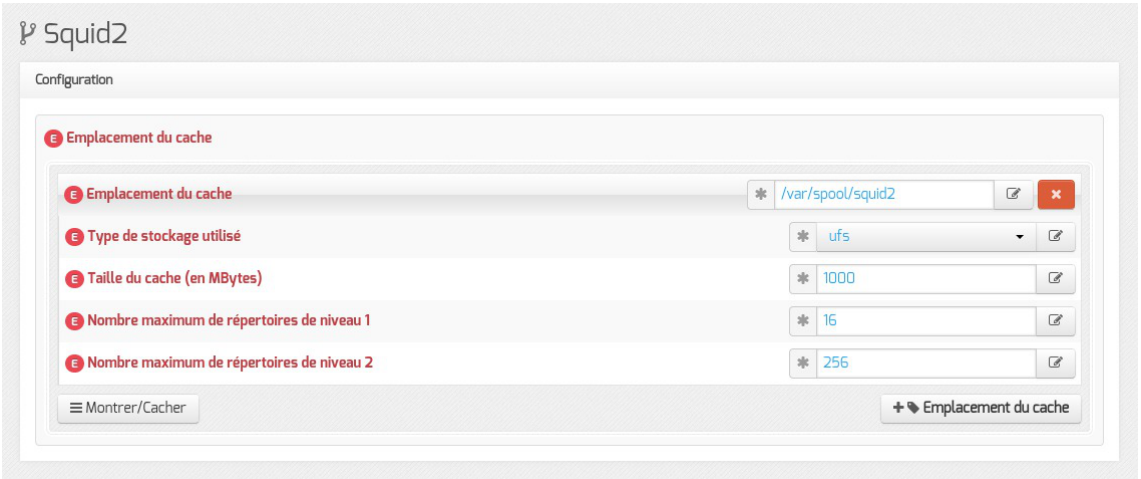
1. Activation de la deuxième instance de Squid dans l'onglet `Authentification` :



2. Configuration du type d'authentification dans l'onglet `Proxy authentifié 2` :

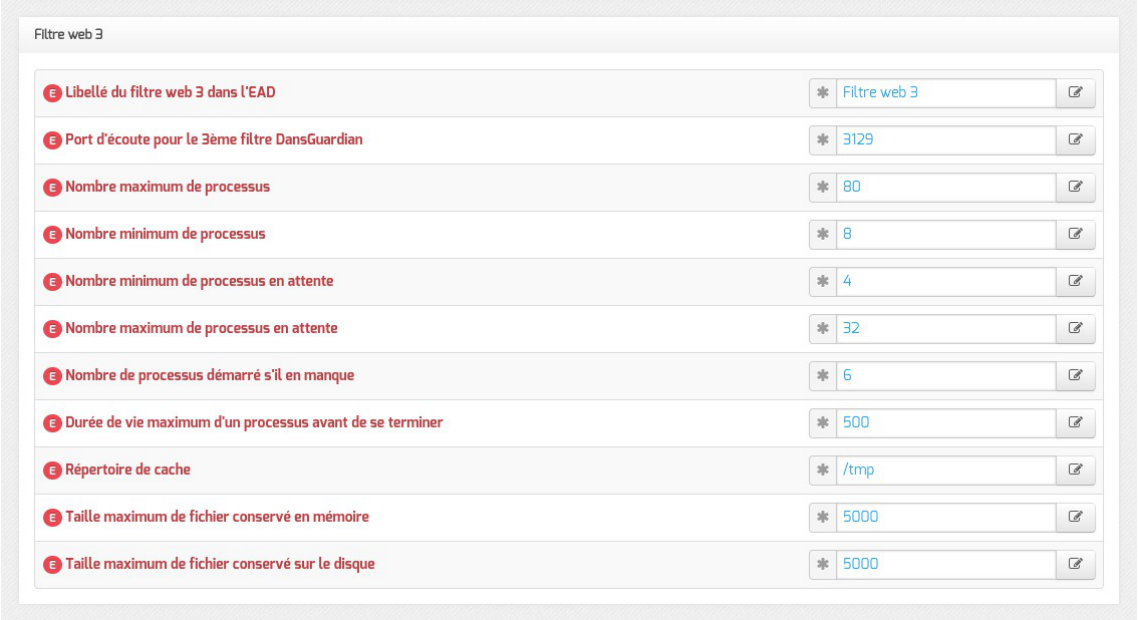


3. Paramétrage de la seconde instance de Squid dans l'onglet expert `Squid2` :



4. Paramétrage du filtrage web associé dans l'onglet expert `Filtrage web` (section `Filtre web 3`)

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



Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log`

Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

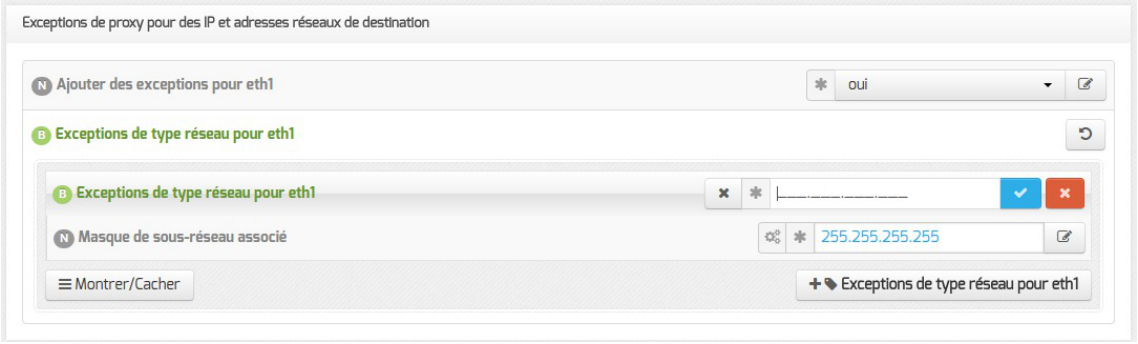
3.40. Onglet Exceptions proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

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

Exception sur un nom de domaine

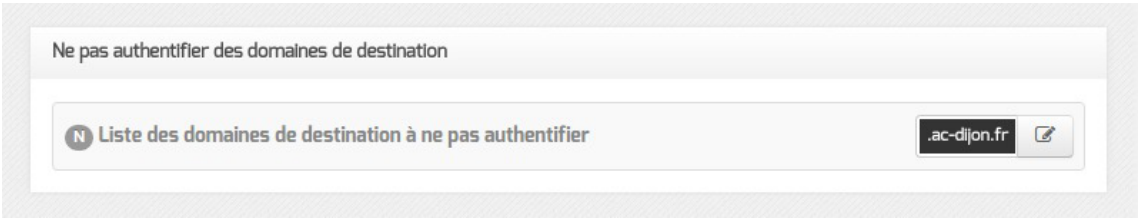
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



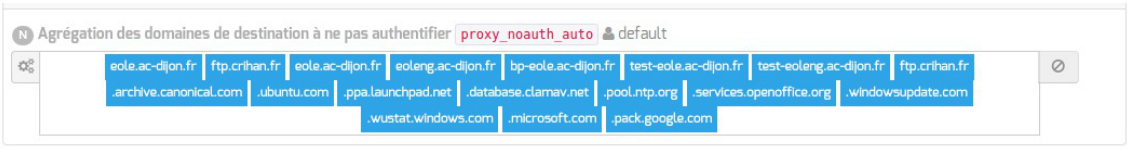
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.

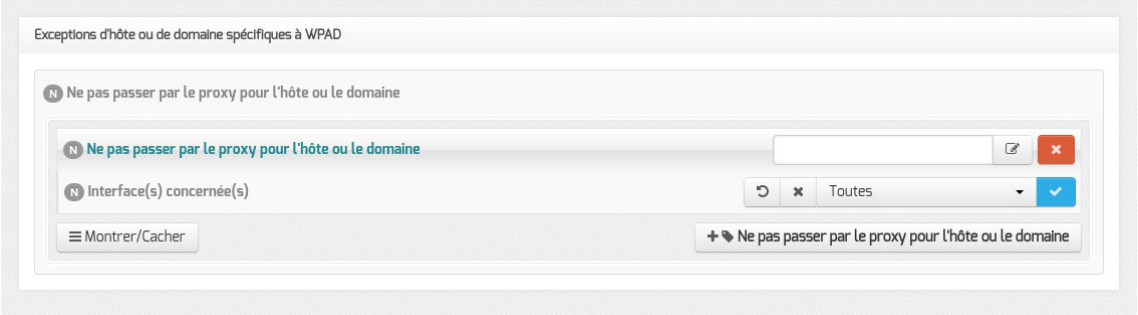


Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

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

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le` domaine (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

3.41. 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.

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

Conserver l'historique des demandes d'impression

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

Conserver les fichiers après impression

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

Purger automatiquement l'historique des travaux

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

Générer le fichier printcap

Cette variable permet de générer un fichier `printcap`.

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

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

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



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

```
# man cupsd.conf
```

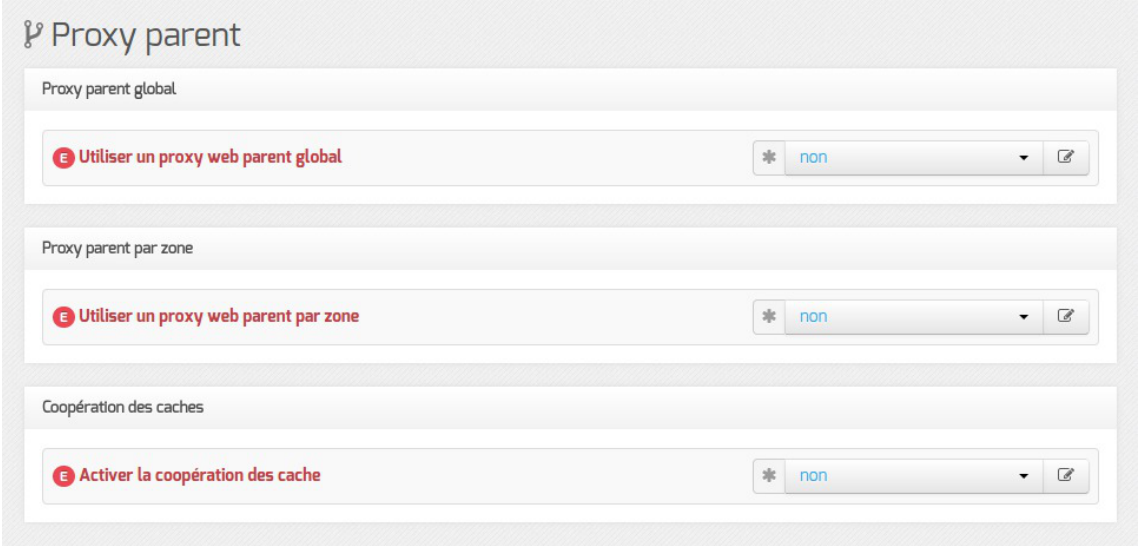
ou en visitant la page suivante : http://manpages.ubuntu.com/manpages/trusty/en/man5/cupsd.conf.5.html

3.42. Onglet Proxy parent : Chaînage du proxy

L'onglet expert `Proxy parent` permet de déclarer un ou plusieurs serveurs proxy à utiliser en amont de celui activé sur le module EOLE.

Cette fonctionnalité est à utiliser dans le cas de la mise en place d'un proxy centralisé au niveau d'une académie ou d'un groupe d'établissements.

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



Si plusieurs proxy parents sont déclarés, un mécanisme de type round-robin[p.900] est utilisé afin de répartir la charge sur les différents serveurs.

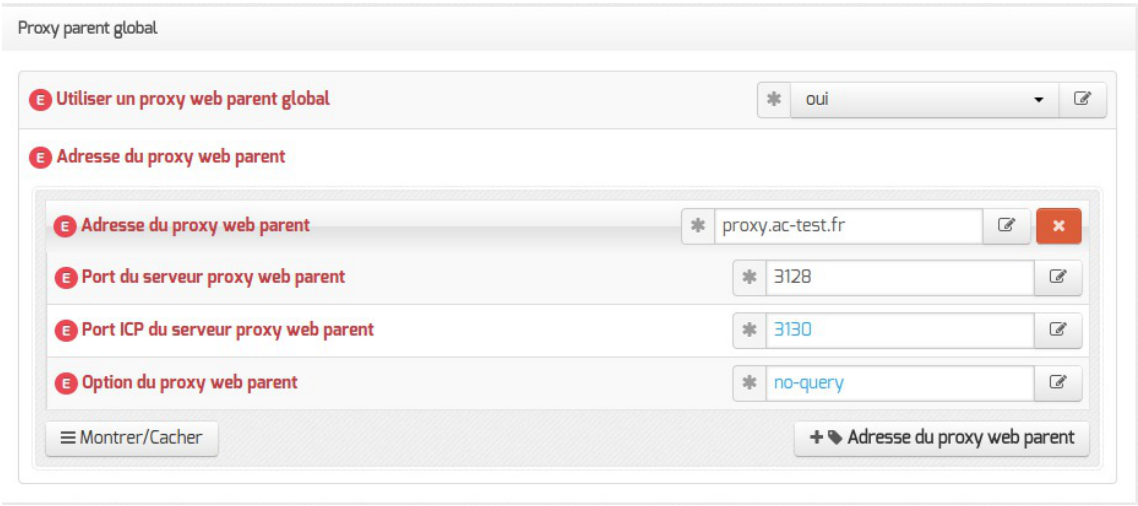


Les proxy déclarés ici ne seront pas utilisés par le serveur lui-même.

La déclaration d'un proxy à utiliser par le module EOLE s'effectue dans l'onglet `Général` en passant la variable : `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui`.

Proxy parent global

Le ou les proxy parents peuvent être déclarés de façon globale en passant la variable `Utiliser un proxy web parent global` à `oui`.



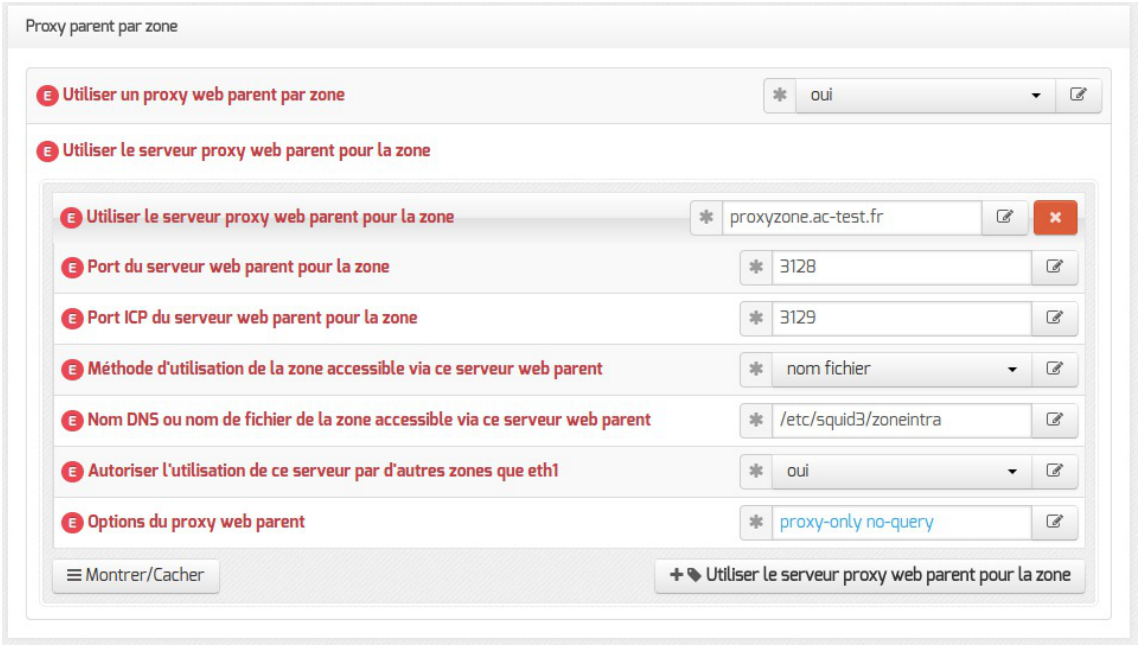
Proxy parent par zone

Pour des besoins spécifiques, des proxy parents peuvent être déclarés pour des zones DNS particulières en passant la variable `Utiliser un proxy web parent par zone` à `oui`.

Les zones DNS de destination peuvent être :

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

- soit renseignées directement dans la variable `Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent` si la `Méthode d'utilisation de la zone accessible via ce serveur web parent` est `DNS` ;
- soit renseignées dans un fichier texte dont le chemin est à indiquer dans la variable `Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent` si la `Méthode d'utilisation de la zone accessible via ce serveur web parent` est `nom fichier` ;



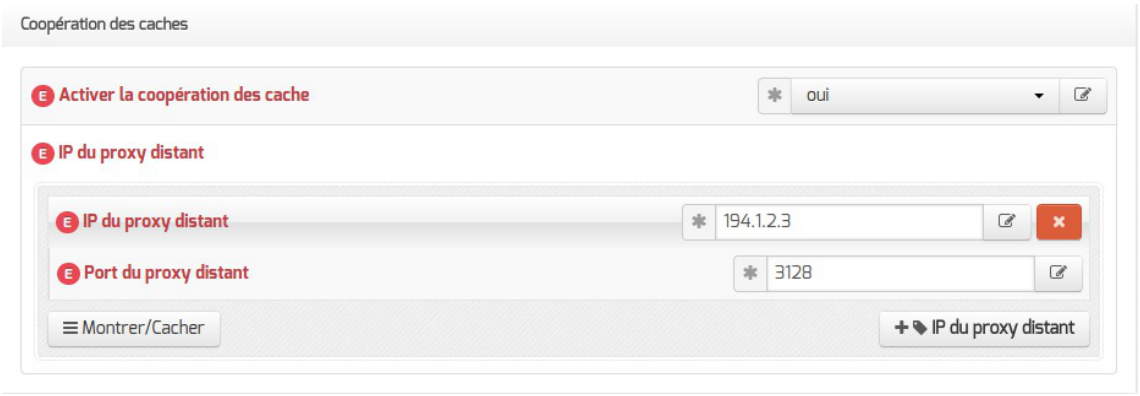
Pour que ces sous-domaines soient également pris en compte, le nom DNS du domaine doit impérativement être précédé d'un point.

Il est possible de renseigner directement plusieurs zones DNS en les séparant par des espaces, exemple : `.domain1 .domain2 .domain3`.

Coopération des caches

Si on a plusieurs proxy cache, il peut être intéressant de les faire collaborer pour partager le cache.

Cela se fait via le mécanisme de proxy sibling[p.898].



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

3.43. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.894].

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.887] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.902].

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.891]*/DNAT*.

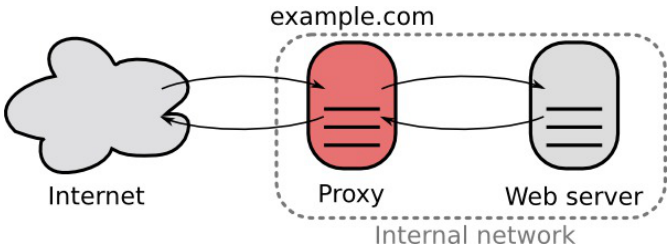
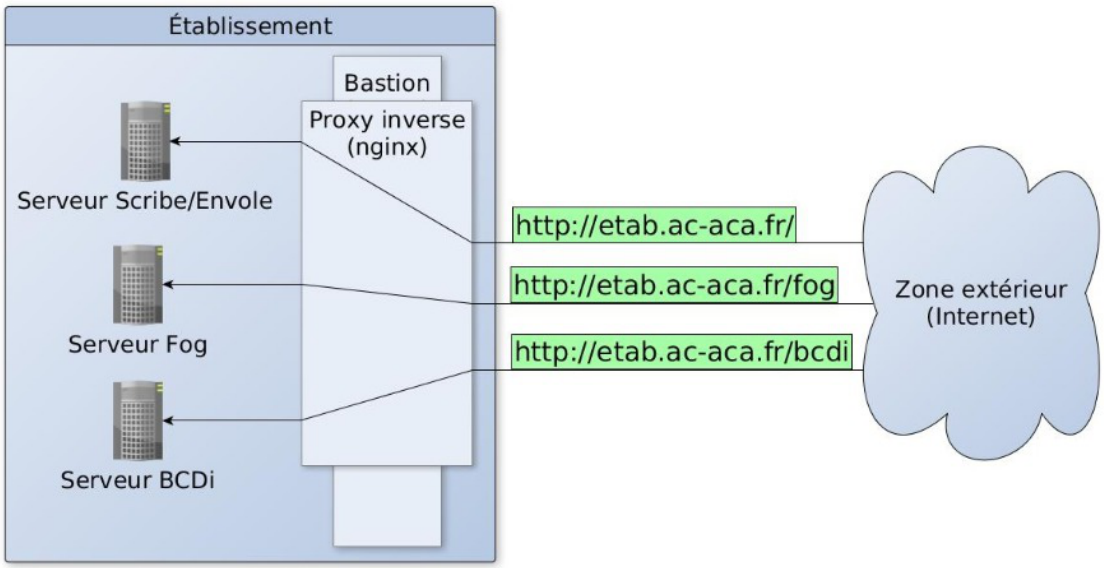


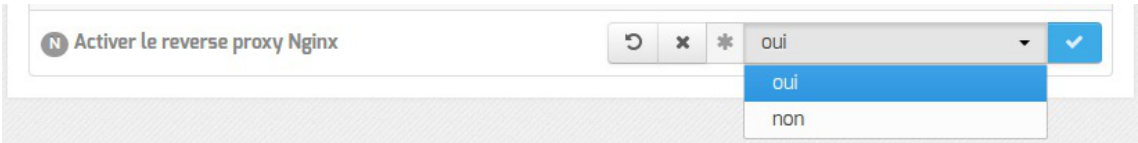
Diagramme d'un proxy inverse - Licence CC0

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

- serveur EoleSSO ;
- outil d'administration EAD[p.888] ;
- application EOP ;
- protocole HTTP[p.890] ;
- protocole HTTPS[p.890].

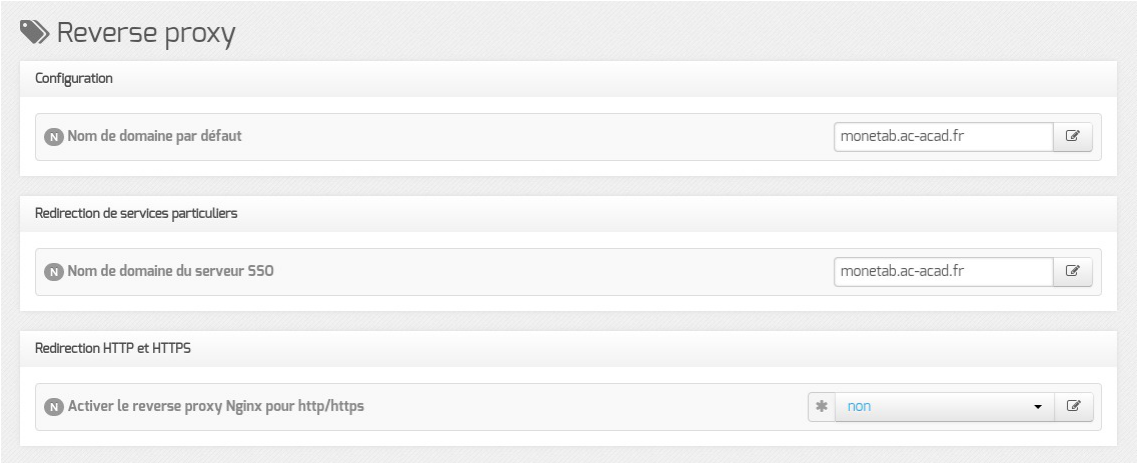


Avant toute chose, le proxy inverse doit être activé dans l'onglet `Services` en passant `Activer le reverse proxy Nginx` à `oui`.



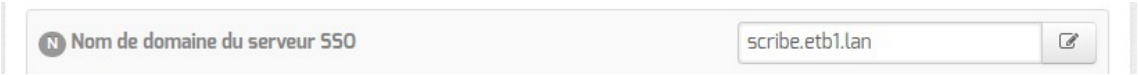
L'activation du service fait apparaître un nouvel onglet.

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



Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

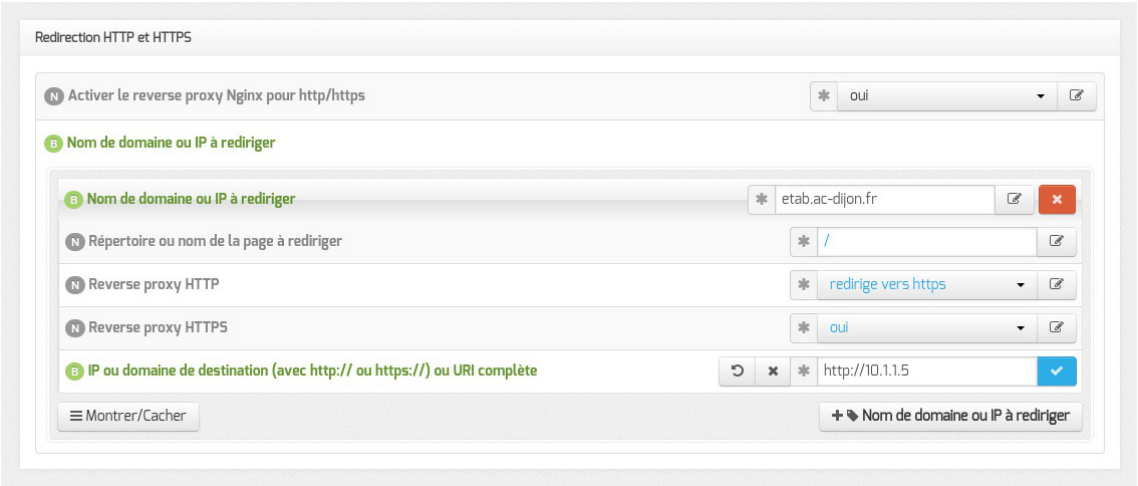


Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.



Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

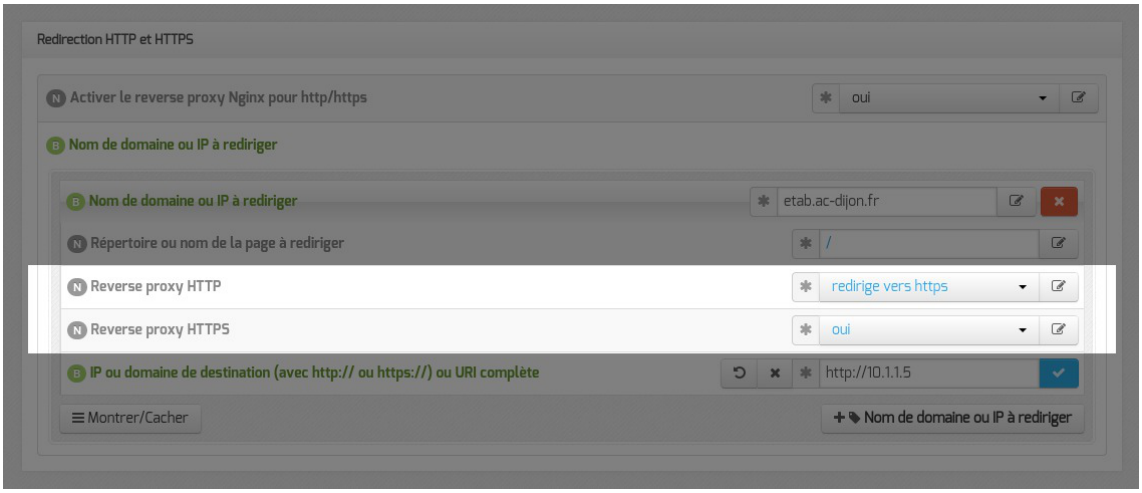


Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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 ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;

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

- 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.904] (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`.

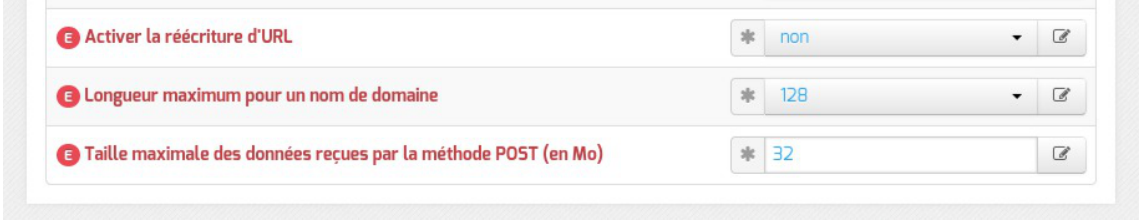
Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `Nom de domaine ou IP à rediriger`.



Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.898], `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).

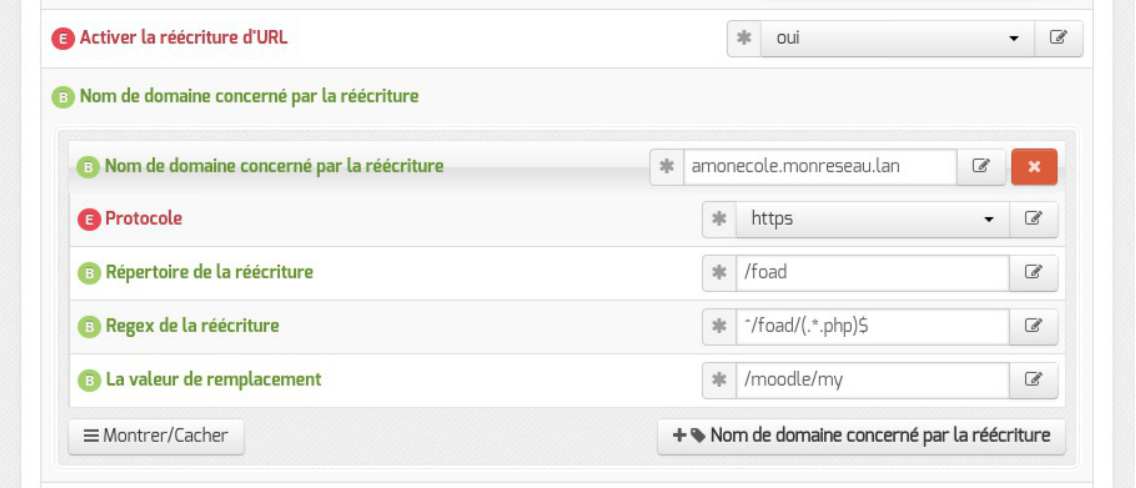
En mode expert il est possible :

- d'`Activer la réécriture d'URL` ;
- d'augmenter ou de diminuer la `Longueur maximum pour un nom de domaine` ;
- de choisir la `Taille maximale des données reçues par la méthode POST (en Mo)`.



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

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



Il n'y a pas de lien automatique entre une "redirection" Nginx renseignée et une réécriture d'URL.

Pour que la réécriture d'URL s'applique à une règle il faut que le nom de domaine, le protocole et le répertoire de la réécriture correspondent aux paramètres saisis dans la règle de "redirection" renseignée.

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

L'option du mode expert `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`).



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 le module AmonEcole et ses dérivés), le paramétrage de cette option est déplacée dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

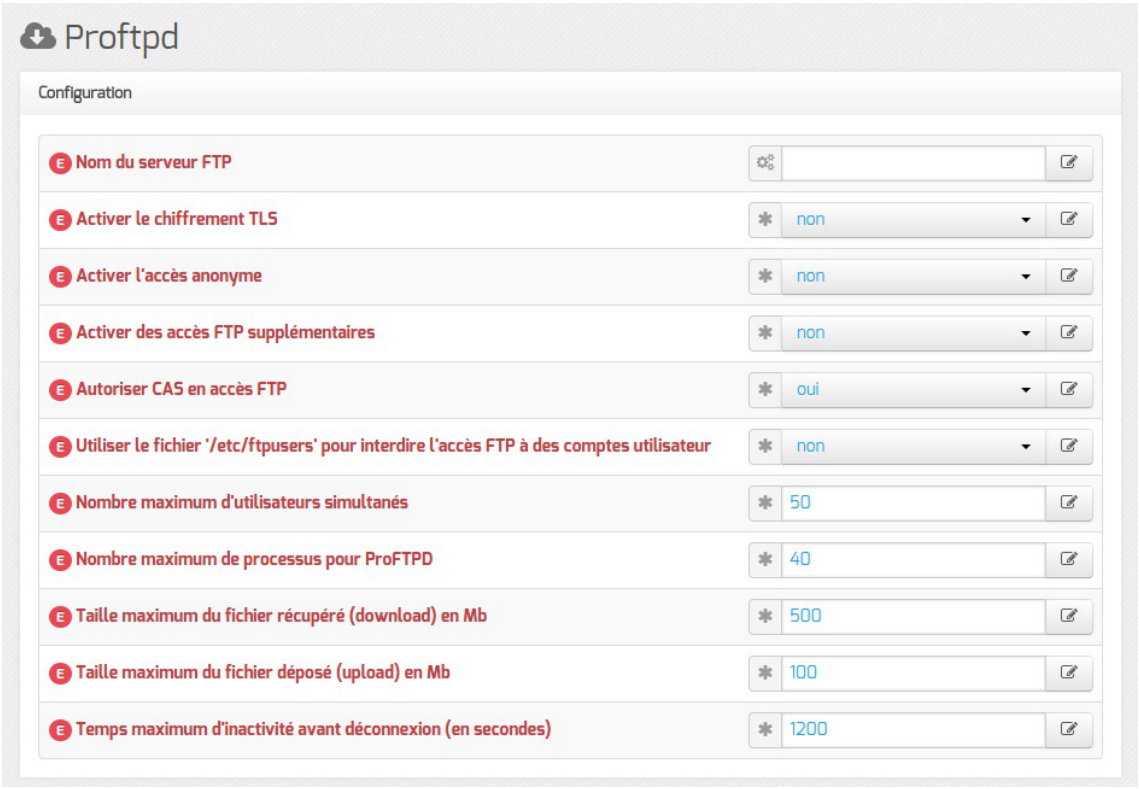
3.44. Onglet Proftpd : Configuration du serveur FTP

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/

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

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

Nom du serveur FTP

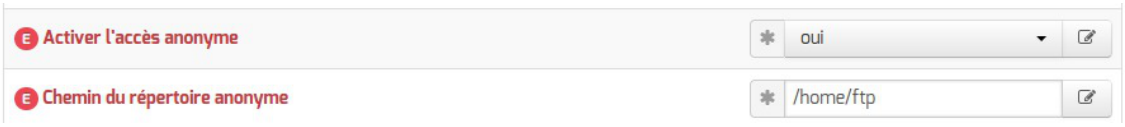
Ce paramètre permet de personnaliser le nom du serveur FTP. Ce nom apparaît lorsqu'on se connecte en FTP sur le serveur avec un client ou en ligne de commande.

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.

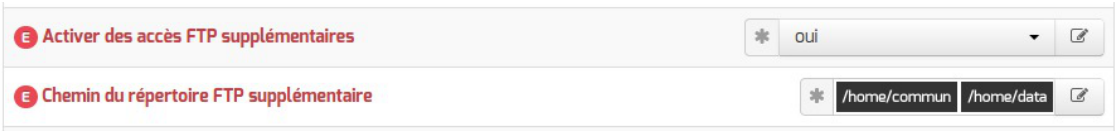
Le fichier de configuration contient la directive `<Limit WRITE>` :

```
<Limit WRITE>
DenyAll
</Limit>
```


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

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.

Utiliser le fichier /etc/ftpusers pour interdire l'accès FTP à des comptes utilisateur

Cette option ajoute la directive `file=/etc/ftpusers` au fichier de configuration /etc/pam.d/proftpd.

Le fichier /etc/ftpusers contient une liste des utilisateurs qui ne doivent pas se connecter via 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 à ce 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 dans les accès FTP le mot de passe transite en clair sur le réseau.

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.

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

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.

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.

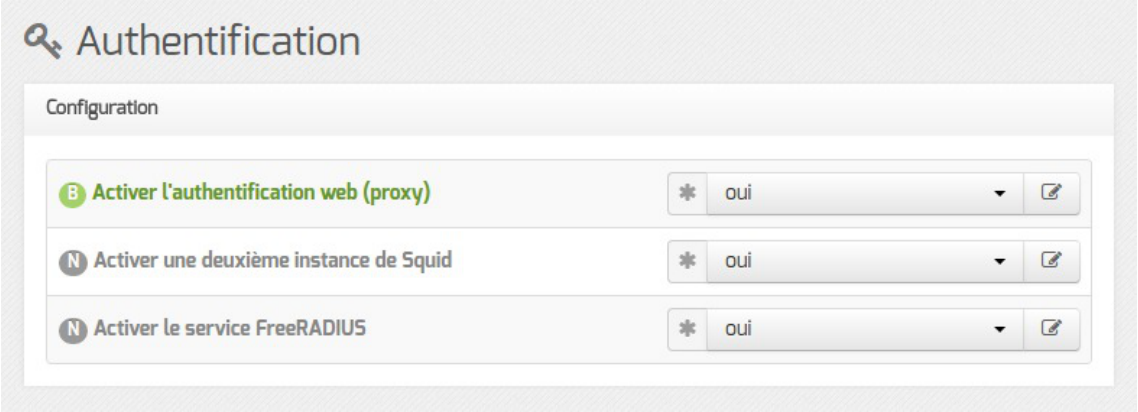
Cette restriction peut être levée en répondant `oui` à la question `Activer l'accès aux dossiers personnels des élèves pour les professeurs`. Cette option diminue légèrement la sécurité du serveur.

3.45. Onglet Freeradius : Configuration de l'authentification Radius

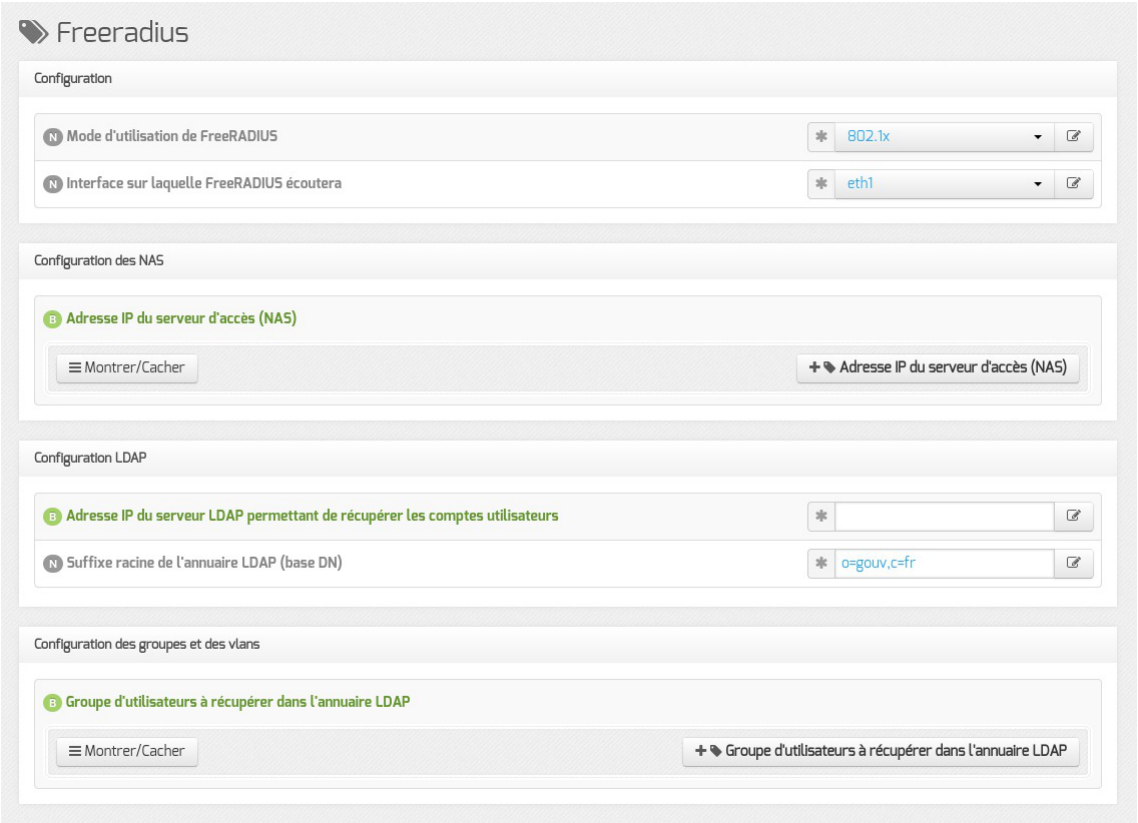
EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.899].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant `Activer le service FreeRADIUS` à `oui` dans l'onglet `Authentification`.

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



Cela fera apparaître l'onglet `Freeradius`.



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

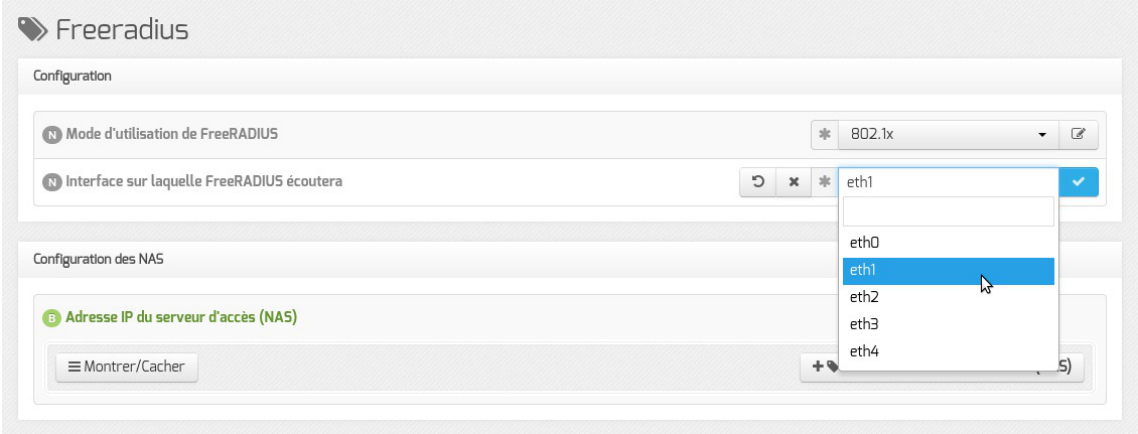
Il est possible de choisir entre 2 modes d'utilisation de FreeRADIUS :

- 802.1x ;
- accounting.

Le mode 802.1x

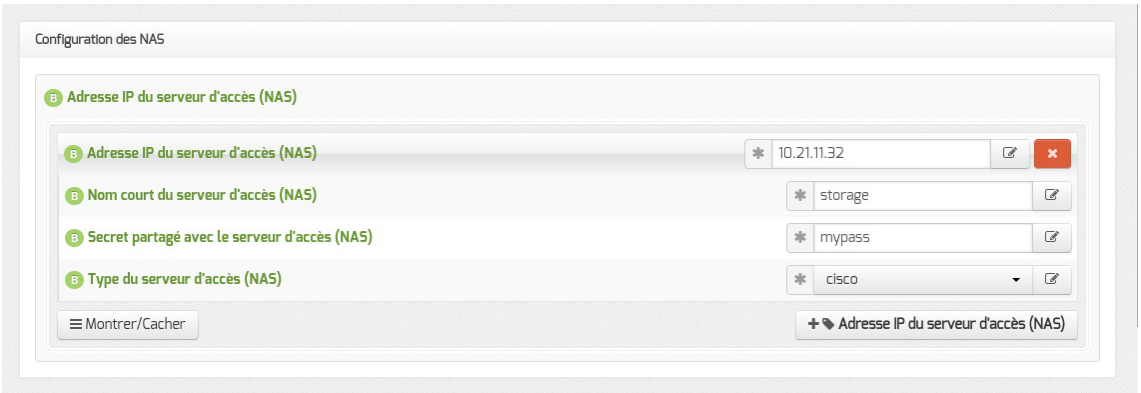
Le mode `802.1x` permet de taguer dynamiquement des ports d'un switch (NAS[p.893]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.

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



`Interface sur laquelle FreeRADIUS écoutera` : définition de l'interface d'écoute de FreeRADIUS.

Configuration des NAS



`Adresse IP du serveur d'accès (NAS)` : adresse IP du switch.

`Nom court du serveur d'accès (NAS)` : libellé du switch.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et le switch.

`Type du serveur d'accès (NAS)` : type de switch.

Configuration LDAP

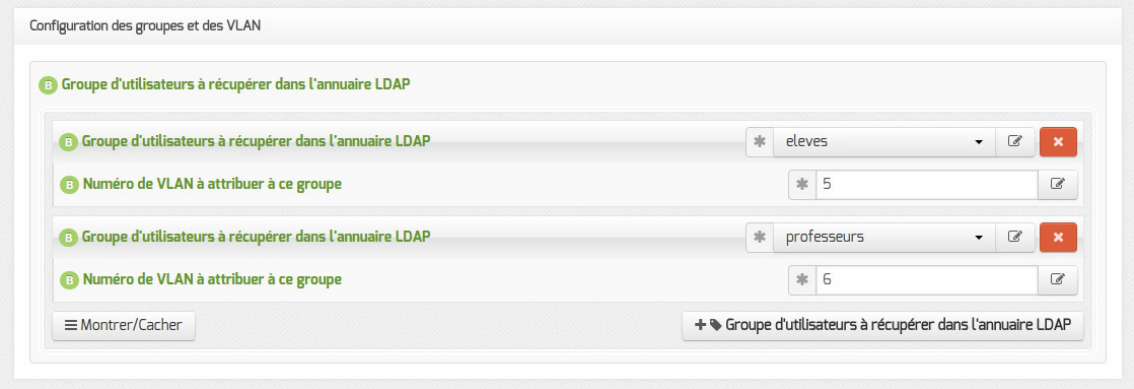


`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP LDAP.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

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

Configuration des groupes et des VLAN



`Groupe d'utilisateurs à récupérer dans l'annuaire LDAP` : saisir ou choisir un groupe existant dans l'annuaire.

`Numéro de VLAN à attribuer à ce groupe` : les machines se connectant avec un utilisateur appartenant au groupe indiqué ci-dessus verra son port tagué sur ce numéro de VLAN.

Le mode accounting

Le mode accounting permet de créer un réseau Wi-Fi WPA enterprise sur une borne Wi-Fi (NAS) ayant pour identifiants autorisés les compte/motDePasse de l'annuaire LDAP déclaré.



Onglet Freeradius - mode accounting

`Adresse IP sur laquelle FreeRADIUS écoutera` : l'adresse IP d'une des interfaces du serveur.

Configuration des NAS



Onglet Freeradius - mode accounting

`Adresse IP du serveur d'accès (NAS)` : adresse IP de la borne Wi-Fi.

`Masque de sous réseau (notation CIDR) du serveur d'accès (NAS)` : 24 (en notation

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

CIDR[p.885]) si le réseau est de classe C.

`Nom court du serveur d'accès (NAS)` : libellé de la borne Wi-Fi.

`Secret partagé avec le serveur d'accès (NAS)` : secret partagé entre FreeRADIUS et la borne Wi-Fi.

`Type du serveur d'accès (NAS)` : type de borne (other en général).

Configuration LDAP



Onglet Freeradius - mode accounting

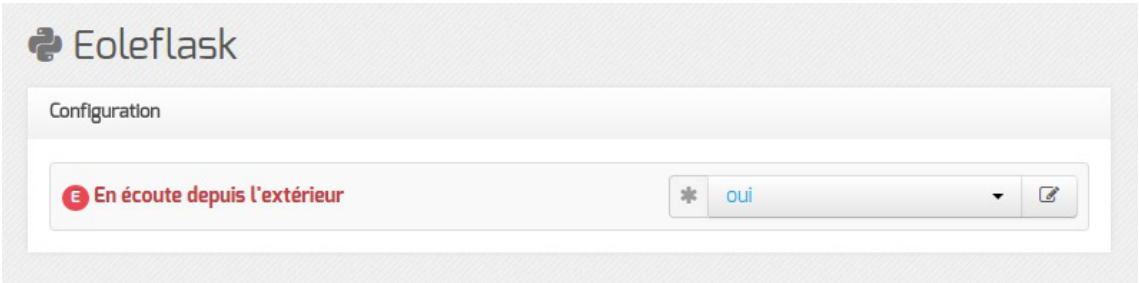
`Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs` : adresse IP ldap.

`Suffixe racine de l'annuaire LDAP (base DN)` : *ou=education,o=gouv,c=fr* par exemple.

`Clé d'accès reader à la base ldap sur Scribe (/root/.reader)` : à récupérer sur le serveur LDAP.

3.46. Onglet Eoleflask

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



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

Accès distant

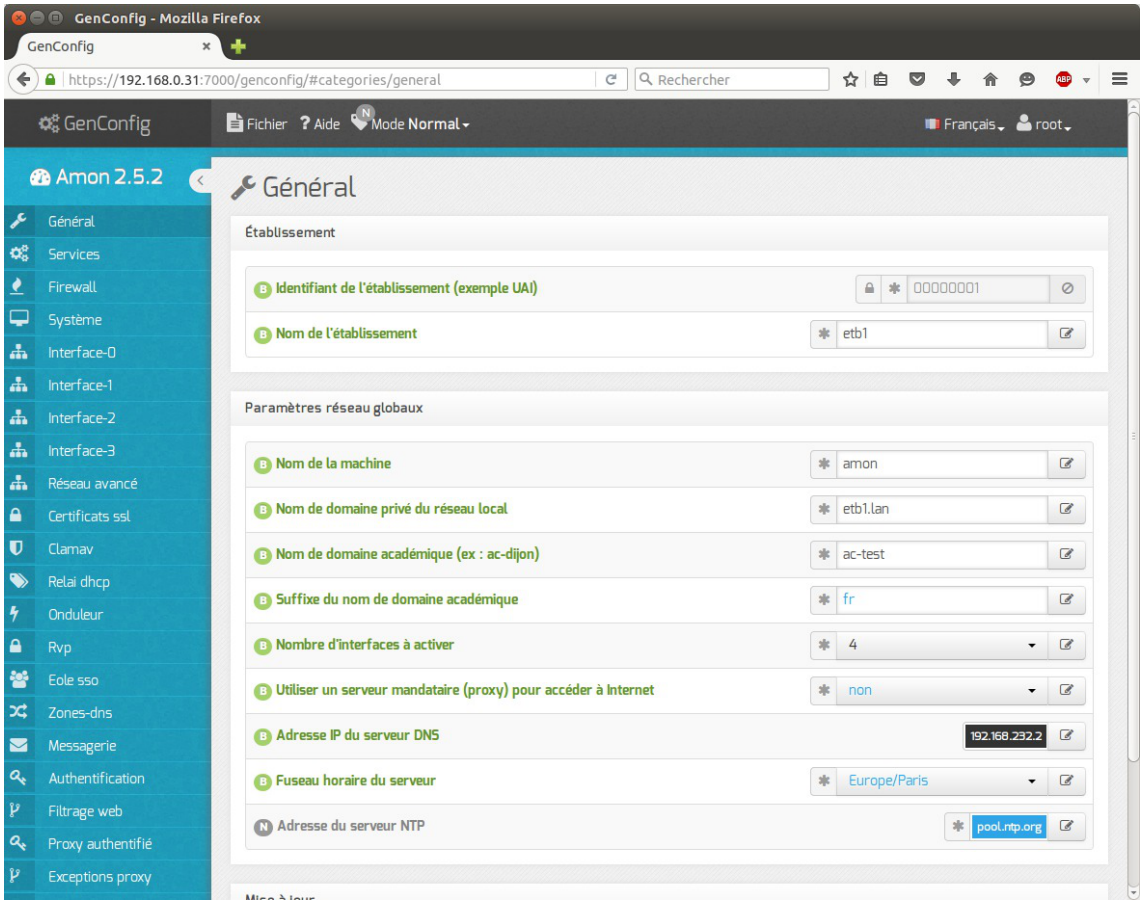
Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

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

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

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

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



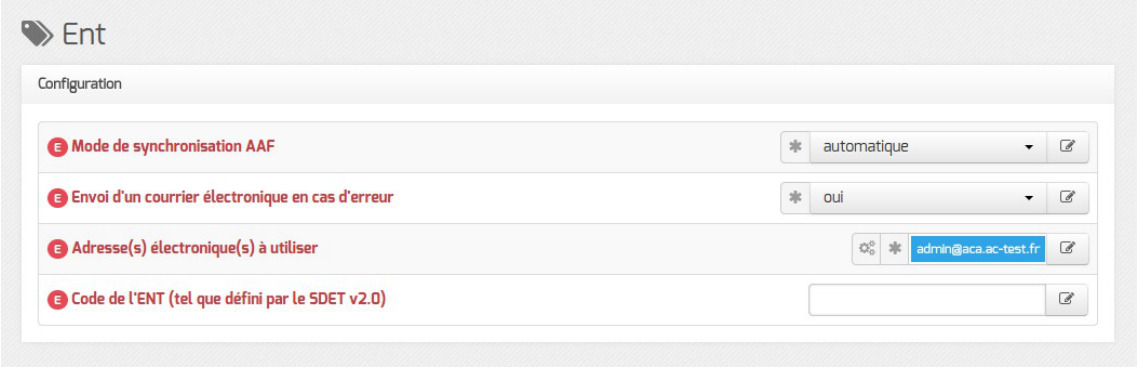
Vue de l'interface de configuration au travers d'un navigateur web

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

3.47. Onglet Ent : Configuration de l'ENT

L'onglet `Ent` permet de configurer des éléments liés à une gestion centralisée du module depuis l'Annuaire Académique Fédérateur (AAF[p.882]).

Il est possible de mettre en place un système d'importation automatisé des comptes depuis les exports de l'AAF.



Mode de synchronisation AAF

La variable `Mode de synchronisation AAF` permet de choisir entre deux modes :

- **automatique** : l'importation des fichiers est exécutée dès leur réception ;
- **manuel** : l'archive est stockée et l'importation est prête à être exécuté par l'EAD (menu `Outils` / `Synchronisation AAF`).

Envoi d'un courrier électronique en cas d'erreur

Que la synchronisation soit manuel ou automatique l'option `Envoi d'un courrier électronique en cas d'erreur` permet d'envoyer des courriers électroniques en cas d'erreur lors de l'import AAF.

Si l'envoi de courrier est activé un nouveau champs `Adresse(s) électronique(s) à utiliser` propose de personnaliser la ou les adresses destinataires de ce message.

Code de l'ENT (tel que défini par le SDET v2.0)



La télédistribution d'identifiants ENT a été intégrée conformément aux préconisations du SDET[p.901] version 2.0 mais ce mode de fonctionnement n'a pas été retenu dans ses versions ultérieures.

Le cahier des charges ENT du SDET version 2.0 requérait :

"un identifiant unique sur le périmètre national mais qui ne permet pas d'être associé à l'identité de l'accédant [...] Cet identifiant est de la forme « LxxCiiii » avec :-

- L et C : lettre et chiffre du code projet ENT- ;
- xx et iiii : 2 lettres et 4 chiffres à générer pour chaque entrée".

Dans le cadre du module Scribe, c'est l'attribut LDAP **ENTPersonLogin** qui est utilisé pour le stocker.

Des plages d'identifiants ENT peuvent être distribuées aux établissements via le module Zéphir.

Le serveur Scribe doit donc être enregistré sur un module Zéphir (de préférence académique).

L'attribution des identifiants ENT uniques se fait ensuite automatiquement lors de la création et l'importation d'utilisateurs.

Voir aussi...

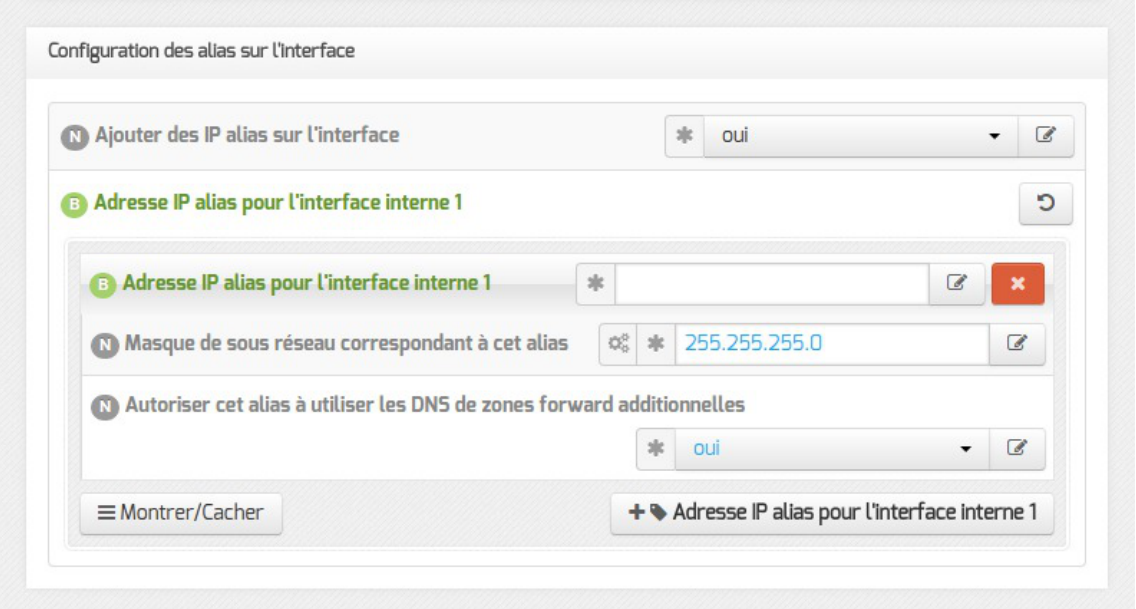
Synchronisation depuis l'Annuaire Académique Fédérateur - AAF [p.556]

4. Configuration DNS pour chaque interface

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

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

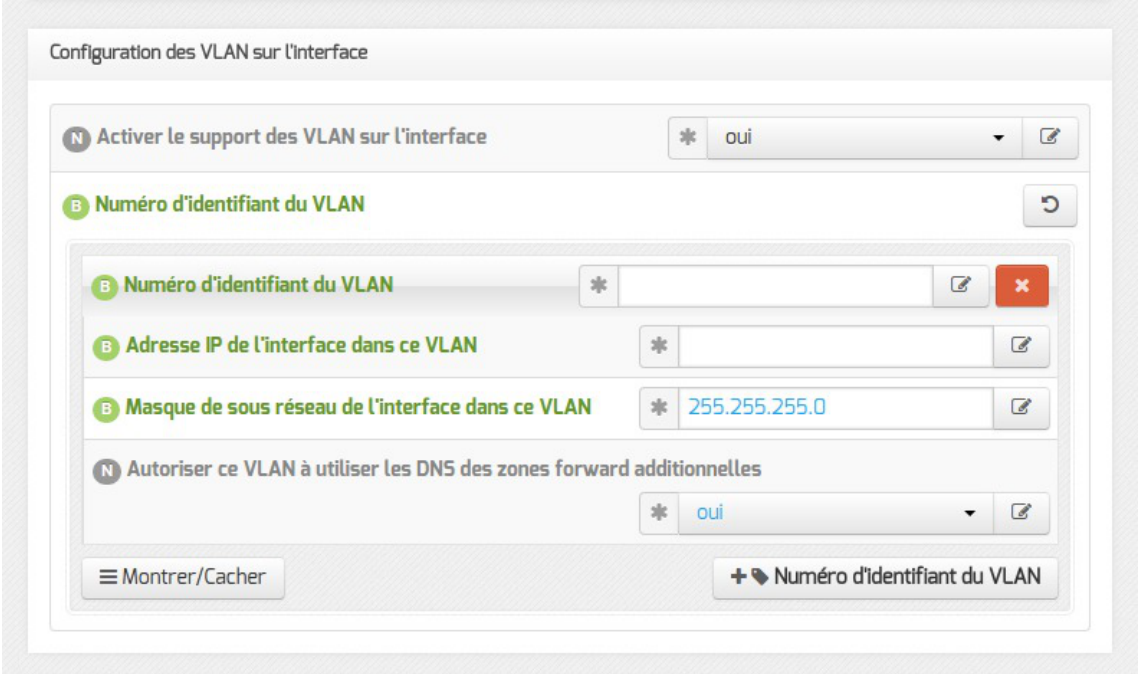
Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (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 son support (`Activer le support des VLAN sur l'interface` à `oui` et ajout d'un numéro identifiant du VLAN avec le bouton `+ Numéro d'identifiant du VLAN`) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

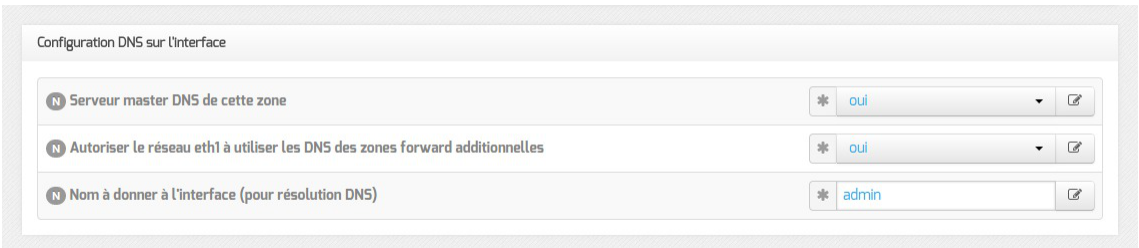
`Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Si le support du RVP est activé une option supplémentaire est disponible :

- `Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.



- `Serveur master DNS de cette zone` : sert à activer le DNS sur l'interface.
- `Autoriser le réseau ethX à utiliser les DNS des zones forward additionnels` : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section `Forward de zone DNS` de l'onglet `Zones-dns`.

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

- `Nom à donner à l'interface (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

Si le support du RVP est activé une option supplémentaire est disponible :

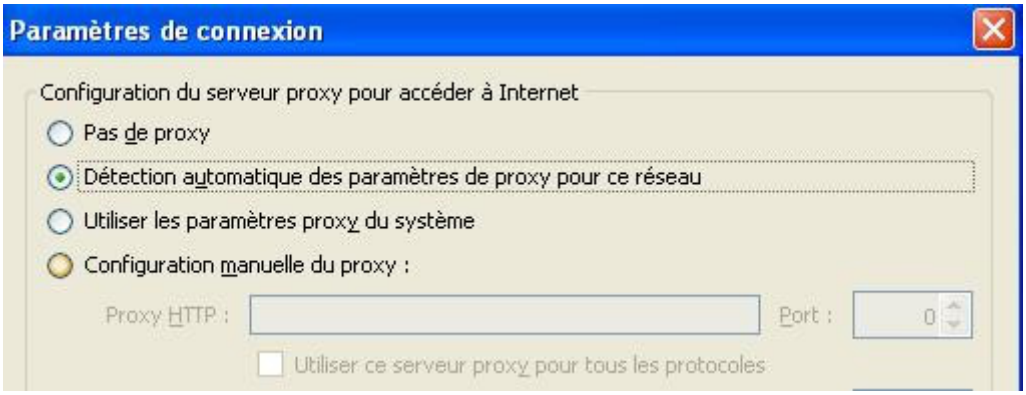
- `Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

5. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.905] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm[p.886] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

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

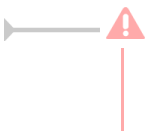
- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx[p.894] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom domain local>` qui pointe vers le serveur web ;
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

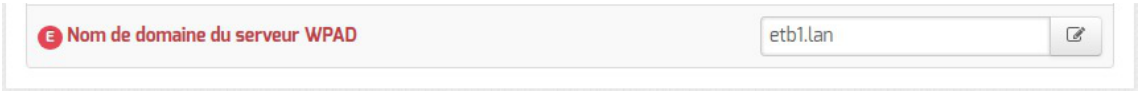
Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.

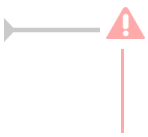


Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.

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.



Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.



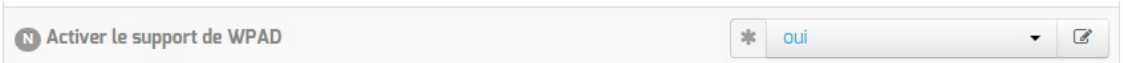
Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

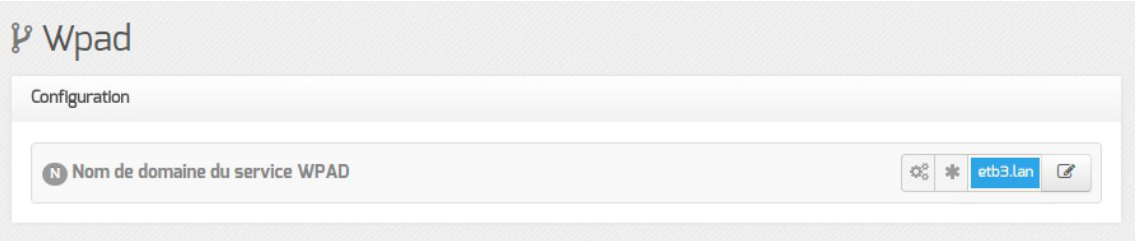
Le support de WPAD doit être activé et correctement configuré sur le module Amon.



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

Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Ajouter des exclusions dans la configuration automatique du proxy

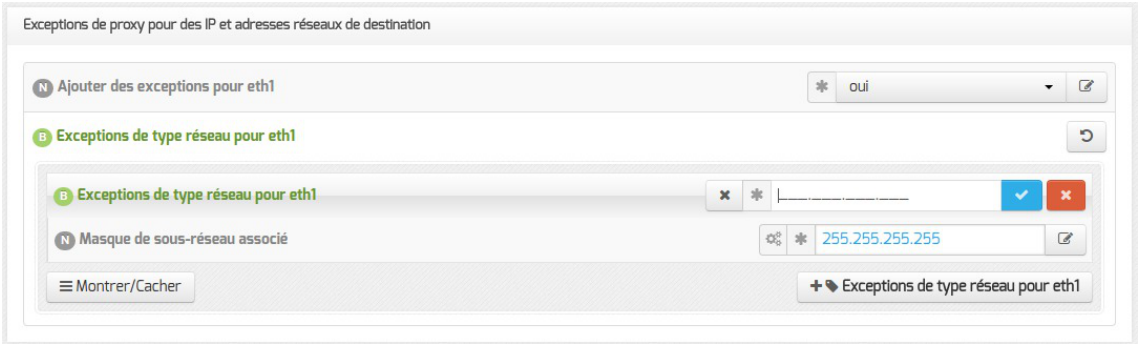
Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.

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



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

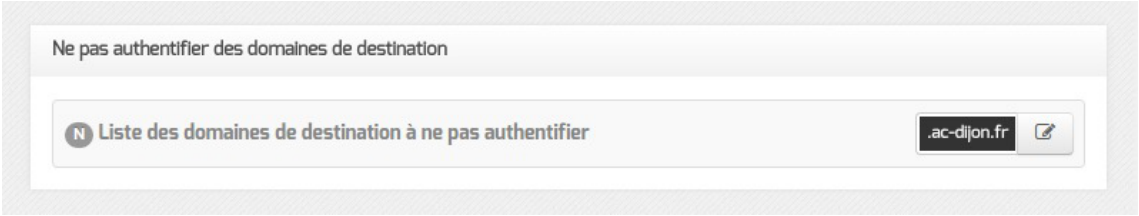
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

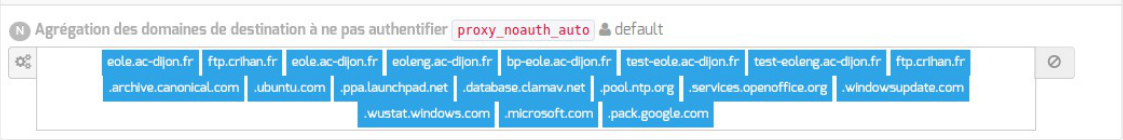
Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy noauth auto`.

Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du

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

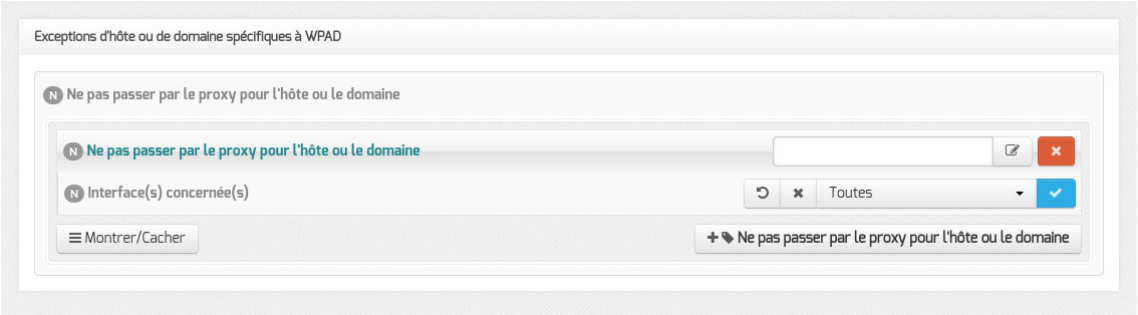
module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.



Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.



Compléments sur `Ne pas passer par le proxy pour le` domaine (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP [p.158]

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

6. Configuration du mode multi-établissement

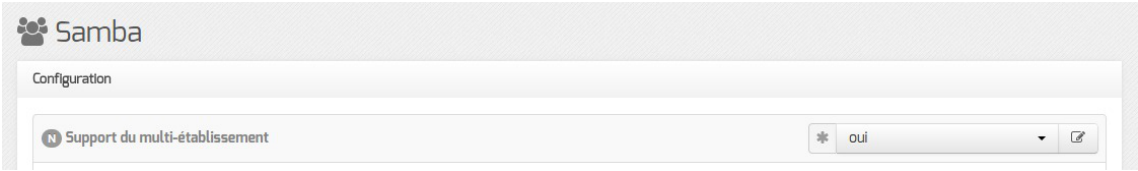


Ce mode de configuration doit être considéré comme expérimental.

Il est fortement déconseillé de passer d'un mode à l'autre sur un serveur en production.

Pour certaines structures, une communauté de communes par exemple, il peut être intéressant de n'avoir qu'un seul module Scribe ou AmonEcole pour gérer plusieurs établissements.

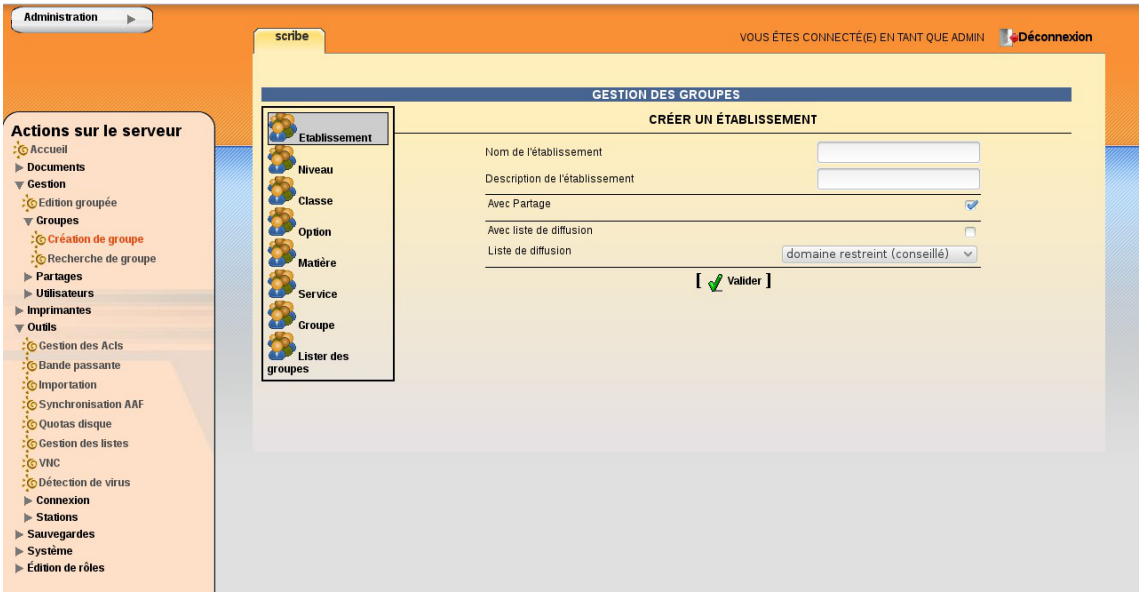
Pour activer le mode multi-établissement il faut se rendre dans l'interface de configuration du module en mode normal, et dans l'onglet `Samba` passer à `oui` l'option `Support du multi-établissement`.



Activation du mode multi-établissement dans l'interface de configuration du module

L'établissement par défaut est celui déjà déclaré dans la variable `Identifiant de l'établissement (exemple UAI)` de l'onglet `Général`.

Le reste des réglages, la création d'un nouvel établissement et l'ajout des utilisateurs se fait dans l'EAD une fois le module instancié ou reconfiguré.



Vue de l'EAD : création d'un établissement

Il est possible d'ajouter un ou plusieurs établissements dans le menu principal de l'EAD. Il faut se rendre dans `Gestion` → `Groupes` → `Création de groupe` → `Etablissement`.

Les champs à remplir sont :

- le `Nom de l'établissement` ;
- un `Descriptif de l'établissement` ;
- `Avec partage` ;
- `Avec liste de diffusion` ;

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

- le type de liste de diffusion.

Le bouton Valider permet d'enregistrer la configuration du nouvel établissement.

Le peuplement de l'établissement se fait via l'outil d'importation de l'EAD : menu de l'EAD → Outils → Importation.

Outil d'importation de l'EAD

> Importation de comptes [p.371]

7. Authentification unique avec EoleSSO

7.1. Présentation du produit EoleSSO

Description du produit

EoleSSO est un serveur d'authentification développé pour répondre à la problématique du SSO[p.902] (authentification unique) dans différentes briques de l'architecture EOLE. Il est développé en langage Python à l'aide du framework Twisted[p.903].

Ce produit implémente en premier lieu un serveur d'authentification compatible avec le protocole CAS[p.885].

Une partie du protocole SAML[p.901] 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.902] (SSO) dans EoleSSO est basée sur le protocole CAS[p.885].

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 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.

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

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).

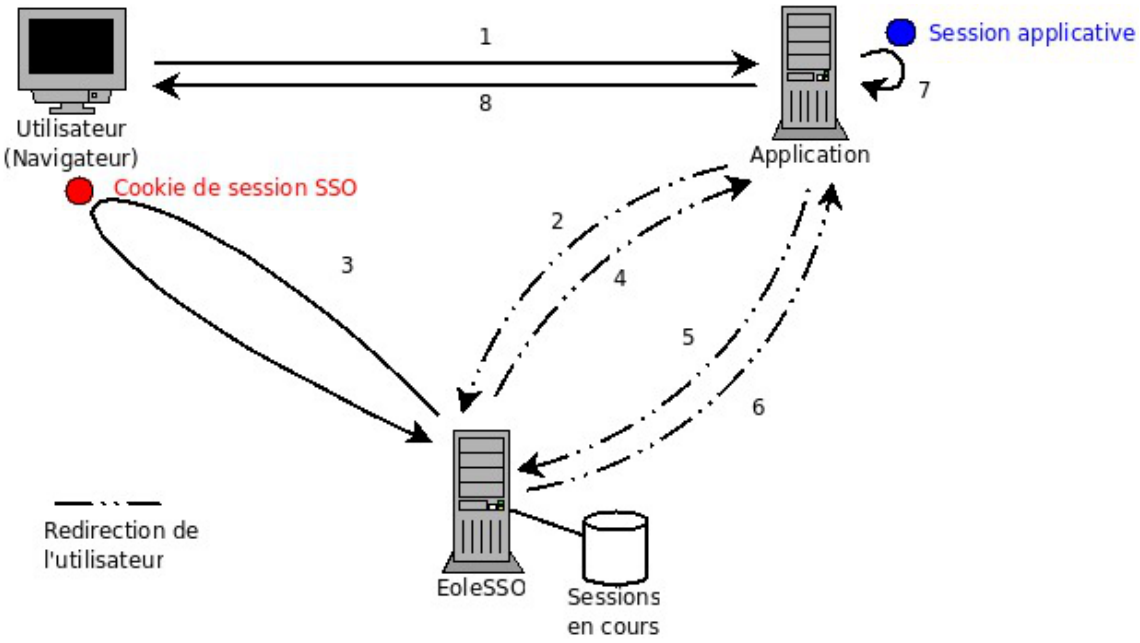
Les applications clientes n'ont pas accès à l'identifiant de la session utilisateur, il est échangé uniquement entre le serveur d'authentification et le navigateur.

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 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).

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

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

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

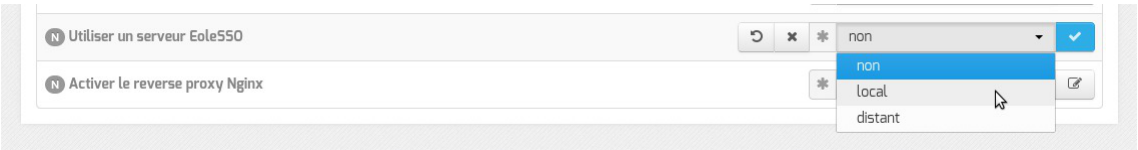
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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`.



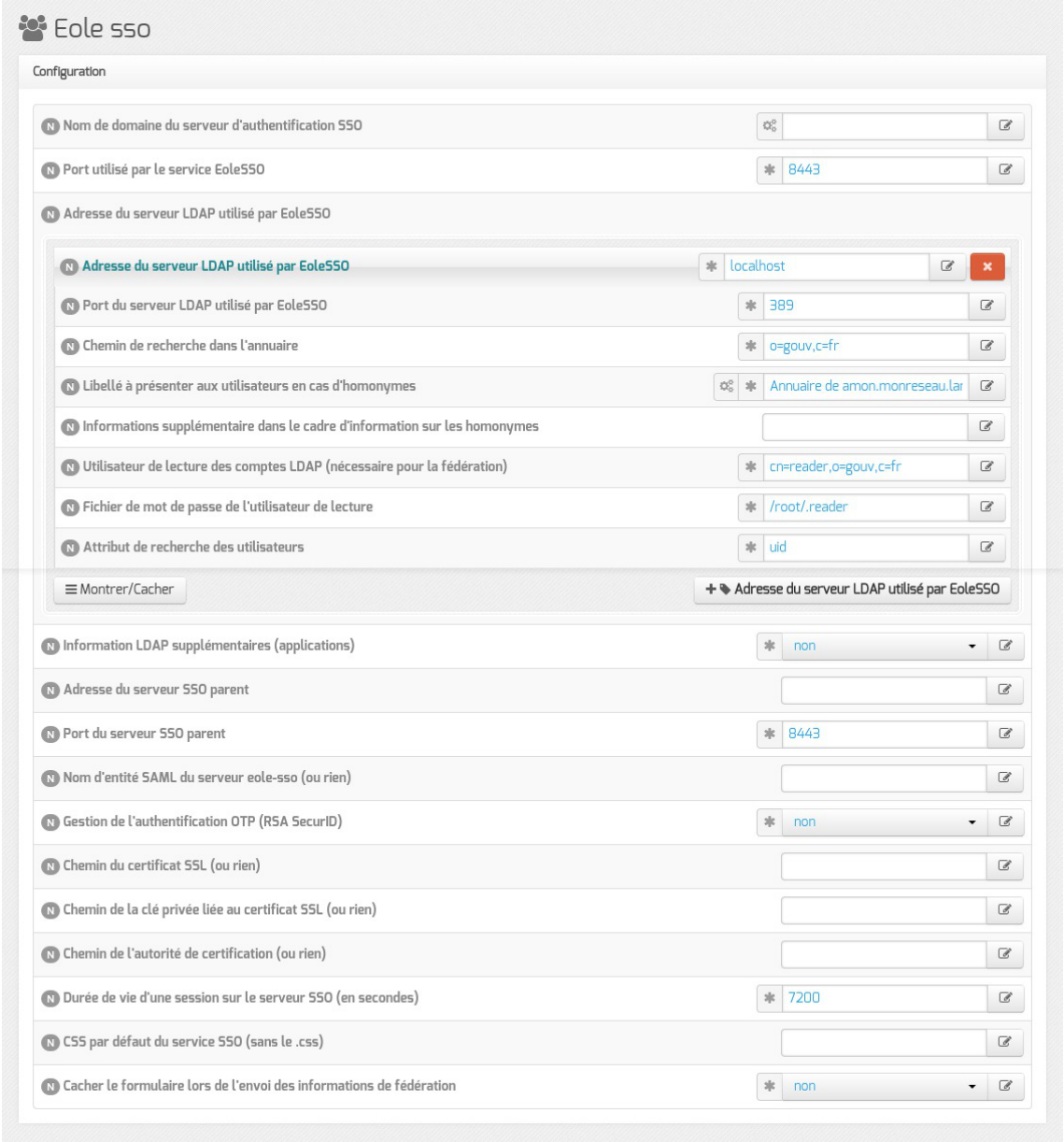
La variable `Utiliser un serveur EoleSSO` permet :

- `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).

Adresse et port d'écoute

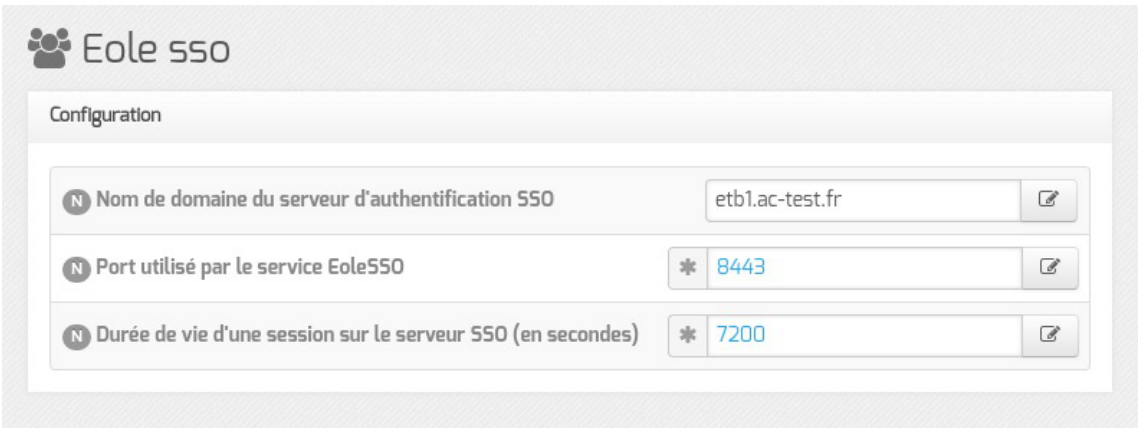
L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

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



Configuration d'un serveur EoleSSO local

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



Configuration d'un serveur EoleSSO distant

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.

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

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

Configuration LDAP

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

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP[p.897] si disponible *(voir plus loin)*.



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

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

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

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

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

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

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

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

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

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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC[p.906] 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.901] 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

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

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.891] 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.901] (version 2).

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

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

Autres options

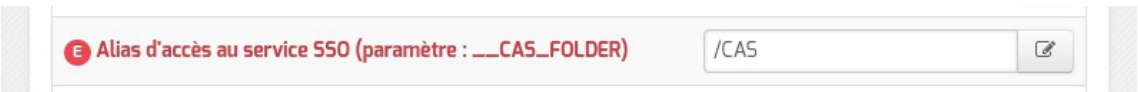
`Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra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

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

Configuration en mode expert

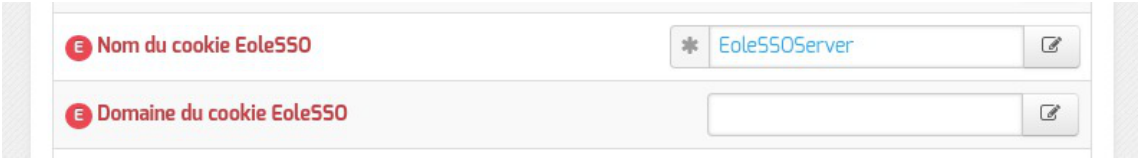
Options générales

En mode expert plusieurs nouvelles variables sont disponibles :

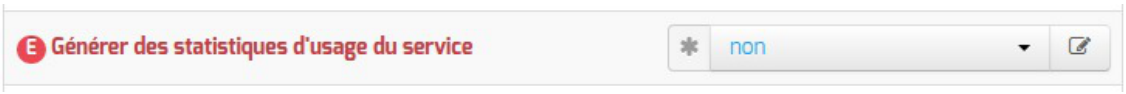


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP ou keycloak.

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



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

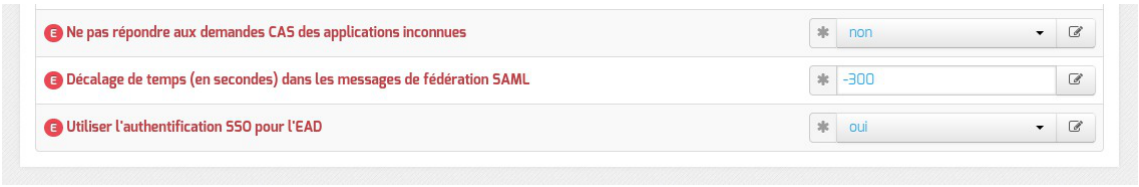


- `Générer des statistiques d'usage du service` est à `non` par défaut.

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



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



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

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

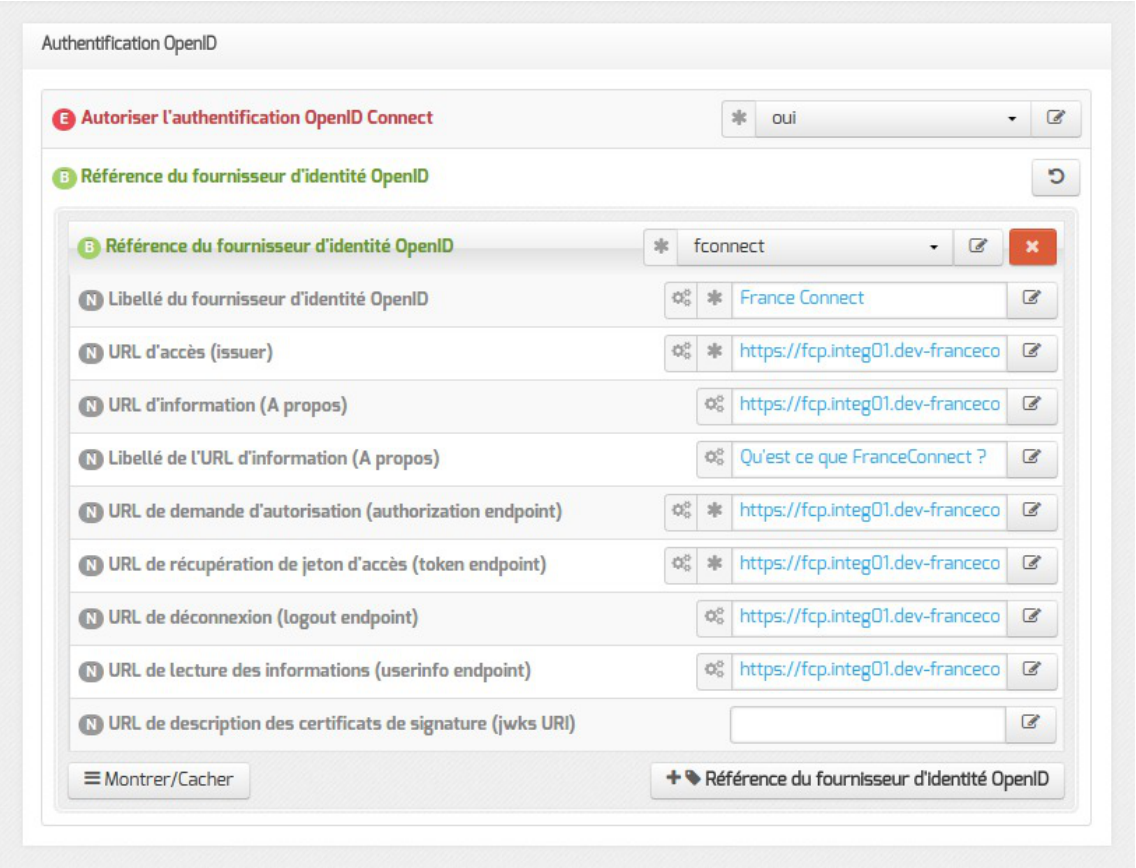
- `Décalage de temps (en secondes) dans les messages de fédération SAML` est à `-300` secondes par défaut

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

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

Configuration d'authentification OpenID Connect

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



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

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

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

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.286]

Compatibilité OpenID Connnect [p.265]

7.3. Protocoles supportés

7.3.1. Compatibilité CAS

Fonctions implémentées au niveau serveur

Le serveur EoleSSO implémente le protocole CAS[p.885].

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

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

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.

7.3.2. 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.901] . 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.

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 :

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

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.

7.3.3. 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.901] (authentification de type One Type Password).

L'authentification est effectuée par l'intermédiaire du module PAM[p.897] 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.897].

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.

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

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.

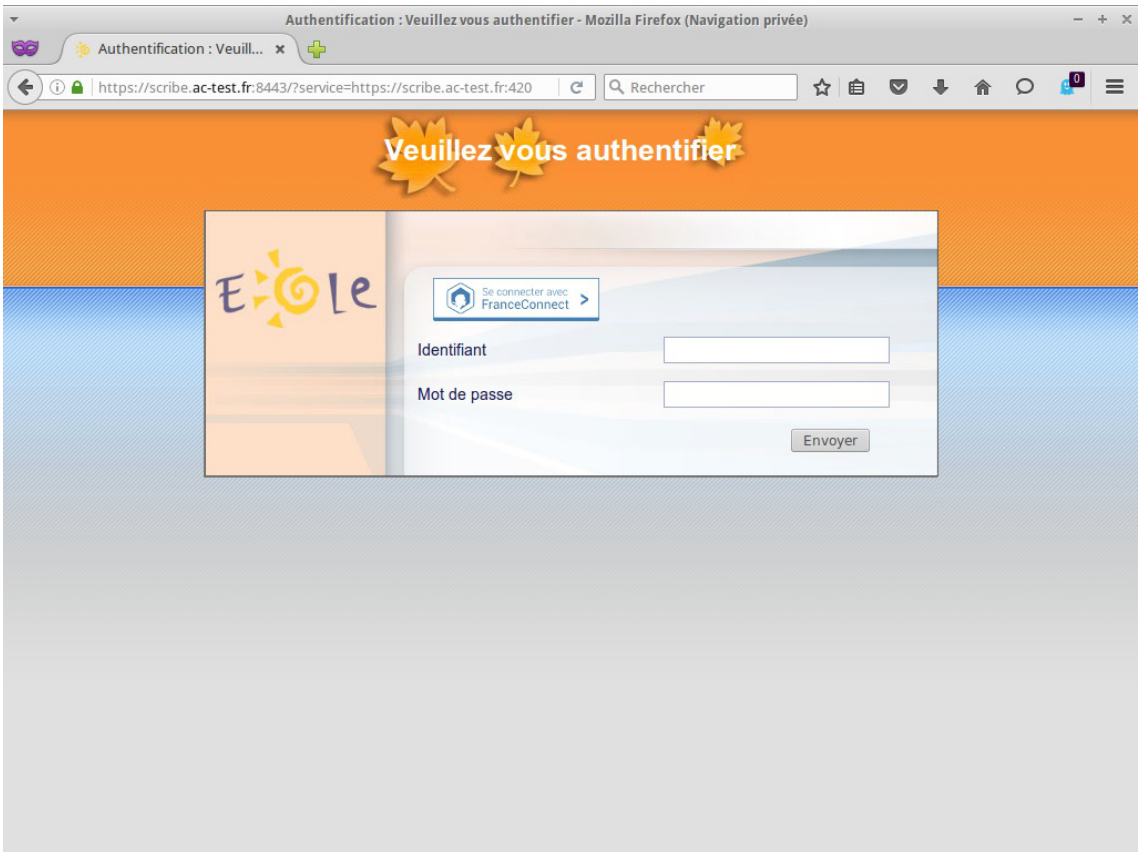
7.3.4. Compatibilité OpenID Connnect

Des modifications ont été apportées à EoleSSO pour permettre d'authentifier les utilisateurs auprès du fournisseur d'identité France Connect[p.890].

Il est également possible de configurer d'autres fournisseurs d'identité OpenID Connect[p.896] dans les limites des fonctionnalités implémentées. Seul France Connect et l'authentification OAuth[p.895] 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 ;



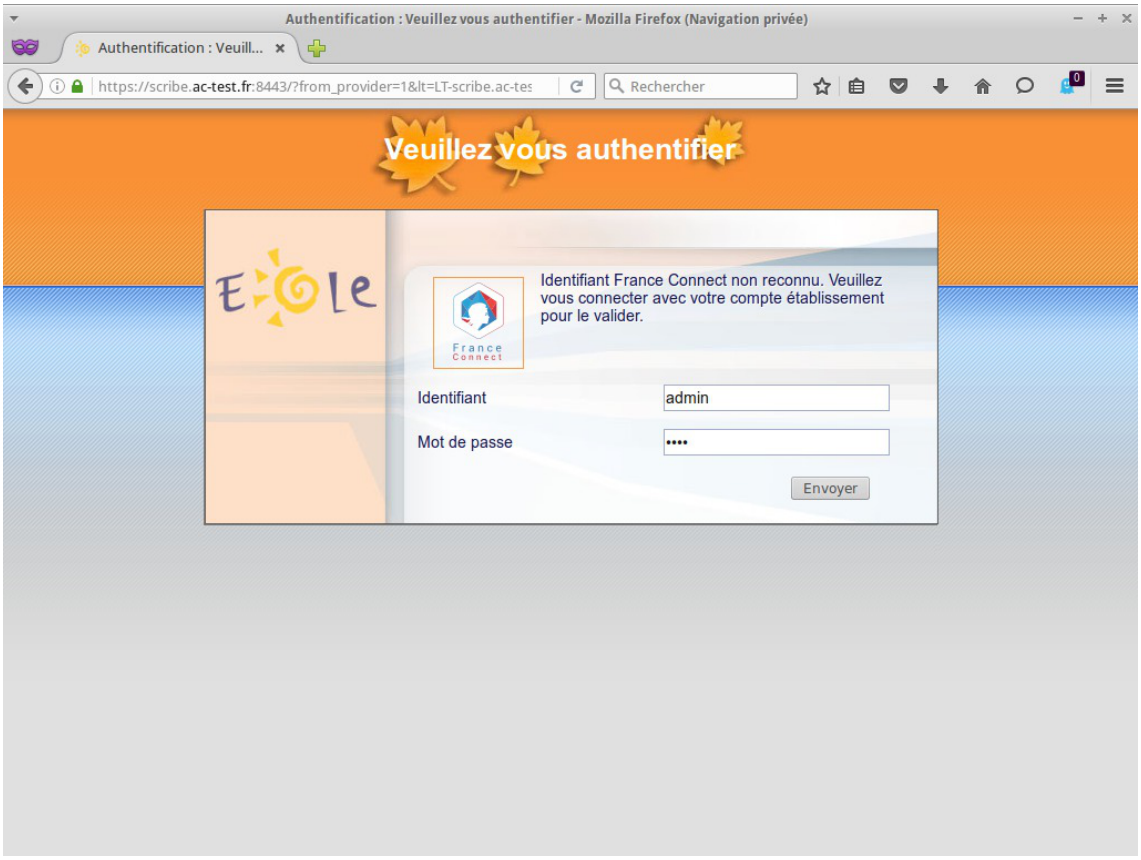
- lorsqu'un utilisateur clique sur un de ces boutons, il est redirigé vers le portail de connexion du fournisseur correspondant ;

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



- 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 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 ;

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



- 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 client.

Un principe de configuration automatique est prévu par le protocole, mais il est rarement

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

> 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).

7.3.4.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.



> 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

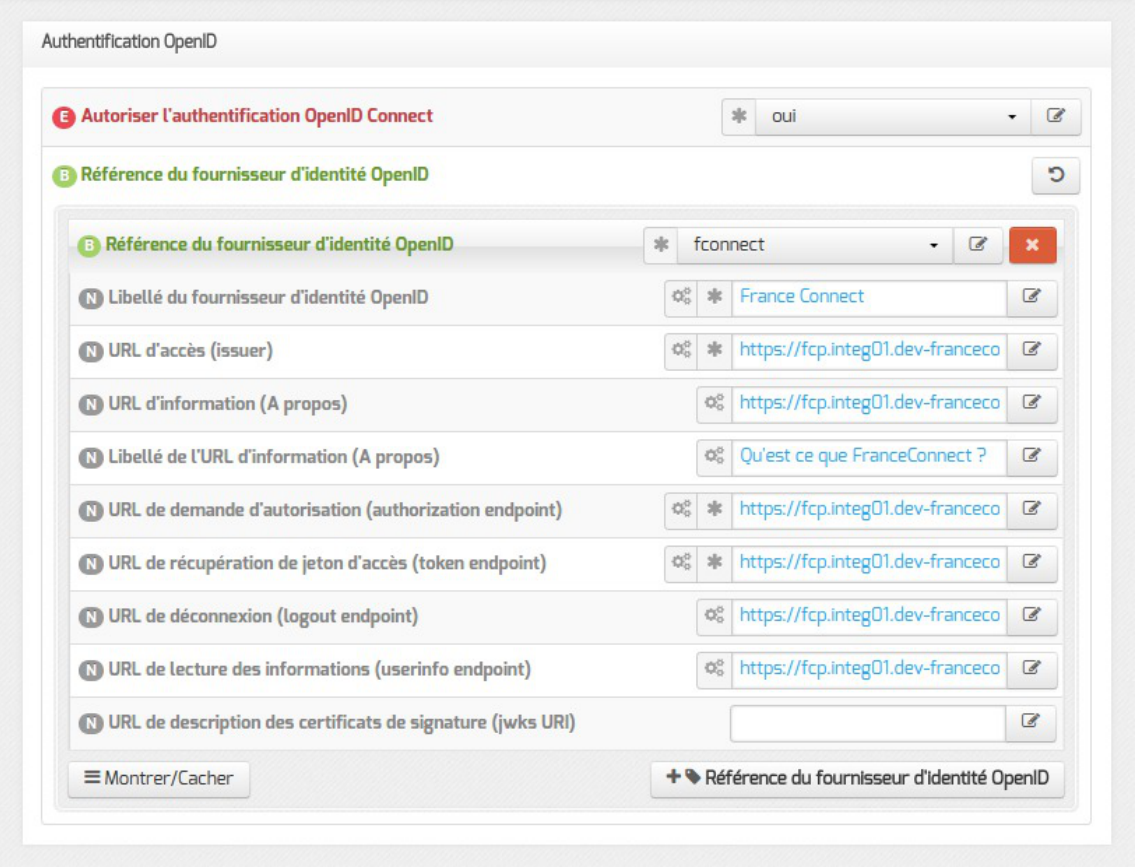
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.901].

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>"
```

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`.

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.189]

7.3.4.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 ;
- `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 :

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

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.189]

7.4. 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
```

7.4.1. 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.

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

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]` ;
- 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` ;

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

- 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 ;
- `disciplines` : les matières enseignées pour un professeur ;
- `niveaux` : le niveau (attribut `Mefclf`) d'un élève ou les niveaux dans lesquels un professeur enseigne ;
- `secureid` : identifiant opaque calculé avec un MD5 de l'UID et du RNE de l'utilisateur ;

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

- `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()]
```

7.4.2. 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 mis dans le répertoire `/usr/share/sso/app_filters` et leur nom doit se terminer par `_app.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

`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

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

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/eole-sso.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.

`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

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

- envoi d'un ticket PGT à un client CAS en mode proxy

7.4.3. 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` (correspond à l'exemple du paragraphe précédent).

```
[utilisateur]
user=uid
codeUtil=uidNumber
nom=sn
prenom=givenName
```


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

```
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`

7.5. 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.901] 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.

7.5.1. 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).

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

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

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.893]), il est conseillé d'utiliser cette solution dans le cadre d'un réseau sécurisé (par exemple, à travers un RVP). Le cas échéant, on préfèrera la solution proposée dans le paragraphe suivant.

7.5.2. Fédération SAML : Gestion des Associations

La solution retenue pour effectuer une fédération entre deux systèmes est l'utilisation de messages SAML[p.901] 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.890]) 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 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).

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

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 :

- 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

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

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 correspondant 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 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)

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

- `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.

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

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

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/eole-sso.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 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.

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



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.

7.5.3. 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.890] 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
- 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.

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

7.5.4. 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).

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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).



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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**.

7.5.5. 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 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=....
```

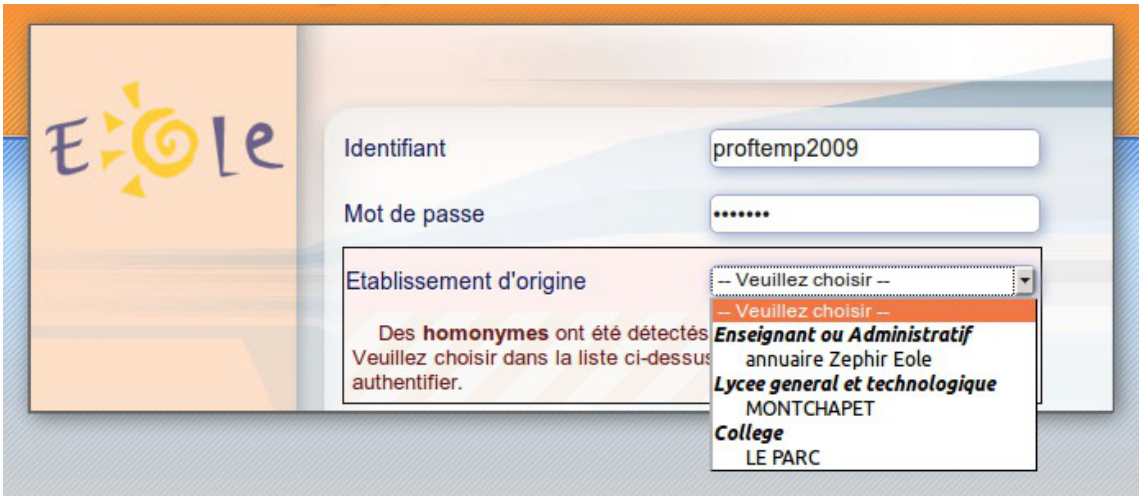

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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.

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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.189]

7.6. 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).

7.7. 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.899] (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 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

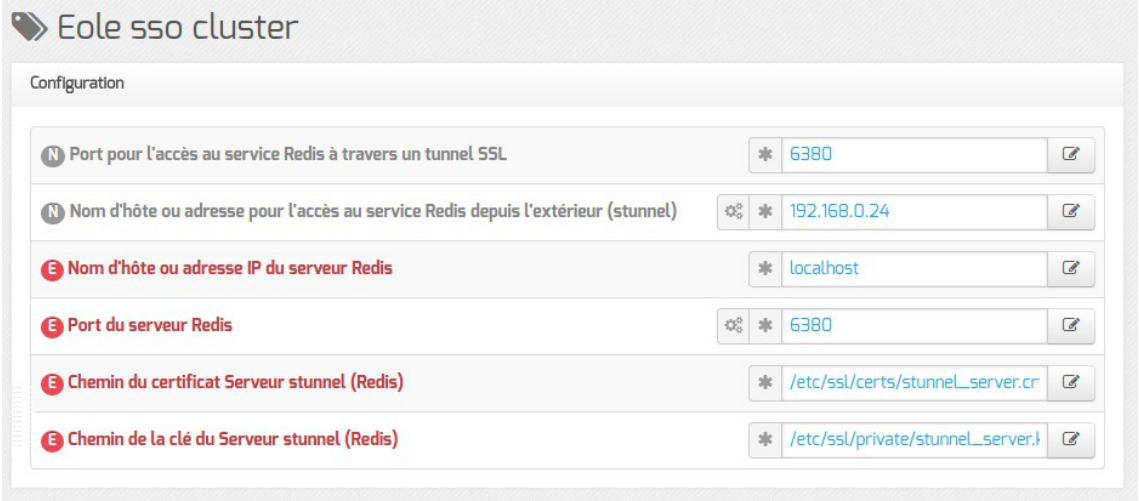
Sur un module Eole, il faut installer le paquet dédié à l'aide de la commande suivante :

```
# 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
```

`/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.903]...).

Voir aussi...

Répartition de charge EoleSSO en mode cluster [p.294]

7.8. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

suivants :

- `sso-1.ac-academie.fr` ;
- `sso-2.ac-academie.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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Penser à redémarrer le service haproxy :

```
# service haproxy restart
```

Mise en place de Prometheus et de Grafana

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.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
```

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,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "values": false
          },
          "lines": true,
          "linewidth": 0,
          "links": [],
          "nullPointMode": "connected",
          "percentage": false,
          "pointradius": 5,
          "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
            }
          ]
        },
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
        {
          "bars": true,
          "datasource": null,
          "editable": true,
          "error": false,
          "fill": 10,
          "grid": {},
          "id": 4,
          "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,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "logBase": 1,
            "max": null,
            "min": null,
            "show": true
          },
          {
            "format": "short",
            "label": null,
            "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": [],
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
          "timeFrom": null,
          "timeShift": null,
          "title": "Nombre de tickets de sessions (auth)",
          "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
            }
          ]
        }
      ],
      "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,
```


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": 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,
```


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": 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"
```


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": "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,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "total": false,
            "values": true
          },
          "lines": true,
          "linewidth": 1,
          "links": [],
          "nullPointMode": "null as zero",
          "percentage": false,
          "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",
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "label": null,
            "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": 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,
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
            "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
            }
          ]
        }
      ],
      "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"
    ],
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
637     "time_options": [
638       "5m",
639       "15m",
640       "1h",
641       "6h",
642       "12h",
643       "24h",
644       "2d",
645       "7d",
646       "30d"
647     ]
648   },
649   "timezone": "browser",
650   "title": "SSO Copy",
651   "version": 0
652 }
```

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

7.9. Compléments de configuration EoleSSO

7.9.1. 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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `/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

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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `/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 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

7.9.2. Astuces d'exploitation

Journalisation du service

Le fichier de journalisation du service EoleSSO est `/var/log/eole-sso.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`) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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`).

7.9.3. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Placer ce fichier dans le répertoire `/usr/share/sso/metadata` (dans cet exemple, `fim_sp.xml`) du serveur EoleSSO et redémarrer le service.



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>

7.9.4. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 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

7.9.5. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Rechercher la section concernant le paramétrage pour Linux (ligne 362 dans la version testée) :

```
'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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 d'EOLE inférieure à 2.5.0 ou dans le répertoire `/lib/x86_64-linux-gnu/security/` dans le cas contraire.

7.9.6. 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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'application n'est pas installée par défaut. Via l'interface de configuration du module, configurer le serveur pour recevoir les applications web :

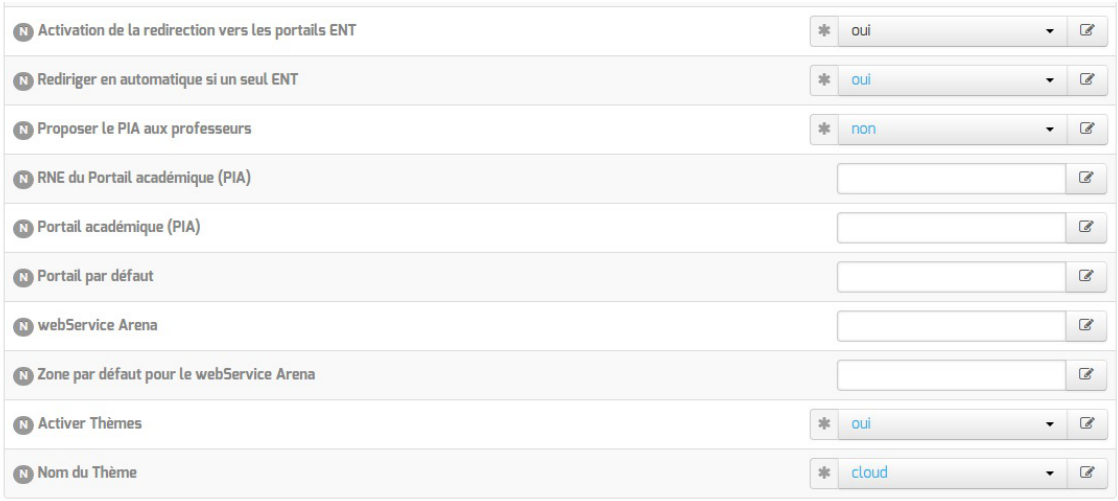
- en mode normal dans l'onglet `Services`, passer `Activer le serveur web Apache` à `oui` ;
- dans l'onglet `Applications web`, saisissez le nom de domaine des applications web dans `Nom de domaine des applications web (sans http://)` ;
- enregistrer la configuration et quitter l'interface de configuration 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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une fois le serveur reconfiguré, l'application est accessible à l'adresse : `http://<adresse serveur>/edispatcher/`

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`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

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.883].

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) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `scoens.ac-reunion.fr` (depuis le réseau pédagogique des établissements) ;
- `scoweb.ac-reunion.fr` (depuis le réseau administratif).

Chaque portail, en fonction de sa zone de confinement, ne présentera pas les mêmes ressources et l'utilisation d'une clé OTP[p.897] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

https://scoweb.ac-reunion.fr.

La variable `arena`, permet de spécifier la zone ClearTrust associée au portail. Elle est 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 [p.286]

7.9.7. 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

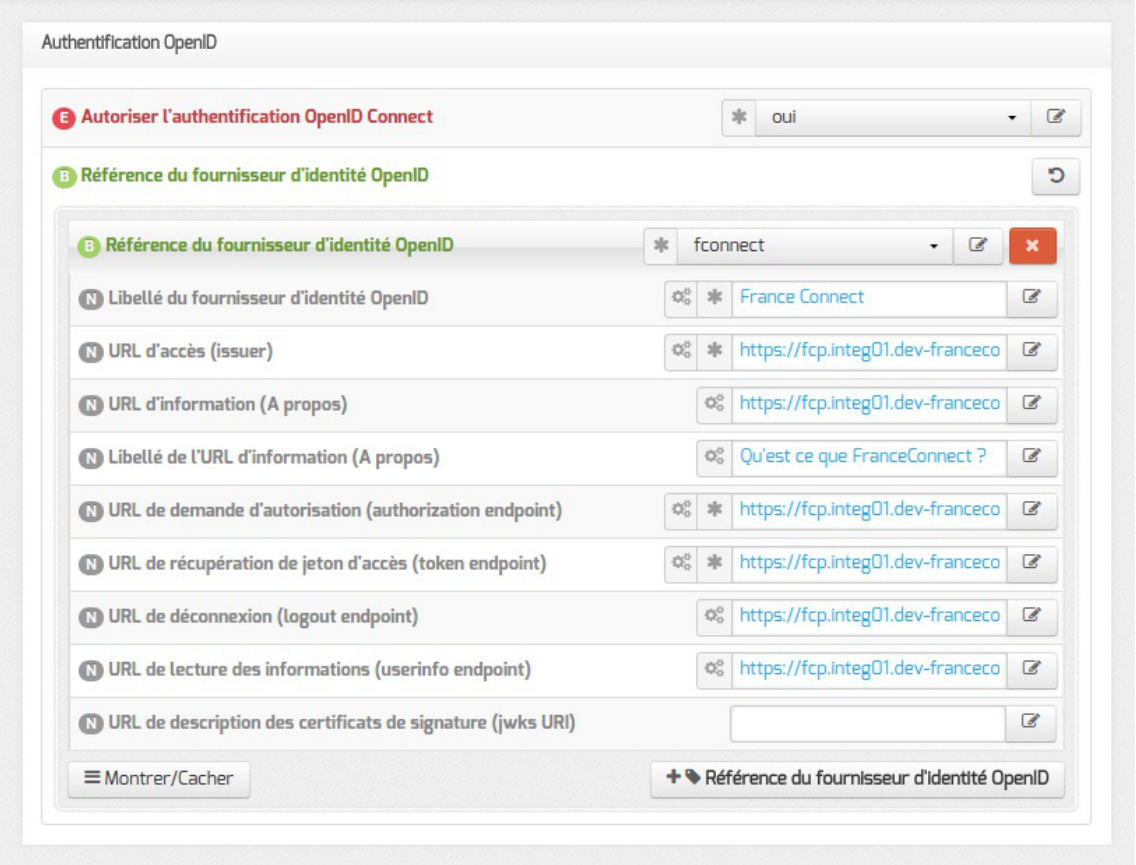
Les conditions d'utilisation de France Connect et le processus de raccordement sont décrites dans le document PDF suivant :

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.901].

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 [p.189]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

7.9.8. 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` :

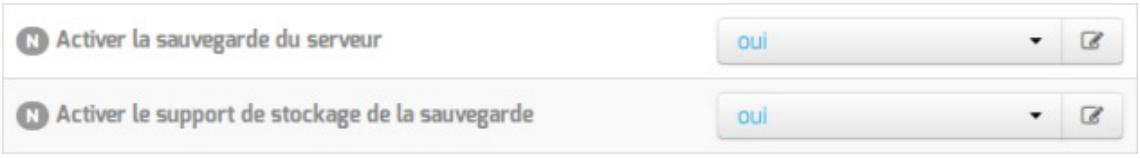
```
<nom_fournisseur> = "<client id> :<client secret>"
```

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` .

8. Activation et configuration de Bareos

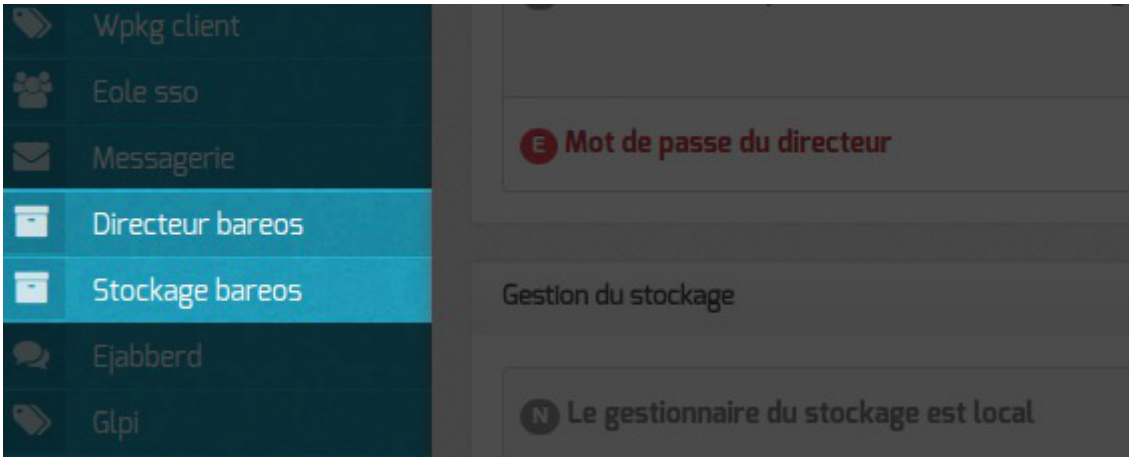
La sauvegarde du serveur et le support de stockage de la sauvegarde sont activés par défaut sur certains modules, il peuvent être activés/désactivés dans l'onglet `Services` de l'interface de configuration du module.



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.



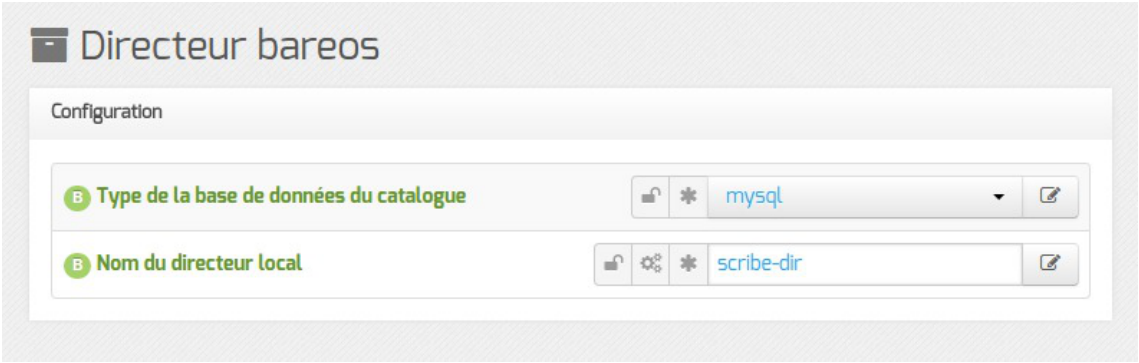
Si le support de stockage de la sauvegarde est activé (`Activer le support de stockage de la sauvegarde` à `oui`) un onglet `Stockage bareos` apparaît dans l'interface de configuration du module.

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



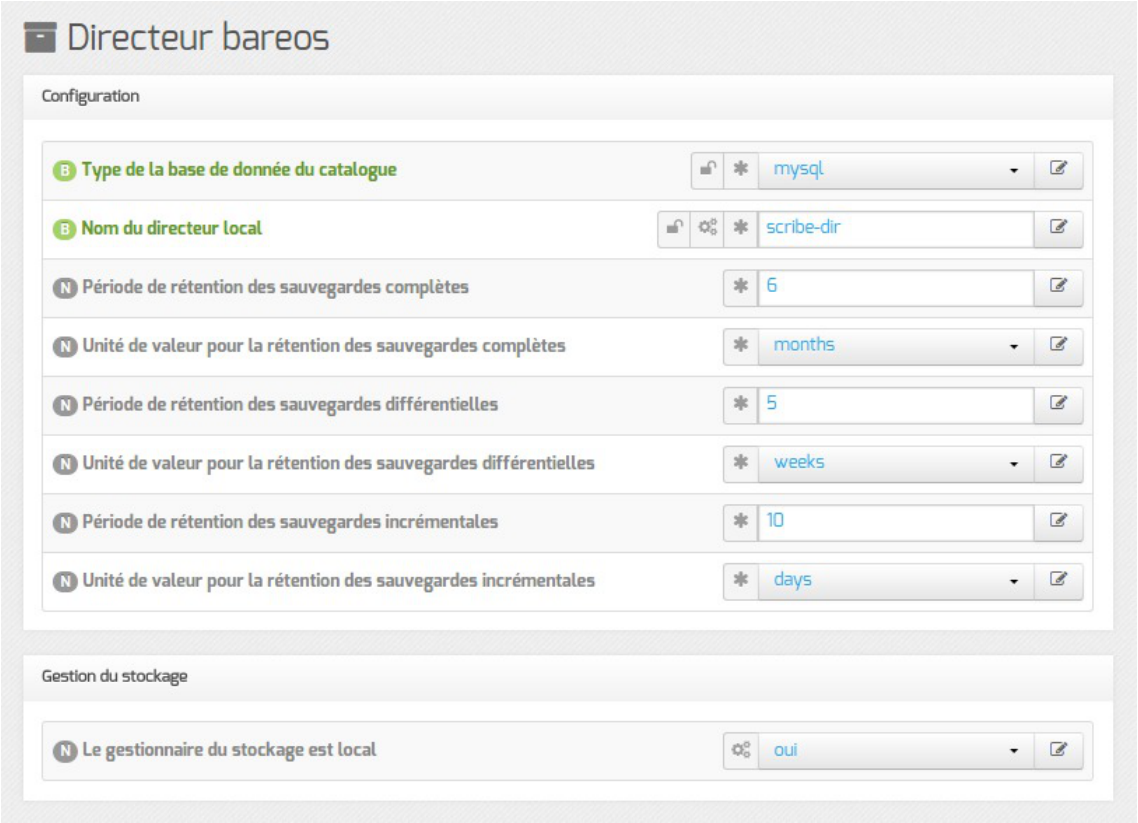
Le type de base de données permet de choisir si l'enregistrement du catalogue se fait dans MySQL ou dans SQLite. Il ne sera plus possible de modifier ce paramètre après l'enregistrement de la configuration.

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.888] 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.



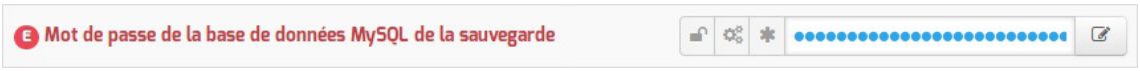
Certaines infrastructures nécessitent une dégradation des fonctionnalités des modules EOLE comme la désactivation des mises à jour automatiques pour que la sauvegarde distante fonctionne correctement.

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.

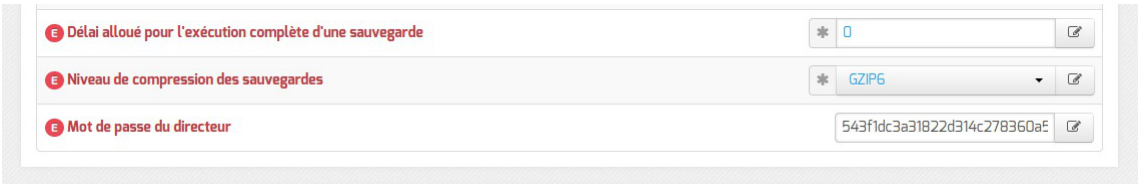
En mode expert, il est possible de définir manuellement le mot de passe de la base de donnée MySQL, le délai accordé à l'exécution de la sauvegarde ainsi que l'algorithme de compression utilisé pour le

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

stockage.



Vue de l'onglet Directeur Bareos



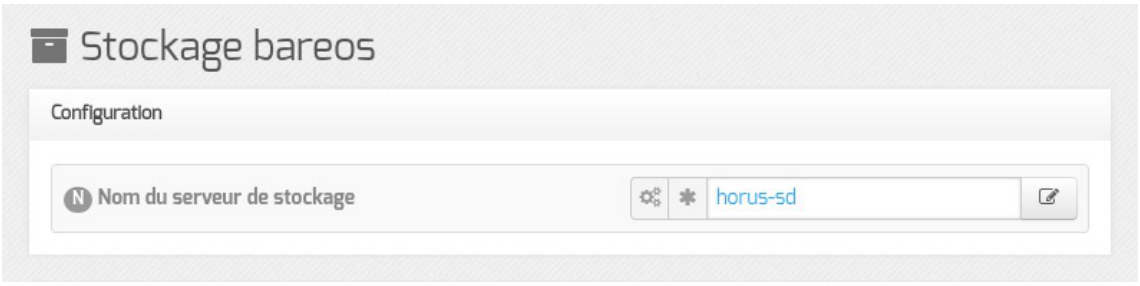
Type de compression et délai alloué

Le délai permet d'arrêter le job après un temps d'exécution fixé en seconde, par défaut le job n'a pas de 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.

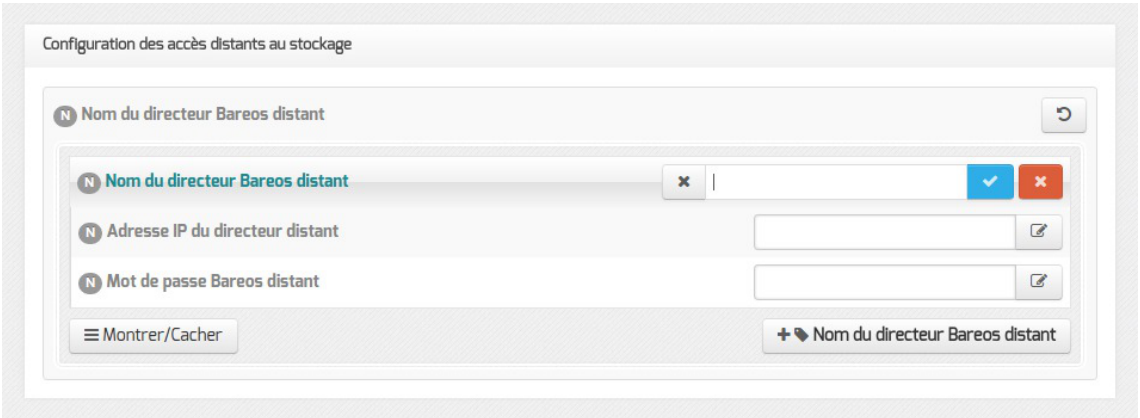
Dans l'onglet `Stockage bareos` il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



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)



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.619]

9. Configuration du module Eclair avec un module AmonEcole

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 AmonEcole permet :

- d'utiliser l'annuaire utilisateurs présent sur le module AmonEcole pour authentifier les utilisateurs sur le module Eclair ;
- d'utiliser les répertoires utilisateur présents sur le module AmonEcole (protocole NFS) ;
- d'utiliser le service DHCP du module AmonEcole.

Configuration du module AmonEcole

Exports NFS

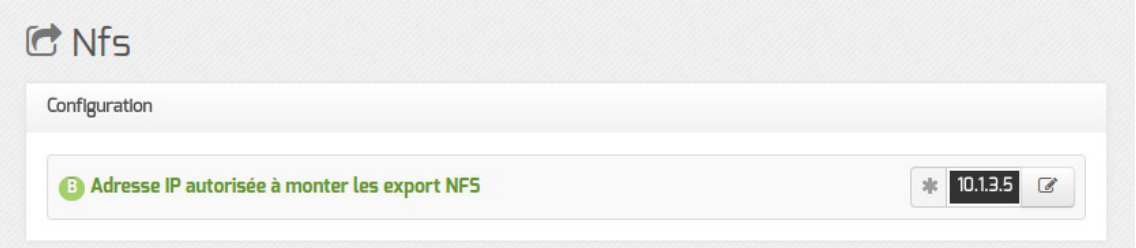
Installer le paquet eole-nfs :

```
# 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`.

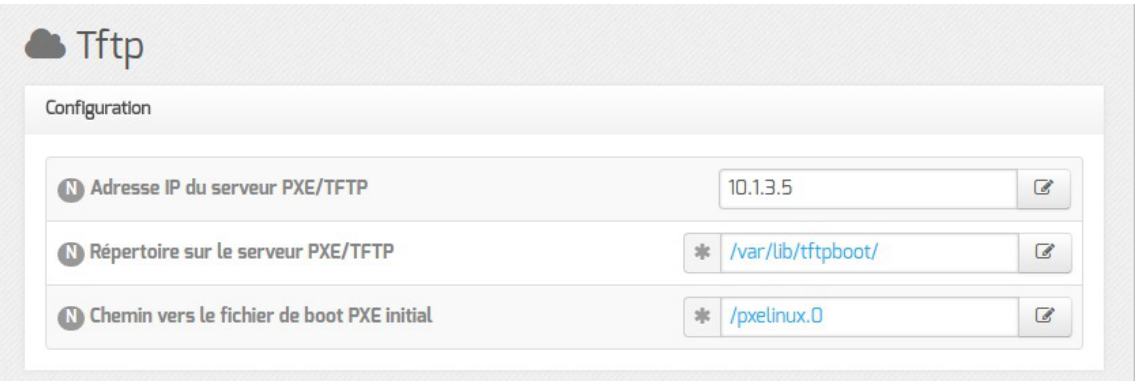
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Services DHCP et TFTP

Pré-requis : le module AmonEcole est déjà configuré en tant que DHCP.

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`.

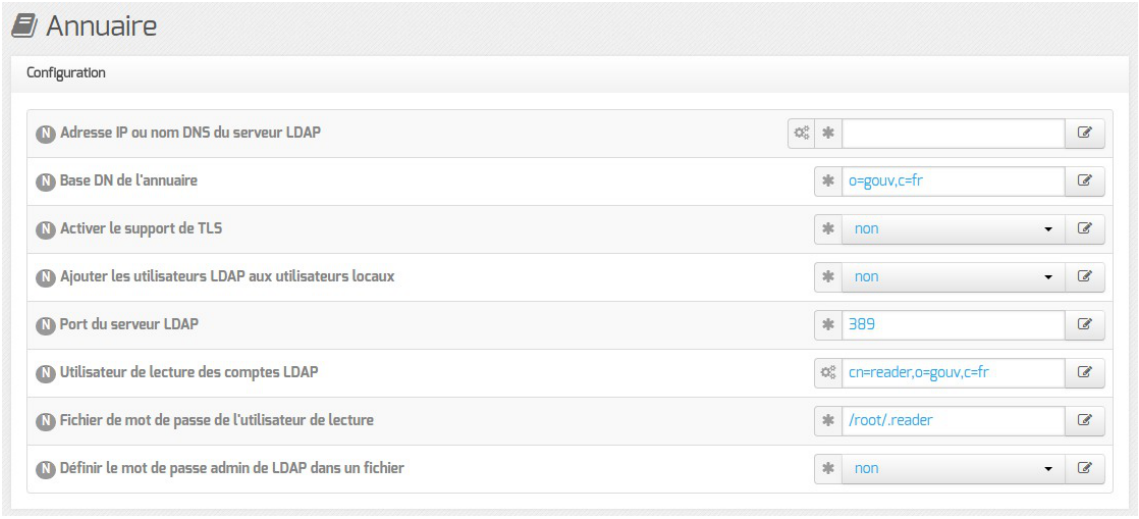


Si ce n'est pas déjà fait, pensez à attribuer un shell valide aux utilisateurs susceptibles d'utiliser les clients légers.

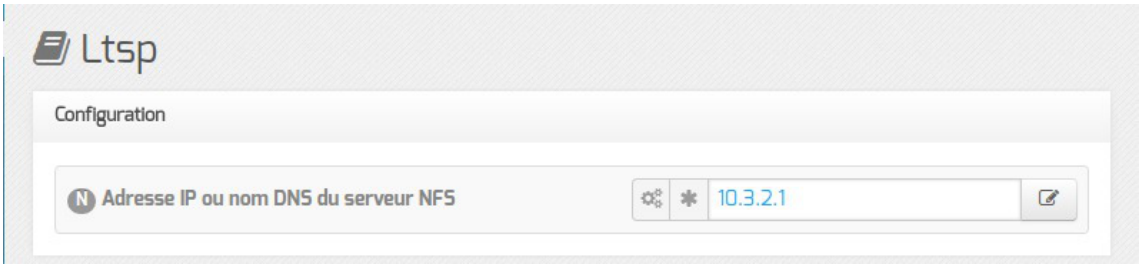
Configuration du module Eclair

Dans l'onglet `Annuaire`, renseigner l'adresse IP de l'interface 1 du serveur AmonEcole (`adresse_ip_eth1`) dans le champ : `Adresse IP ou nom DNS du serveur LDAP`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Dans l'onglet `Ltsp`, vérifier que le champ : `Adresse IP ou nom DNS du serveur NFS` contient bien l'adresse IP de l'interface 1 du serveur AmonEcole.



10. 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 ne gère que les bases de données MySQL.

Installation d'EoleDB

L'installation d'EoleDB se fait manuellement sur le serveur qui héberge l'application web avec la

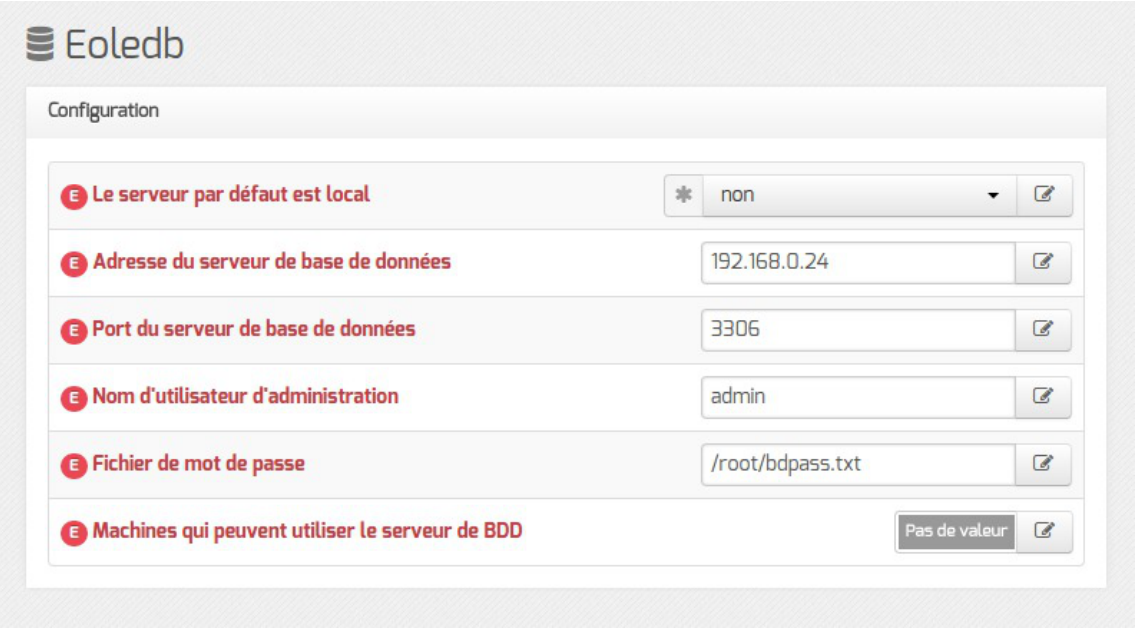
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

commande `apt-eole` :

```
# apt-eole install eole-db
```

Configuration d'EoleDB

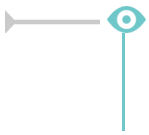
Par défaut le serveur est paramétré comme étant local. Dans le cas où le serveur est distant quelques variables sont à renseigner.



- `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.906], il définit le comportement par défaut d'EoleDB si aucune configuration spécifique n'est définie par l'application web.



```
1 dbhost: 192.168.0.24
2 dbport: 3306
3 dbroot: root
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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.906] qui surcharge le fichier de configuration principal d'EoleDB.

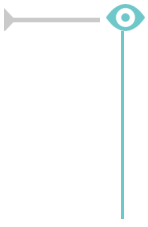
Ces fichiers de configuration spécifiques aux applications redéfinissent le comportement par défaut d'EoleDB, ils sont stockés dans `/etc/eole/eole-db.d/`.

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`) ;
- **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) ;
- **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"
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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:
- {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 '.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

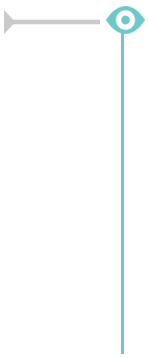
```
define('DBPASS': 'JeSuisUnMauvaisPassword');
pattern : "define('DBPASS': '"
end_pattern: ");",
```

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.



```
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' }
```

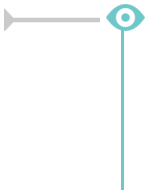


Si le comportement d'EoleDB est changé, celui-ci impactera l'application.

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**.

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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>`

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` :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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/`

```
<?xml version="1.0" encoding="utf-8"?>
<creole>
    <files>
        <service_access service='mysql'>
        <port>3306</port>
        <tcpwrapper>mysqld</tcpwrapper>
        </service_access>
    </files>
    <variables />
    <constraints />
    <help />
</creole>
<!-- 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>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 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
```

Voir aussi...

Les sauvegardes [p.590]

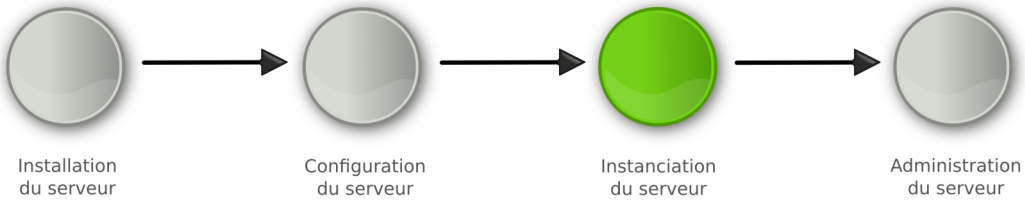
Les applications web sur le module Scribe

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 5

Instanciation du module

La troisième des quatre phases



Instanciation

Les généralités sur l'instanciation commune aux différents modules **ne sont pas traitées** dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module concerné.

- La **phase d'instanciation** s'effectue au moyen de la commande `instance` .

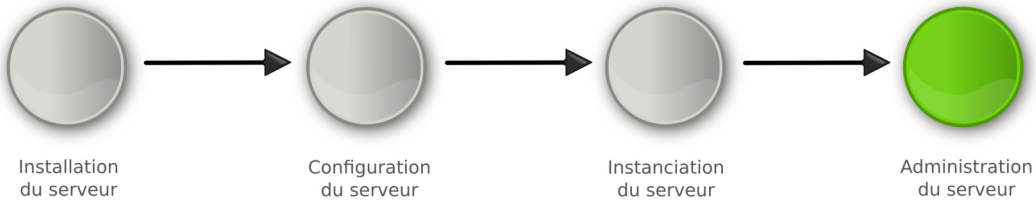
  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

  À l'issue de cette phase, le serveur est utilisable en exploitation.

  Cette phase doit être complétée par un diagnostique complet du module à l'aide de la commande `diagnose -L` .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 6
Administration du module AmonEcole



Administration

Les généralités sur l'administration et l'administration commune aux différents modules ne sont pas traités dans cette documentation, veuillez vous reporter à la documentation de mise en œuvre d'un module EOLE ou à la documentation complète du module.

- La **phase d'administration** correspond à l'exploitation du serveur.
  Chaque module possède des fonctionnalités propres, souvent complémentaires.
  Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

1. Les rôles sur le module AmonEcole

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 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

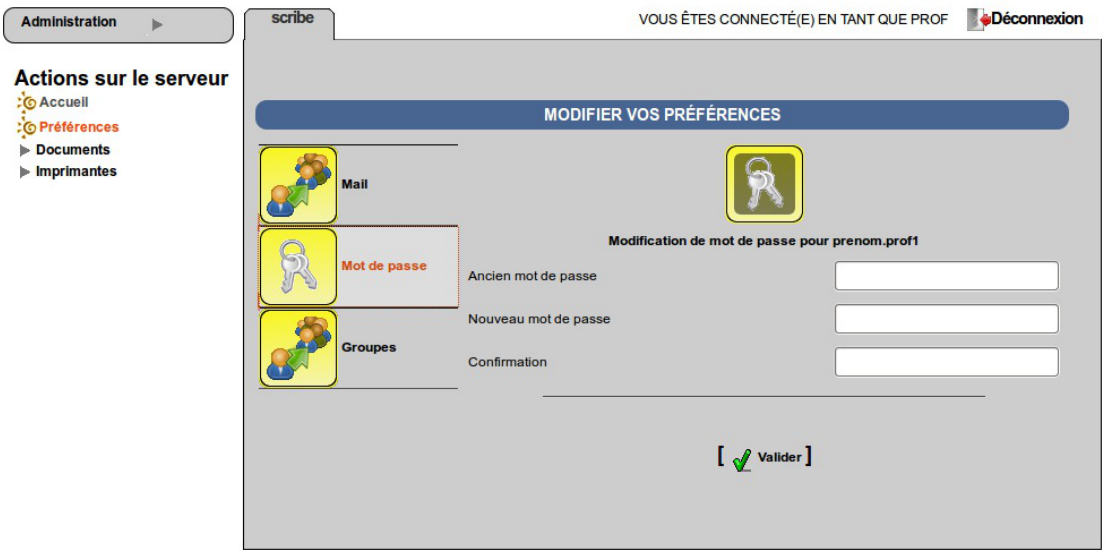
- configurer ses préférences personnelles ;
- distribuer des documents ;
- gérer les imprimantes.



l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

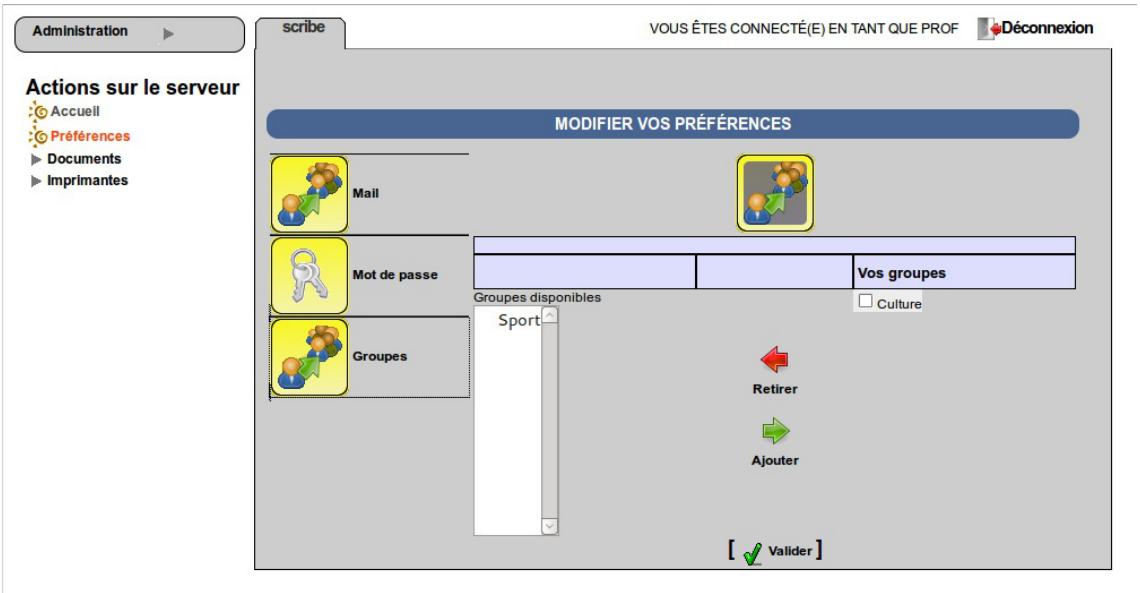
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

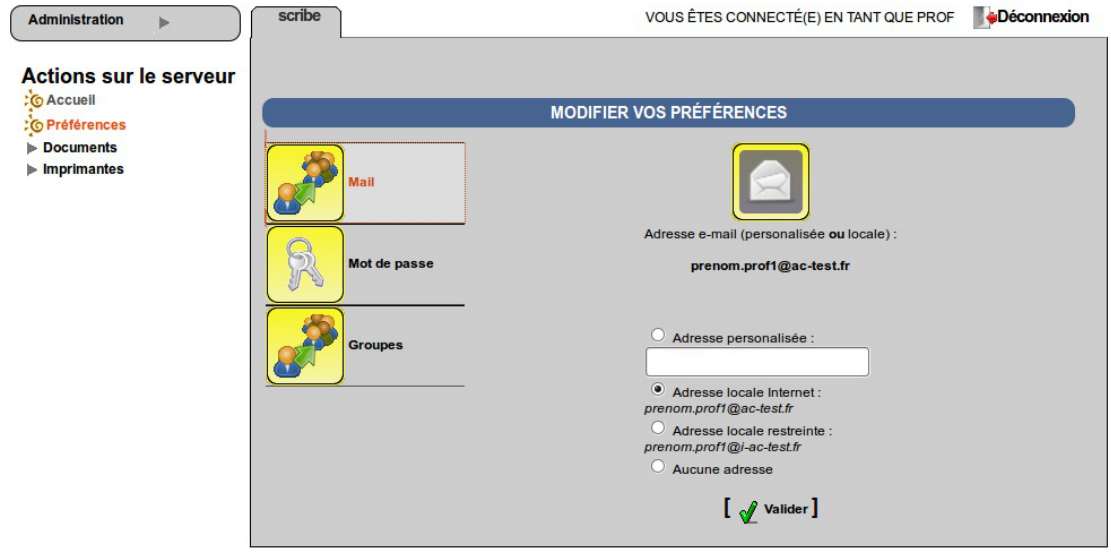
- s'inscrire/se désinscrire d'un groupe ;

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 "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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

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 "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) ;
- importation CSV/SIECLE/AAF/ONDES ;
- gestion des ACL ;
- gestion des quotas disque ;
- gestion des listes de diffusion ;
- test de la bande passante du serveur ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

2. Fonctionnalités de l'EAD propres au module AmonEcole

2.1. Les rôles sur le module AmonEcole

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

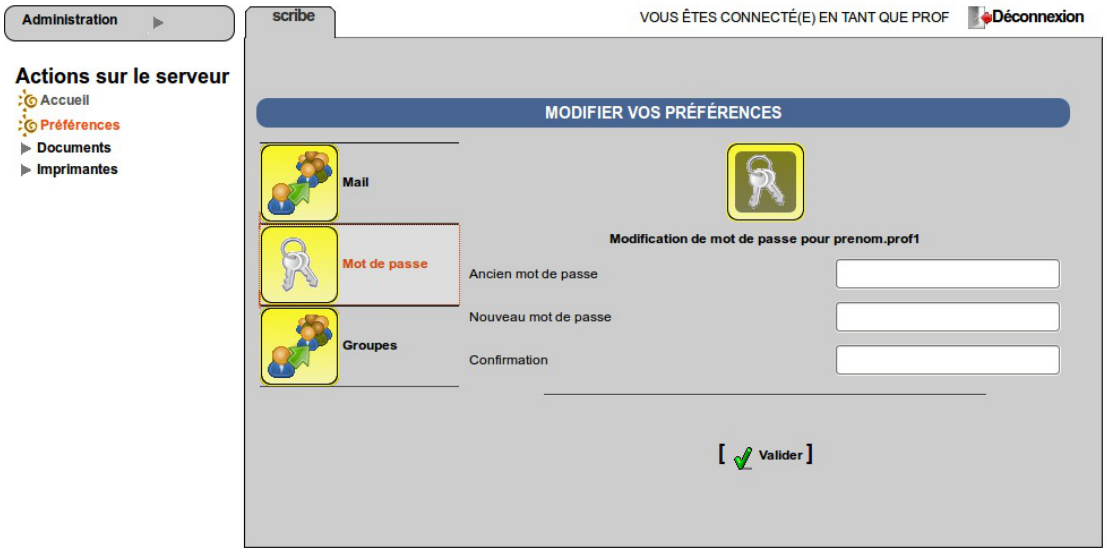


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

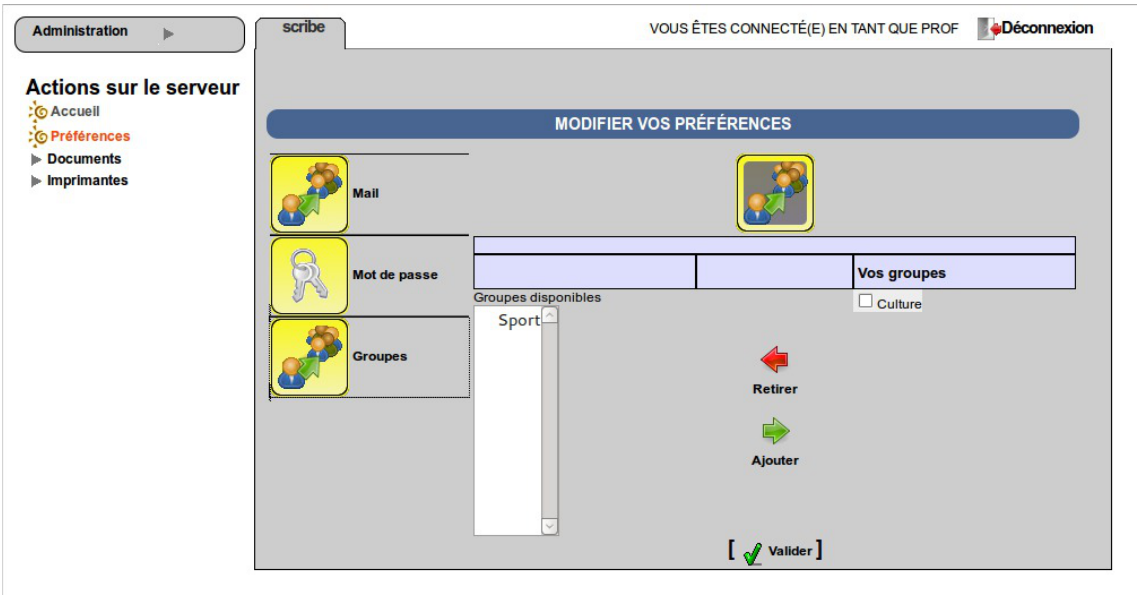
- modifier son mot de passe ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



EAD vue enseignant avec thème Envole, changement de mot de passe

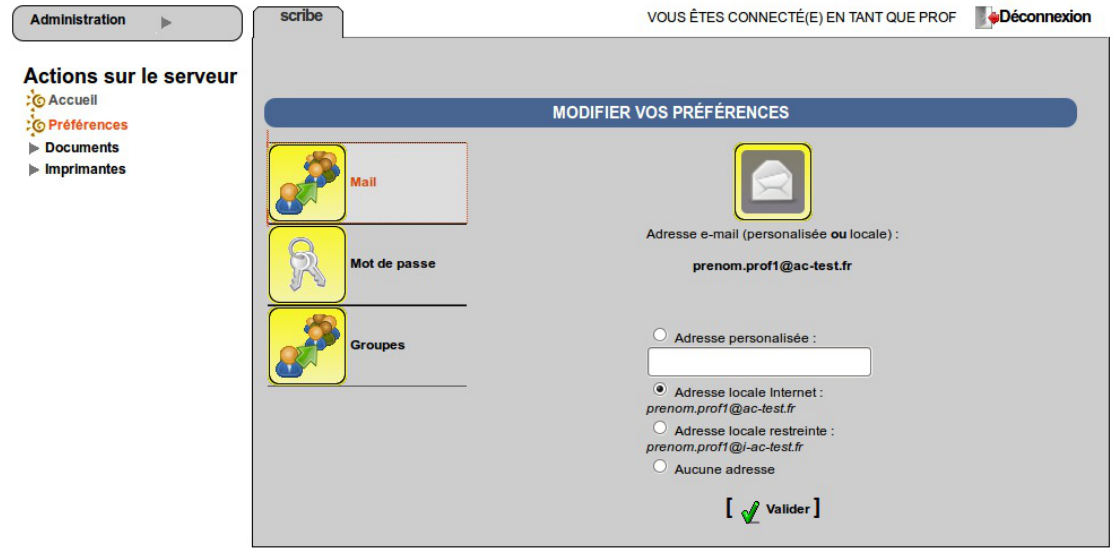
- s'inscrire/se désinscrire d'un groupe ;



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 "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) ;
- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

2.2. Groupes et utilisateurs

2.2.1. Groupes

Un groupe est un ensemble d'utilisateurs (professeurs, personnels administratif ou élèves) pouvant avoir accès à un partage, à des applications web et/ou à des listes de diffusion.

Types de groupe

Il existe six types de groupe :

- niveau, regroupe les élèves d'un niveau (Exemple : *3eme*) ;
- classe, regroupe les élèves d'une classe (un groupe de type équipe pédagogique *profs-<classe>* est automatiquement créé) ;
- option, regroupe les élèves d'une option (un groupe de type équipe pédagogique *profs-<option>* est automatiquement créé) ;
- matière, regroupe les professeurs d'une même matière (Exemple : *higeo*) ;
- service, regroupe les personnels administratifs d'un même service ;
- groupe de travail, permet de créer tout autre groupe thématique d'élèves et/ou de professeurs et/ou de personnels administratif .

Il existe un mode multi-établissement qui permet de n'avoir qu'un seul module Scribe pour gérer plusieurs établissements. Dans ce mode un type de groupe supplémentaire nommé Établissement existe et se gère comme un nouveau type de groupe.

Partages

Un partage est un espace disque accessible par plusieurs utilisateurs permettant de stocker des documents communs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En général, les enseignants et les personnels administratifs ont les droits de lecture/écriture sur tous les partages auxquels ils ont accès.

Pour les élèves, il existe trois modèles de partage :

- lecture seule ;
- lecture/écriture ;
- données/travail : c'est un partage (en lecture seule) avec un sous répertoires `donnees` (en lecture seule) et `travail` (en lecture/écriture).

Les droits peuvent ensuite être affinés grâce à la mise en place de droits appelés ACL[p.882].

Listes de publipostage

Une liste de publipostage est une méthode de diffusion de courrier électronique, dans laquelle les abonnés de la liste peuvent envoyer des messages qui seront diffusés à tous les membres.

Trois listes existent systématiquement sur le module :

- liste professeurs (ex. *professeurs@i-etabtest.ac-dijon.fr*)
- liste élèves (ex. *eleves@i-etabtest.ac-dijon.fr*)
- liste personnels administratif : *administratifs@i-etabtest.ac-dijon.fr*)

Lorsqu'une importation de comptes est effectuée, des listes de publipostage associées aux groupes sont créées :

- par classe (ex. *3e2@i-etabtest.ac-dijon.fr*)
- par niveau (ex. *3eme@i-etabtest.ac-dijon.fr*)
- par équipe pédagogique (ex. *profs-3e2@i-etabtest.ac-dijon.fr*)
- par option (ex. *3all1g1@i-etabtest.ac-dijon.fr*)
- par matière (ex. *histgeo@i-etabtest.ac-dijon.fr*)
- par service administratif (ex. *compta@i-etabtest.ac-dijon.fr*)
- par responsables des élèves d'une classe (ex. *resp-3e2@i-etabtest.ac-dijon.fr*)

Lors de la création d'une nouvelle liste, il y a deux possibilités :

- les listes restreintes ;
- les listes internet.

Il est possible d'envoyer des mail à la liste de publipostage depuis l'extérieur dans le cas de la liste Internet mais pas dans le cas de la liste restreinte.



Cette restriction doit être configurée sur le relai mail académique.

Il n'y a pas de lien entre le domaine restreint et les listes restreintes. Le choix du type des adresses mail n'influence en rien le type des listes.

Des listes statiques peuvent être créées à partir de l'interface web de Sympa indépendamment de celles

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

générées automatiquement.

Dans l'EAD, les listes associées aux groupes sont des listes dynamiques.

Pour personnaliser les listes dynamiques, il est également nécessaire de passer par l'interface web de Sympa.

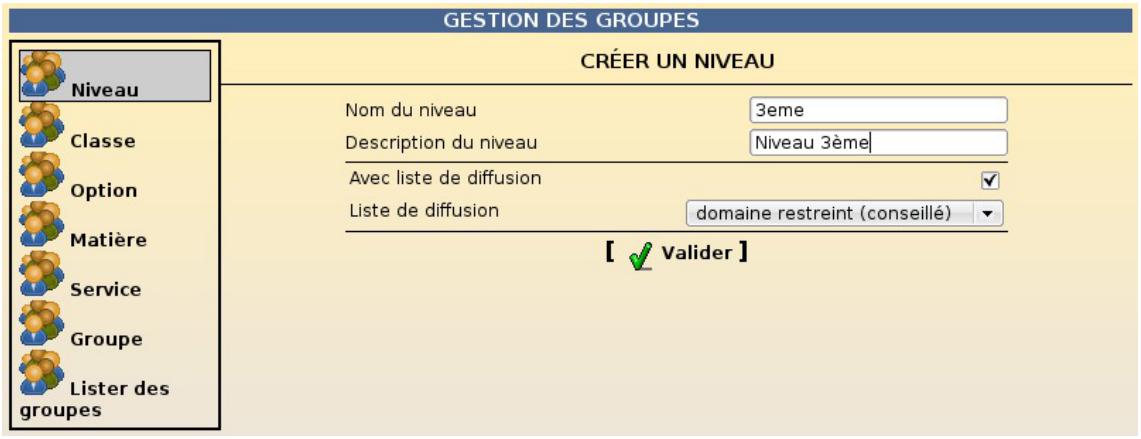
2.2.1.a. Création de groupes

Pour créer un groupe de type *niveau*, *classe, option*, *matière, service* ou un *groupe de travail*, il suffit d'aller dans le menu `Gestion/Groupes/Création de groupe` de l'EAD et de choisir le type désiré.

Création d'un niveau

Pour créer un *niveau*, il faut choisir son nom, son libellé (facultatif) et si on lui associe une liste de publipostage.

Puis cliquer sur `valider` .



Création d'un niveau dans l'EAD

Lors de l'importation, les niveaux sont créés avec une liste de publipostage sur le domaine restreint.

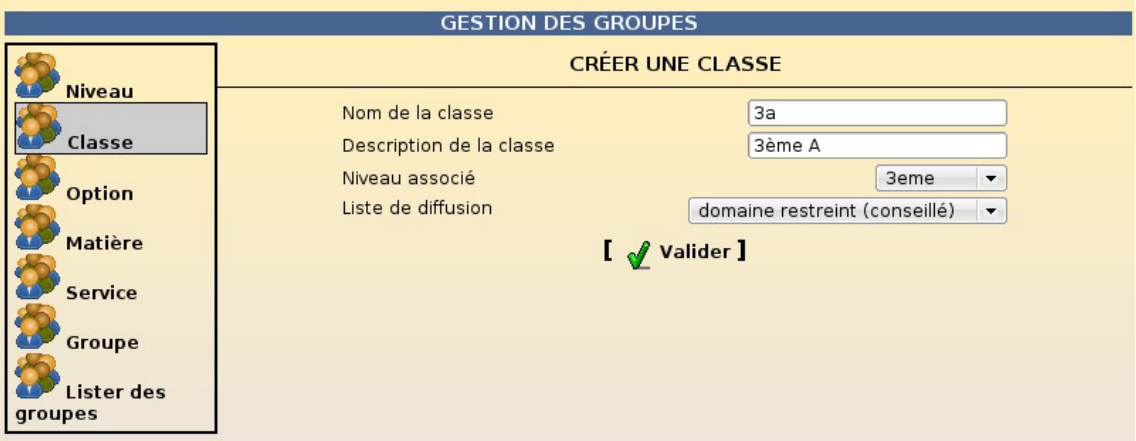
En mode multi-établissement, il faut également choisir l'établissement auquel le niveau doit être rattaché.

Création d'une classe

Pour créer une *classe*, il faut choisir son nom, son libellé (facultatif), le niveau associé et son type de liste de publipostage.

Puis cliquer sur `valider` .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Création d'une classe dans l'EAD

Les groupes de type *classe* sont créés obligatoirement avec un partage de type `données/travail` et une liste de publipostage dont on doit choisir le type.

Les classes sont obligatoirement associés à un niveau.

La création d'une classe crée automatiquement un groupe de type équipe pédagogique *profs-<classe>*.

> À la création d'une classe, le groupe équipe pédagogique associé, son partage et les listes de publipostage (classe, équipe pédagogique et responsables légaux de la classe) sont créés automatiquement.
>
> Un professeur est associé à une ou plusieurs équipes pédagogiques alors qu'un élève ne pourra être associé qu'à une classe.
>
> En mode multi-établissement, la classe est automatiquement associée à l'établissement auquel est rattaché son niveau.

Liste de publipostage

À la création d'une classe, les listes de publipostage lié à la classe sont créés automatiquement :

- une liste pour la classe (xxxx@) ;
- une liste pour les profs (prof-xxxx@) ;
- une liste pour les responsables (resp-xxxx@).

Il est possible de choisir entre deux options :

- `domaine restreint (conseillé)` qui va créer :
  - une liste en domaine restreint pour la classe (xxxx@i-domaine) ;
  - une liste en domaine restreint pour les profs (prof-xxxx@i-domaine) ;
  - une liste en domaine restreint pour les responsables (resp-xxxx@i-domaine) qui aura le même domaine que la liste de classe (contrairement à celle des profs).
- `internet` qui va créer :
  - une liste internet pour la classe (xxxx@domaine) ;
  - une liste **en domaine restreint** pour les profs (prof-xxxx@i-domaine) ;
  - une liste internet pour les responsables (resp-xxxx@domaine).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le partage de l'équipe pédagogique

Un partage "équipe pédagogique" contient les deux éléments suivants :

- le sous-répertoire "classe" : correspond au partage *classe* accessible par les élèves ;
- le sous-répertoire "eleves" : permet d'accéder à l'espace personnel de chaque élève de la classe, afin éventuellement de contrôler son travail. Le sous-répertoire "prive" n'est pas accessible aux professeurs. Il permet de garantir à l'élève un espace réellement personnel.

Les données spécifiques à l'équipe pédagogique doivent être placées à la racine du partage, mais il est tout à fait possible d'y créer un sous-répertoire, nommé par exemple "equipe", afin d'éviter toute confusion.



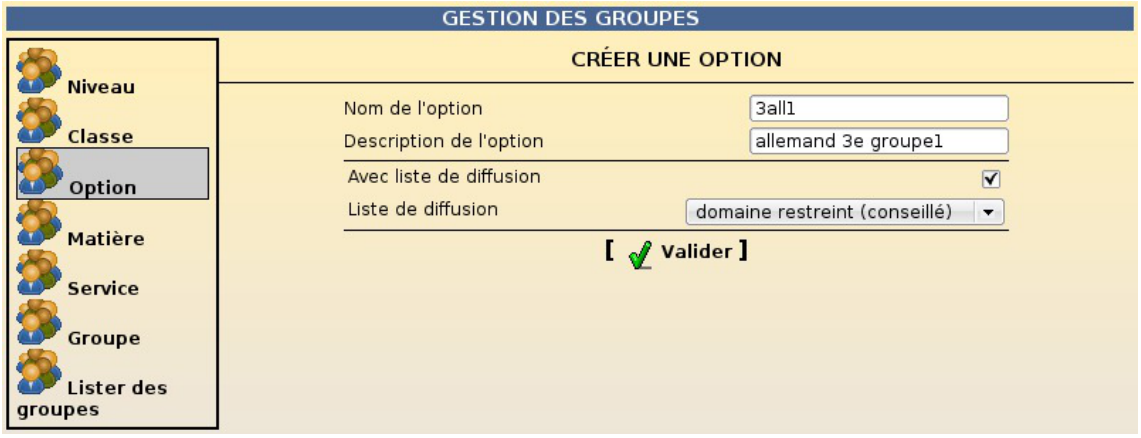
Partage d'une équipe pédagogique

Création d'une option

Une option correspond à un sous-groupe d'élève suivant généralement un ou plusieurs cours ensemble.

Pour créer une *option*, il faut choisir son nom, son libellé (facultatif) et si on lui associe une liste de publipostage.

Puis cliquer sur valider .



Création d'une option dans l'EAD

La création d'une option crée automatiquement un groupe de type équipe pédagogique *profs-<option>*.

Les groupes de type *option* sont créés obligatoirement avec un partage de type données/travail.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Lors d'une importation, les options correspondent à la notion de *Groupe* dans SIECLE.
>
> En mode multi-établissement, il faut également choisir l'établissement auquel l'option doit être rattachée.

A la création d'une option, l'équipe pédagogique associée est créée automatiquement.

Un élève peut être associé à plusieurs options.

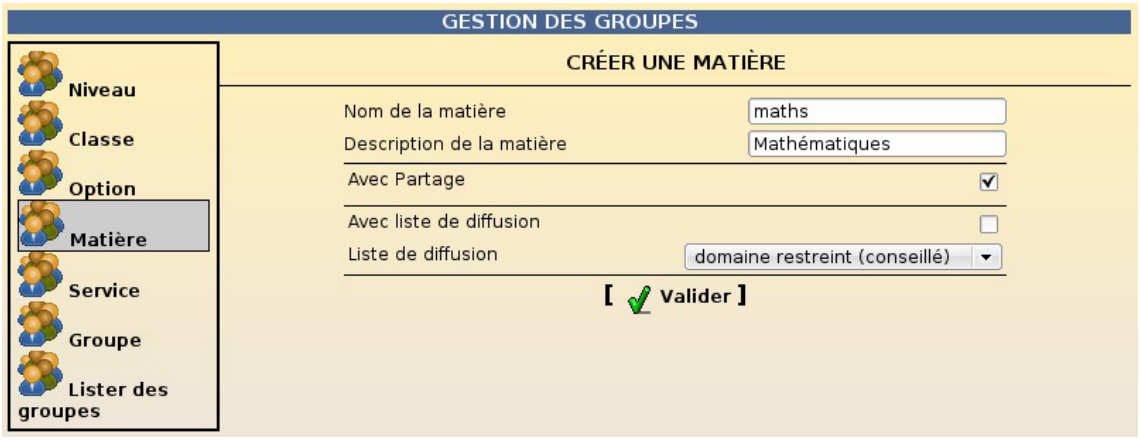
La liste de publipostage de l'équipe pédagogique n'est pas créée automatiquement mais elle peut être ajoutée ultérieurement.

Le partage "équipe pédagogique" d'une option fonctionne de la même manière que celui d'une classe.

Création d'un matière

Pour créer une *matière*, il faut choisir son nom, son libellé (facultatif) et si on lui associe un partage et/ou une liste de publipostage.

Puis cliquer sur `valider` .



Création d'une matière dans l'EAD

Lors de l'importation, les matières sont créées avec un partage en lecture/écriture pour ses membres et une liste de publipostage sur le domaine restreint.

Un professeur a accès aux partages des matières qu'il enseigne.

A sa création, le partage est vide. Les professeurs peuvent donc l'organiser à leur guise.

> En mode multi-établissement, il faut également choisir l'établissement auquel la matière doit être rattachée.

Création d'un service administratif

Pour créer une *service administratif*, il faut choisir son nom, son libellé (facultatif) et si on lui associe un partage et/ou une liste de publipostage.

Puis cliquer sur `valider` .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Création d'un service administratif dans l'EAD

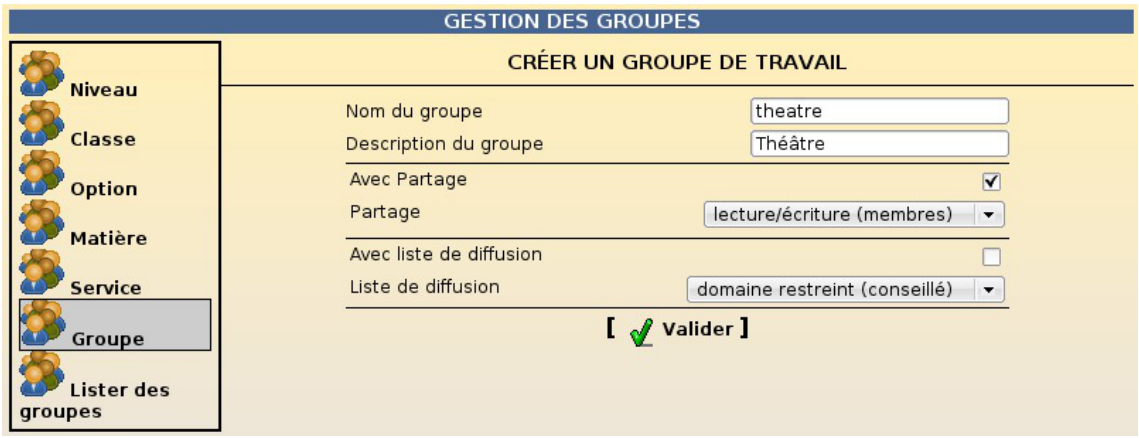
Lors de l'importation, les services administratifs sont créés avec un partage en lecture/écriture pour ses membres et une liste de publipostage sur le domaine restreint.

En mode multi-établissement, il faut également choisir l'établissement auquel le service doit être rattaché.

Création d'un groupe de travail

Pour créer un *groupe de travail*, il faut choisir son nom, son libellé (facultatif) et si on lui associe un partage et/ou une liste de publipostage.

Puis cliquer sur `valider` .



Création d'un groupe de travail dans l'EAD

En mode multi-établissement, il faut également choisir l'établissement auquel le groupe de travail doit être rattaché.

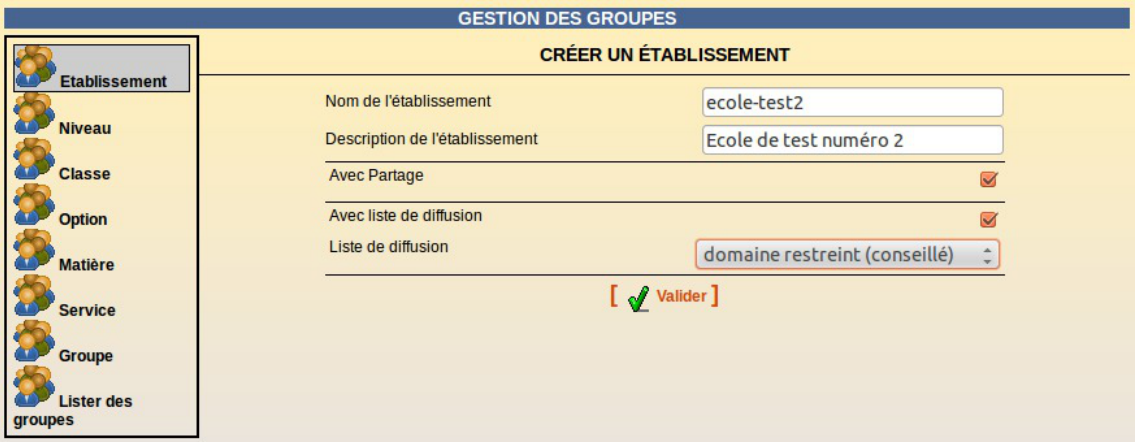
Création d'un établissement

En mode multi-établissement, les nouveaux établissements doivent être déclarés dans l'EAD.

Pour créer un *établissement*, il faut choisir son nom, son libellé (facultatif) et si on lui associe un partage et/ou une liste de publipostage.

Puis cliquer sur `valider` .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Création d'un établissement dans l'EAD

Il n'est pas possible de renommer un groupe.

2.2.1.b. Peuplement des groupes

Ajouter un utilisateur à un groupe

La gestion des groupes d'un utilisateur est disponible dans la fiche utilisateur.

Celle-ci apparaît lorsque l'on édite l'utilisateur via les menus Gestion / Utilisateurs / Recherche d'utilisateur puis cliquer sur Éditer.

La fiche utilisateur peut aussi être atteinte en passant par la recherche de groupes même si le cheminement est plus long : Gestion / Groupes / Recherche de groupe / Lister des groupes, choisir le type de groupe (niveau, matière, groupe…). Dans la liste de groupe affichée, cliquez sur Membres pour afficher les utilisateurs appartenant au groupe sélectionné puis cliquez sur Éditer.

L'ajout de l'utilisateur à un ou à plusieurs groupes se fait dans la partie *Groupes* de la fiche utilisateur. L'ajout est effectif après avoir cliqué sur Valider .

Il n'est pas possible de supprimer un élève de sa classe mais il est possible de changer un élève de classe.

Cette manipulation se fait par la liste déroulante *Classe*, il faut choisir une autre classe et cliquer sur Valider.

Inscription groupée

L'inscription simultanée d'utilisateurs à un groupe de travail ou à une option se fait par le menu Gestion/Edition groupée.

Il faut rechercher les utilisateurs suivant différents critères.

Ensuite, il faut cliquer sur le bouton Inscrire ces utilisateurs à d'autres groupes, choisir le groupe et Valider.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'inscription groupée

Seuls les élèves sont concernés par l'inscription à un groupe *option*.

2.2.1.c. Suppression de groupes et d'appartenance à un groupe

Supprimer l'appartenance d'un utilisateur à un groupe

La gestion des groupes d'un utilisateur est disponible dans la fiche utilisateur.

Celle-ci apparaît lorsque l'on édite l'utilisateur via les menus Gestion / Utilisateurs / Recherche d'utilisateur puis cliquer sur Éditer.

La fiche utilisateur peut aussi être atteinte en passant par la recherche de groupes même si le cheminement est plus long : Gestion / Groupes / Recherche de groupe / Lister des groupes , choisir le type de groupe (niveau, matière, groupe…). Dans la liste de groupe affichée, cliquez sur Membres pour afficher les utilisateurs appartenant au groupe sélectionné puis cliquez sur Éditer.

La suppression de l'utilisateur d'un ou de plusieurs groupes se fait dans la partie *Groupes* de la fiche utilisateur. La suppression n'est effectif qu'après avoir cliqué sur Valider .

Il n'est pas possible de supprimer un élève de sa classe mais il est possible de changer un élève de classe.

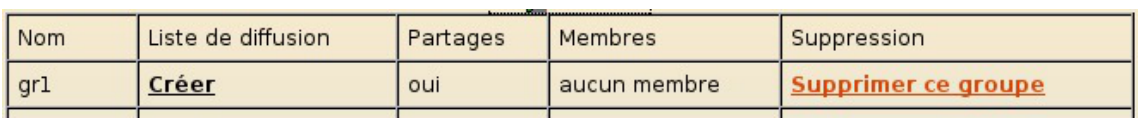
Cette manipulation se fait par la liste déroulante *Classe*, il faut choisir une autre classe et cliquer sur Valider.

Suppression de groupes

Pour supprimer un groupe, il faut auparavant le sélectionner via le menu Gestion / Groupes / Recherche de groupe / Lister les groupes .

Il est possible de choisir le type de groupe (niveau, matière, *groupe*…) et/ou éventuellement d'autres critères (partie du nom, vide ou non) afin de limiter le nombre de résultats affichés.

Une fois que le groupe souhaité apparaît dans la liste des groupes affichés, il faut cliquer sur le lien Supprimer ce groupe qui lui est associé.



Lien vers la suppression d'un groupe

La suppression devra ensuite être confirmée en cliquant sur Valider .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ecran de confirmation pour la suppression d'un groupe

La suppression des répertoires associés est pré-cochée.

Si vous choisissez de conserver les répertoires, les partages seront déplacés dans `/home/recyclage/<année>/workgroups`

Une classe pourra être supprimée uniquement si elle ne contient plus d'élèves.

Un niveau pourra être supprimé uniquement si plus aucune classe ne lui est associée.

La suppression d'une classe ou d'une option entraîne la suppression de l'équipe pédagogique associée.

Un groupe de type *groupe* peut être supprimé même si des utilisateurs lui sont encore associés.

Le dossier `/home/recyclage/` peut grossir assez vite.

2.2.1.d. Groupes spéciaux

Présentation

DomainAdmins

Les membres du groupe *DomainAdmins* sont des utilisateurs privilégiés sur le domaine.

Ils ont :

- les droits d'administrateurs locaux des postes clients ;
- la possibilité de joindre les postes Windows au domaine ;
- un accès à l'ensemble des partages.

Il est fortement **déconseillé** d'inscrire l'ensemble des professeurs au groupe *DomainAdmins* .

Cela leur donnera un accès en lecture et en écriture sur tous les partages, y compris sur les répertoires personnels de tous les utilisateurs (*admin* inclus).

PrintOperators

Les membres du groupe *PrintOperators* sont des administrateurs pour les imprimantes.

Ils peuvent :

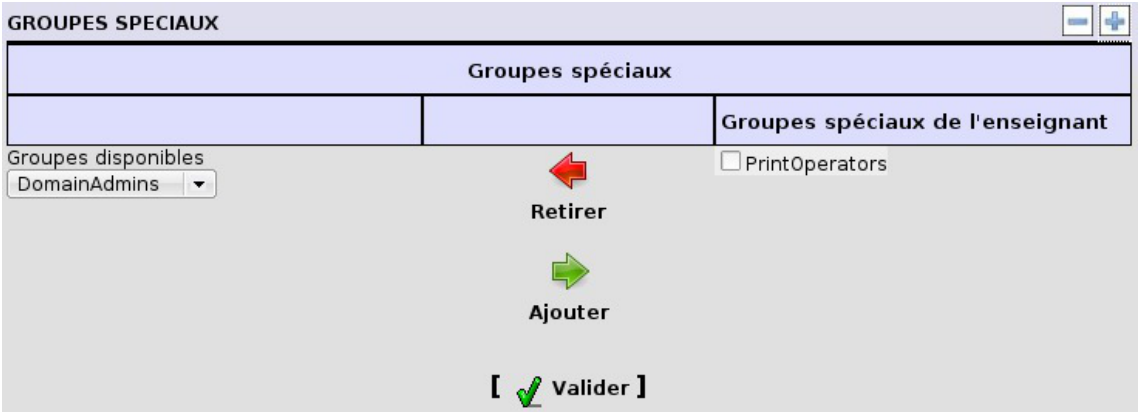
- installer les pilotes d'impression sur le serveur Samba ;
- installer et configurer les imprimantes dans CUPS.

Ajouter/supprimer un utilisateur à un groupe spécial

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Seuls les professeurs et les personnels administratifs peuvent être ajoutés aux groupes spéciaux.

Il est possible de les ajouter ou de les supprimer à la création ou à la modification de l'utilisateur.



Gestion des groupes spéciaux d'un utilisateur

Voir aussi...

Configuration du mode multi-établissement [p.252]

Administration des listes de diffusion [p.548]

2.2.2. Utilisateurs

Il existe cinq types d'utilisateurs : les élèves, les professeurs, les personnels administratifs, les responsables légaux et les invités.

Pour chaque type, les informations demandées et les options disponibles sont différentes.

On peut regrouper les utilisateurs en deux catégories principales : les utilisateurs locaux et les utilisateurs externes.

Utilisateurs locaux

Les utilisateurs locaux sont ceux ayant accès au domaine local (partage de fichiers) ce sont :

- les élèves ;
- les professeurs ;
- les personnels administratifs.

Pour les utilisateurs locaux, il est possible de définir des quotas disque représentants la taille maximale de données que l'utilisateur peut créer sur le système de fichiers.

Utilisateurs externes

Les utilisateurs externes sont ceux dont le compte ne donne accès qu'au portail et à une sélection d'applications web.

Ce sont :

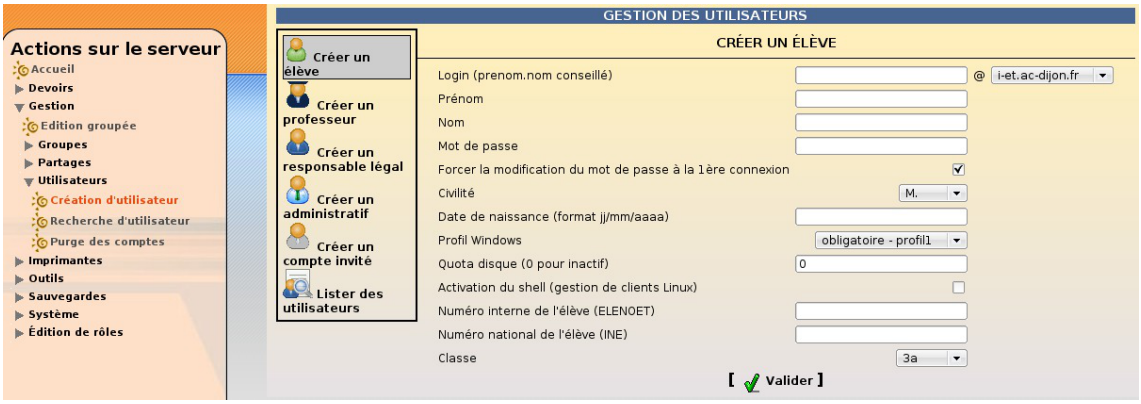
- les responsables légaux ;
- les titulaires de comptes "invités".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.2.2.a. Création de comptes utilisateurs

Création d'un compte élève

Avant de pouvoir créer un élève il est indispensable qu'au moins un niveau et une classe aient été préalablement créés.



Création d'un compte élève dans l'EAD

Depuis le remplacement de BE1D par ONDE, l'INE[p.891] est disponible dans les fichiers exportés ce qui permet de retrouver les élèves plus facilement.

Depuis la version `AAF-VE1803`, l'INE[p.891] est présent dans les fichiers exportés depuis AAF. Il est pris en compte par la procédure d'importation à partir de la version 2.5.2 d'EOLE.

Domaine mail restreint et domaine mail Internet

Il est possible de choisir entre deux domaines de messagerie pour les élèves :

- une adresse dans le `domaine restreint` : n'autorise l'envoi et la réception de courrier que depuis et vers une adresse située dans le même domaine académique que le domaine de la messagerie Scribe (voir `Nom de domaine de la messagerie de l'établissement` dans l'interface de configuration du module).

  Par exemple si votre domaine de messagerie Scribe est *etab.ac-acad.fr*, les utilisateurs ayant un compte mail dans le `domaine restreint` ne pourront envoyer ou recevoir que du courrier à destination ou en provenance d'adresses mail se terminant par *ac-acad.fr* (élèves et enseignant d'un même établissement ou de la même académie) ;
- une adresse dans le `domaine Internet` : autorise l'envoi et la réception de courrier depuis et vers n'importe quelle adresse.

Mode multi-établissement

Il existe un mode multi-établissement qui permet de n'avoir qu'un seul module Scribe pour gérer plusieurs établissements. Dans ce mode l'élève est automatiquement rattaché à l'établissement associé à sa classe.

Création d'un compte professeur

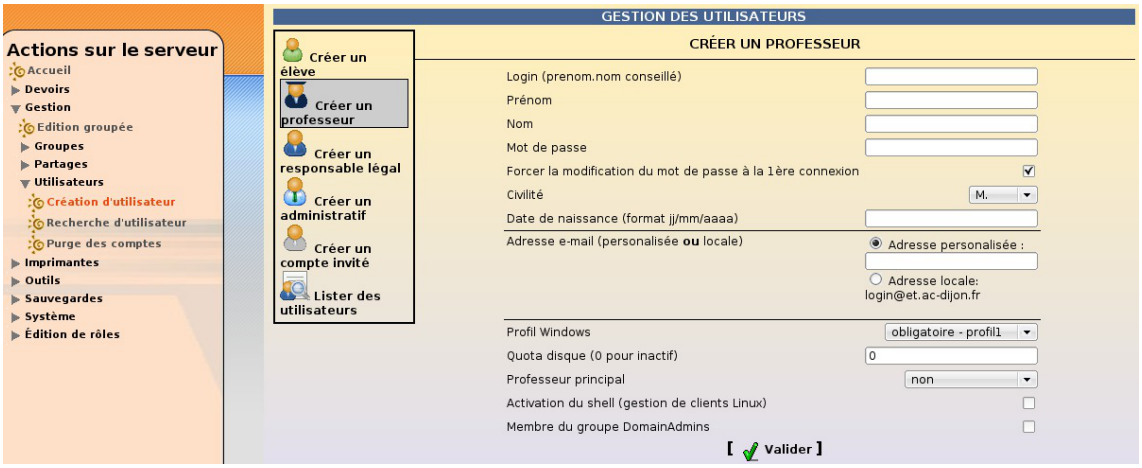
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Un professeur peut utiliser son adresse mail académique afin de communiquer avec les utilisateurs Scribe.

Cette adresse sera aussi utilisée dans les listes de diffusion auto-générées (équipe pédagogique, matière, niveau, etc.).

Le professeur peut se connecter à l'EAD avec son propre login pour modifier ses préférences.

Il peut notamment modifier son adresse mail.

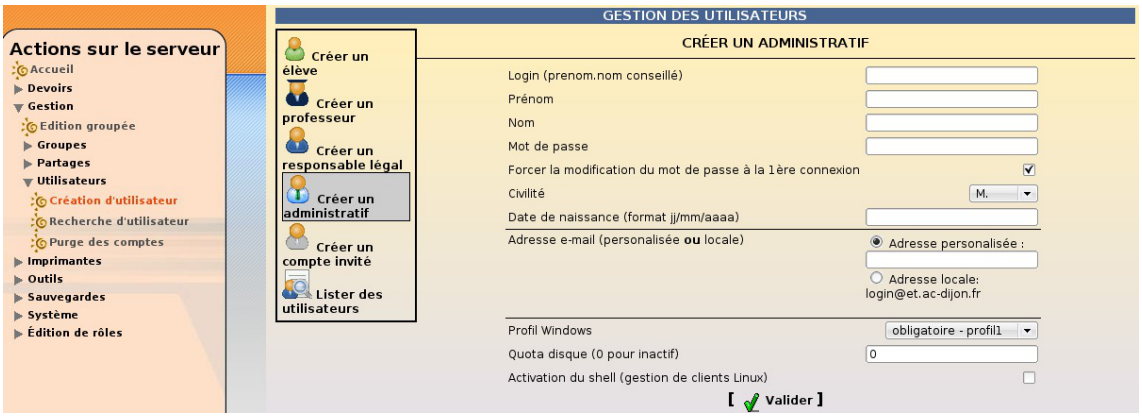


Création d'un compte enseignant dans l'EAD

En mode multi-établissement, il faut également choisir l'établissement associé à l'utilisateur.

Création d'un compte personnel administratif

Tout comme les professeurs, les personnels administratifs peuvent soit renseigner une adresse mail externe, soit choisir une boite mail locale.



Création d'un compte personnel administratif dans l'EAD

En mode multi-établissement, il faut également choisir l'établissement associé à l'utilisateur.

Création d'un compte responsable légal

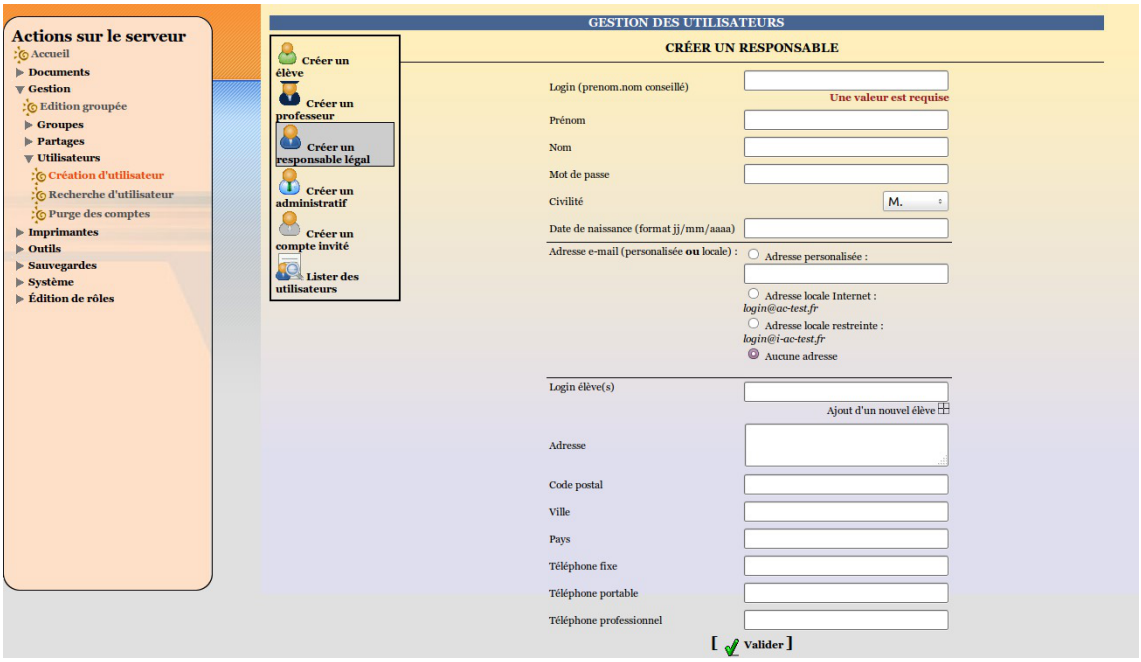
La création d'un compte responsable légal nécessite de connaître l'identifiant (login) d'au moins un des élèves dont il a la responsabilité.

création : Mai 2015 Version : révision : Avril 2018
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les responsables légaux peuvent obtenir une adresse mail locale s'ils en font la demande.

Le remplissage des renseignements personnels permettra par la suite de fournir ces informations à d'autres applications (logiciel de suivi scolaire...).

Le champ `Adresse` est multi-lignes à partir de la version 2.5.2 du module.

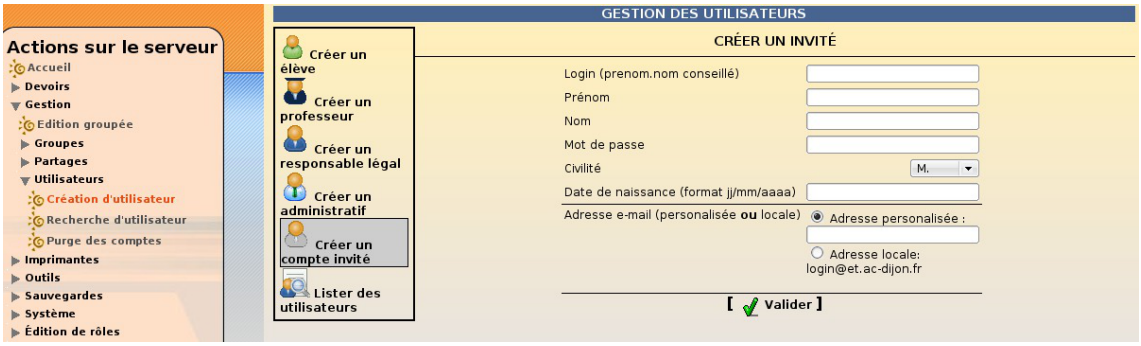


Création d'un compte responsable légal dans l'EAD

> En mode multi-établissement, les responsables légaux peuvent être associés à des élèves appartenant aux différents établissements déclarés.

Création d'un compte invité

Les comptes invités permettent d'offrir un accès à certaines applications et éventuellement une boite aux lettres à des personnes extérieures à l'établissement.



Création d'un compte invité dans l'EAD

> En mode multi-établissement, les comptes invités sont obligatoirement rattachés à l'établissement principal.

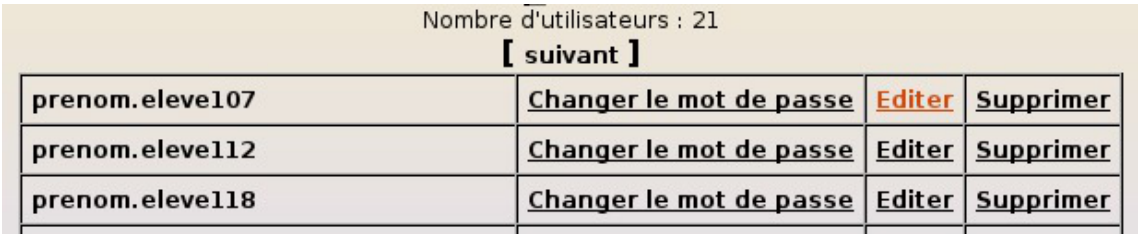
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.2.2.b. Gestion des comptes utilisateurs

Pour sélectionner un compte utilisateur, il faut auparavant le sélectionner *via* le menu `Gestion/Utilisateurs/Recherche d'utilisateur` de l'EAD.

Il faut choisir judicieusement les critères de recherche afin de limiter le nombre de résultats affichés et cliquer sur `Lister` .

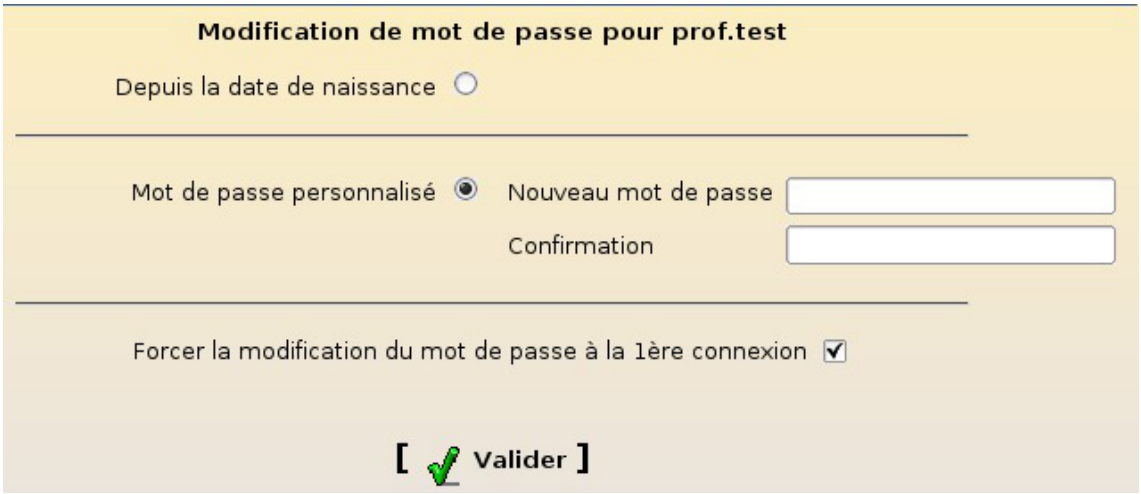
Les utilisateurs apparaissent alors



Résultat d'une recherche d'utilisateurs

Modification du mot de passe d'un utilisateur

Pour accéder au formulaire de modification de mot de passe, il faut cliquer sur le lien *Changer le mot de passe* associé à l'utilisateur affiché dans la liste.



Le formulaire de modification de mot de passe

Édition d'un compte utilisateur

Pour accéder à la fenêtre d'édition d'un utilisateur, il faut cliquer sur le lien *Editer* associé à l'utilisateur affiché dans la liste.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Edition d'un compte personnel administratif

Suppression d'un compte utilisateur

Pour supprimer un compte utilisateur, il faut cliquer sur le lien *Supprimer* associé à l'utilisateur affiché dans la liste.

La suppression devra ensuite être confirmée.



Ecran de confirmation pour la suppression d'un utilisateur

Si la case associée à la suppression des données de l'utilisateur est décochée :

- ses données (`perso`) seront déplacés dans `/home/recyclage/<année>/<lettre>/<login>`;
- ses messages électroniques (`mailDir`) seront déplacés dans `/home/recyclage/<année>/<mail>/<login>`.

Sinon elles seront supprimées définitivement.

Si tous les élèves d'un responsable ont été supprimés, celui-ci doit l'être également.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

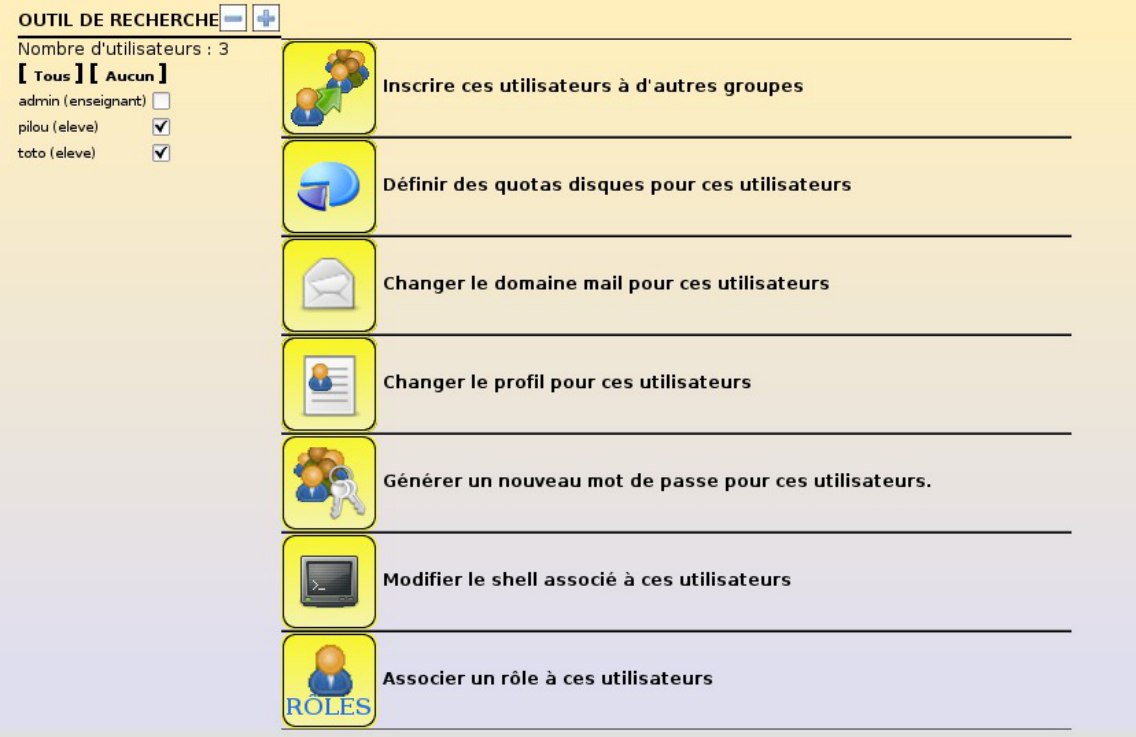
> Le dossier `/home/recyclage/` peut grossir assez vite.

L'édition groupée

L'édition groupée, disponible par le menu `Gestion/Edition groupée` de l'EAD permet d'effectuer des modifications sur des sélections d'utilisateurs.

Un outil de recherche (semblable à celui de l'outil `Recherche d'utilisateur`) permet de réaliser une présélection des utilisateurs à modifier

La sélection peut ensuite être affinée par l'utilisation des cases à cocher et des boutons *Tous* et *Aucun*.



Actions disponibles dans l'édition groupée

Les opérations disponibles sont les suivantes :

- inscription des utilisateurs à une option (élèves uniquement) ou à un groupe de travail
- attribution d'un quota disque aux utilisateurs (comptes locaux uniquement)
- modification du domaine mail local des utilisateurs
- modification du profil Windows des utilisateurs (comptes locaux uniquement)
- réinitialisation du mot de passe des utilisateurs selon certains critères
- activation/désactivation du shell des utilisateurs (comptes locaux uniquement)
- association d'un rôle aux utilisateurs

L'outil de purge des comptes

L'outil de purge des comptes permet de faciliter la suppression des comptes des utilisateurs n'ayant plus de lien avec l'établissement.

Il est accessible par le menu `Gestion/Utilisateurs/Purge des comptes` de l'EAD.

Le principe de fonctionnement de l'outil de purge des comptes est d'afficher les comptes utilisateurs qui

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

n'ont pas été modifiés/retrouvés depuis un nombre de jours défini.

L'outil permet également de mettre en valeur les comptes susceptibles d'être des doublons (Homonymes).



L'outil de purge des comptes

Les actions possibles sur les comptes sélectionnés sont :

- *supprimer (en conservant leurs données)* : suppression des comptes et sauvegardes de leurs données dans `/home/recyclage/<année>/` ;
- *supprimer totalement* : suppression des comptes et de leurs données ;
- *mettre à jour (leur date de mise à jour sera mise à aujourd'hui)* : les comptes n'apparaîtront plus dans la liste.

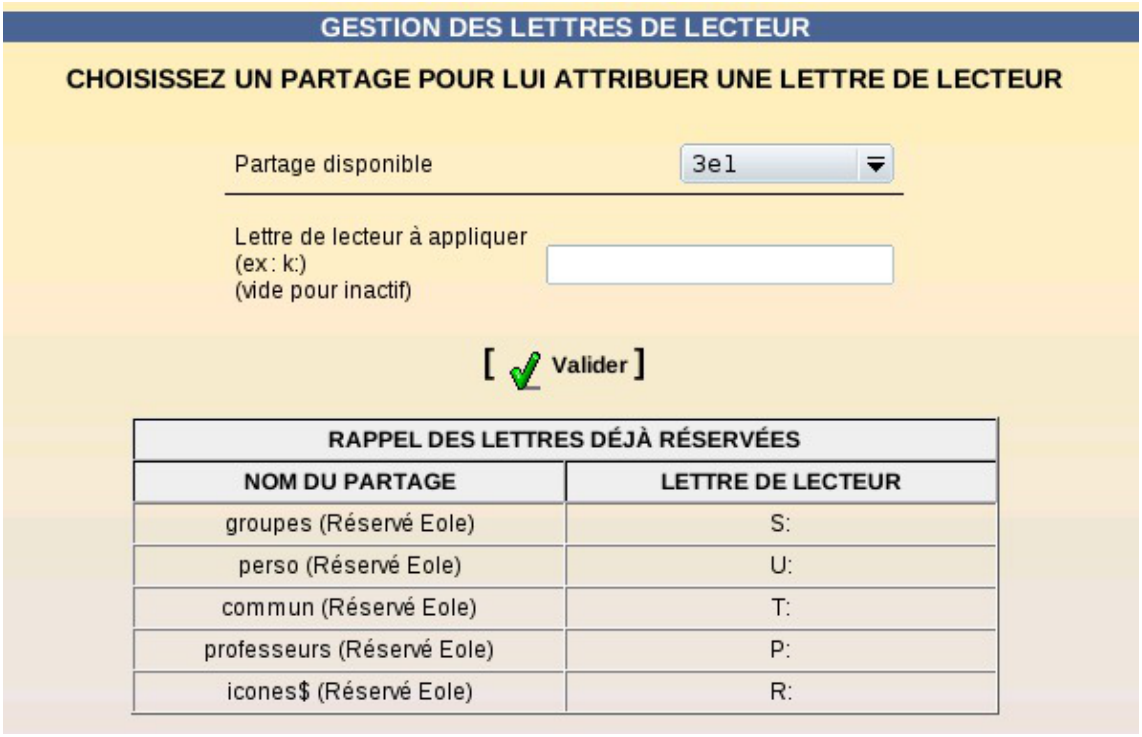
Si une importation a été réalisée, le nombre de jours proposé est calculé en fonction de la date de la dernière importation.

2.2.3. Lettres de lecteur

Par défaut, les partages associés à un groupe sont disponibles dans le partage *groupes* de l'utilisateur (lecteur `S:` sous Windows).

Dans l'EAD, il est possible d'ajouter ou de supprimer des lettres de lecteur pour un partage de groupe via le menu `Gestion/Partages/Lettre de lecteur` .

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Attribution d'une lettre à un partage

Pour ajouter une lettre de partage, il suffit de sélectionner un groupe et indiquer la lettre désirée (exemple `E:`) et `valider`.

Pour supprimer une lettre de partage, il faut sélectionner le groupe, laisser à vide le champ lettre de lecteur et `valider`.

2.2.4. Gestion fine des groupes et des utilisateurs : ACL

Des ACLs[p.882] 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` ;

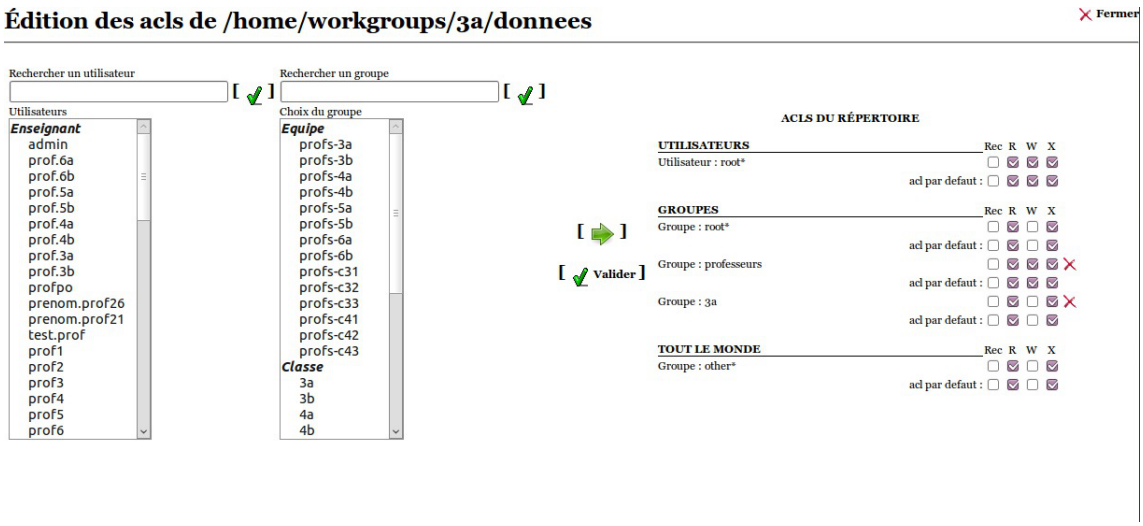
Modification des ACLs dans l'EAD

Le menu `Outils/Gestion des Acls` permet de modifier les ACLs[p.882] (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.

2.2.5. Visualisation des quotas disque dans l'EAD

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,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

...) ;

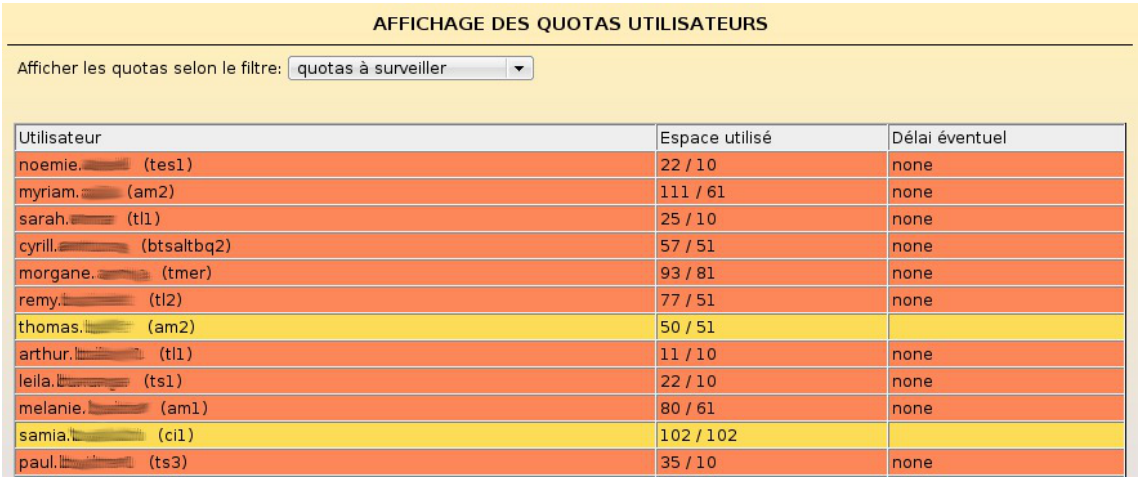
2. démonter les éventuels montages liés à cette partition (images ISO, ...) ;
3. désactiver les quotas sur la partition : `quotaoff /home` ;
4. lancer la vérification des quotas : `quotacheck -vug /home` ;
5. réactiver les quotas sur la partition : `quotaon /home` ;
6. remonter les partitions : `mount -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.

Les quotas sur le module Scribe

Pour consulter les quotas, le menu `Outils/Quotas disque` de l'EAD permet d'afficher les quotas utilisateurs selon 3 filtres :

- Quotas dépassés
- Quotas à surveiller (quotas presque atteint)
- Tous les quotas



Affichage des quotas utilisateur dans l'EAD

Les quotas sont appliqués sur la partition `/home`. Les quotas concernent, ainsi, l'ensemble des fichiers créés par l'utilisateur sur le serveur (dossiers personnels, partages équipe pédagogique, classe, groupes, etc.).

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.

2.2.6. Étendre les droits d'un personnel administratif avec les droits d'un enseignant

Cette fonctionnalité, disponible à partir de la version 2.5.2 du module, est utile pour permettre à un personnel administratif (chef d'établissement, adjoint, CPE, documentalistes, vie scolaire) d'accéder à des fonctionnalités attribuées d'office à un enseignant :

- accéder à l'observation de poste au travers de Gestion-poste ou d'EOP ;
- accéder au partage professeurs (montage `P:`) ;
- distribuer des documents au travers de l'EAD ou d'EOP ;
- avoir un accès en lecture au répertoire personnel des élèves d'une classe ;
- changer le mot de passe des élèves d'une classe ;
- être inscrit à la liste de diffusion professeurs.



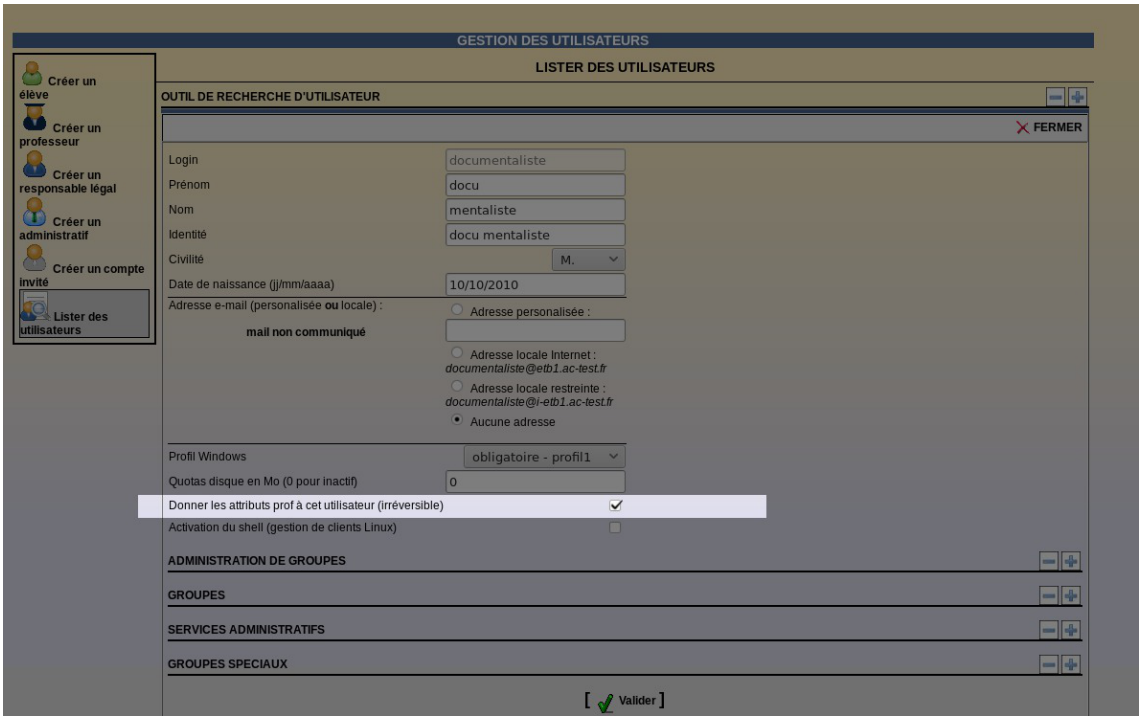
Une fois ajoutée, cette extension des droits est irréversible.

Il n'est pas possible de réaliser cette opération à la création d'un compte administratif, il faut d'abord procéder à la création si le compte n'existe pas et ensuite procéder à son édition.

Pour étendre les droits d'un compte administratif il faut se rendre dans le menu Gestion → Utilisateurs → Recherche d'utilisateur, puis dans la page, choisir `administratif` dans la liste Type de l'utilisateur et cliquer sur `Lister`.

Un tableau récapitule la liste des utilisateurs de type administratif, cliquer sur le lien `Editer` de la ligne correspondant à l'utilisateur auquel il faut étendre les droits.

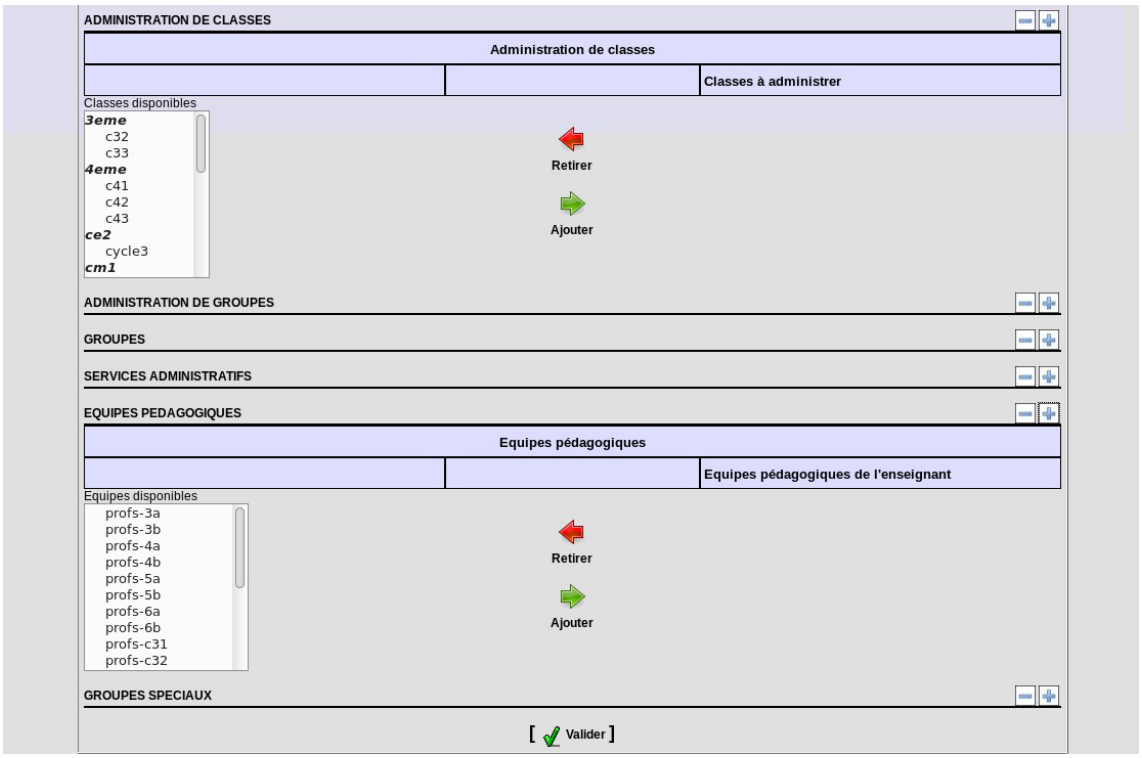
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Dans le formulaire qui s'affiche, cocher la case ☑ Donner les attributs prof à cet utilisateur (irréversible) et cliquer sur le bouton Valider.

Une fenêtre surgissante s'affiche avec un message expliquant que les modifications ont bien été effectuées.

Cliquer sur le bouton Valider de la fenêtre.



Toujours dans le formulaire d'édition du compte principal, attribuer à l'utilisateur la ou les classes désirées dans la partie `ADMINISTRATION DE CLASSES`, et attribuer la ou les équipes pédagogiques correspondantes dans la partie `EQUIPES PEDAGOGIQUES`, puis cliquer sur le bouton Valider.

Une fenêtre surgissante s'affiche avec un message expliquant que les modifications ont bien été effectuées.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cliquer sur le bouton `Valider` de la fenêtre.

2.3. Importation de comptes

L'importation est le mécanisme permettant de créer des comptes utilisateurs et des groupes à partir de données extraites d'outils externes tels que SIECLE (ex Sconet), AAF ou ONDE (ex BE1D).

Elle peut s'effectuer par l'EAD ou en mode console.

L'ordre d'importation recommandé est le suivant : d'abord les élèves puis les enseignants.

En effet, un enseignant est affecté à ses équipes pédagogiques uniquement si celles-ci existent et que la classe ou le groupe associé comporte des élèves. En important les enseignants en premier, il y a un risque pour que ceux-ci ne soient pas affectés aux équipes pédagogiques.

Cette situation peut se vérifier par la présence des lignes suivantes dans le fichier journal `/var/log/eole/importation.log`

```
DEBUG Option <option> non trouvée (sans élèves ?)
```



Il est recommandé d'effectuer une sauvegarde avant de lancer la procédure d'importation.

2.3.1. Préparation des fichiers nécessaires à l'importation

Avant une importation il faut préparer ou récupérer les fichiers requis.

Il est conseillé d'enregistrer ces fichiers et de les conserver après l'importation.

2.3.1.a. SIECLE/STS

Pour l'importation des comptes élèves et responsables, il faut récupérer quatre fichiers XML compressés parmi ceux proposés dans les "Exports XML génériques" de l'application SIECLE (ex Sconet).

Ces fichiers sont traditionnellement nommés :

- `ExportXML_ElevesSansAdresses.zip`
- `ExportXML_Nomenclature.zip`
- `ExportXML_ResponsablesAvecAdresses.zip`
- `ExportXML_Structures.zip`

Pour l'importation des comptes professeurs et personnel administratifs, il faut télécharger un fichier XML depuis les "Exports"' de l'application STS-Web. Ce fichier possède un nom de la forme :

- `sts_emp_<rne_etablissement>_<année>.xml`

Voir aussi...

Exportation des fichiers depuis SIECLE et STS [p.834]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3.1.b. AAF

Il faut exporter quatre fichiers XML AAF depuis l'application AAF[p.882] (Annuaire Académique Fédérateur).

Ces fichiers sont traditionnellement nommés :

- ENT_<rne_etablissement>_Complet_<date>_Eleve_0000.xml
- ENT_<rne_etablissement>_Complet_<date>_PersEducNat_0000.xml
- ENT_<rne_etablissement>_Complet_<date>_EtabEducNat_0000.xml
- ENT_<rne_etablissement>_Complet_<date>_PersRelEleve_0000.xml

Ces fichiers peuvent être obtenus auprès de votre rectorat.

Les adresses électroniques des responsables ainsi que leurs numéros de téléphone mobile sont désormais disponibles dans les exports AAF. Les adresses postales sont également multi-lignes. Ces nouveautés sont prises en charge par la procédure d'importation AAF à partir de la version 2.5.2 d'EOLE.

Depuis la version `AAF-VE1803`, l'INE[p.891] est présent dans les fichiers exportés depuis AAF. Il est pris en compte par la procédure d'importation à partir de la version 2.5.2 d'EOLE.

2.3.1.c. ONDE/BE1D

Il faut exporter un fichier CSV[p.887] élèves depuis l'application ONDE[p.884] (ex BE1D).

Le fichier obtenu doit impérativement posséder les champs suivants :

- Nom élève
- Prénom élève
- Date naissance
- Sexe
- INE
- Niveau
- Libellé classe

Ancien format BE1D

L'ancien format d'export de BE1D et toujours supporté. Les champs attendus dans ce cas sont les suivants :

- Nom Élève
- Prénom Élève
- Date naissance

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Sexe
- Niveau
- Classe

Il est également possible d'importer les responsables légaux des élèves.

Le fichier CSV décrivant les responsables légaux doit posséder les champs : "Nom responsable", "Prénom responsable", "Civilité Responsable", "Adresse responsable", "CP responsable", "Commune responsable", "Pays", "Courriel", "Téléphone domicile", "Téléphone travail", "Téléphone portable", "Nom de famille enfant", "Prénom enfant", et "Classes enfants".

Depuis le remplacement de BE1D par ONDE, l'INE[p.891] est disponible dans les fichiers exportés ce qui permet de retrouver les élèves plus facilement.

2.3.1.d. Texte

Cette fonctionnalité est l'équivalent de l'*importation texte version 2* et remplace définitivement l'ancienne *importation texte version 1*. Elle permet aux établissements n'utilisant pas l'une des applications précédemment citées (lycées agricoles, établissements situés à l'étranger, ...) d'importer facilement des utilisateurs à partir de fichiers CSV[p.887] simplifiés.

Elle peut également compléter une importation faite à partir des fichiers générés avec les outils précédemment cités.

Les fichiers peuvent être créés à la main ou extraits depuis une application tierce.

Les fichiers CSV doivent respecter les éléments suivants :

- en-tête indiquant les champs fournis
- séparateur le *point-virgule* (";")
- pas de séparateur de texte
- encodage en *ISO-8859-1* ou en *UTF-8*

En-tête du fichier CSV

Les fichiers d'entrée doivent impérativement posséder un champ d'**en-tête** comprenant au minimum chacun des mots clé associés aux champs obligatoires du type de compte importé.

L'en-tête permet une pré-validation les informations et permet de s'affranchir de l'ordre des champs.

Quelque soit le type d'utilisateur importé, les champs login et le mot de passe sont facultatifs.

Il servent uniquement dans le cas où l'on veut forcer leur valeur (exemple : récupération de comptes existants). Si ces champs sont absents ou à vide, le login sera généré automatiquement par l'application.

Si les notions de numéro élève, numéro professeur et/ou niveau n'existent pas dans l'établissement, il est possible de remplir ces champs avec une valeur identique pour tous.

Champs élève

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Champs obligatoires

- numero : numéro de l'élève
- nom : nom de famille
- prenom : prénom
- sexe : civilité (M ou F)
- date : date de naissance au format `jjmmaaaa` ou `jj/mm/aaaa`
- classe : classe
- niveau : niveau

Champs facultatifs

- login : login forcé
- password : mot de passe forcé
- options : options suivies par l'élève, séparées par le caractère "|"

Champs enseignant

Champs obligatoires

- numero : numéro de l'enseignant
- nom : nom de famille
- prenom : prénom
- sexe : civilité (M ou F)
- date : date de naissance au format `jjmmaaaa` ou `jj/mm/aaaa`

Champs facultatifs

- login : login forcé
- password : mot de passe forcé
- classes : classes dans lesquelles intervient l'enseignant, séparées par le caractère "|"
- options : options dans lesquelles intervient l'enseignant, séparées par le caractère "|"

Champs personnel administratif

Champs obligatoires

- numero : numéro du personnel administratif
- nom : nom de famille
- prenom : prénom
- sexe : civilité (M ou F)
- date : date de naissance au format `jjmmaaaa` ou `jj/mm/aaaa`

Champs facultatifs

- login : login forcé
- password : mot de passe forcé

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Champs compte invité

Champs obligatoires

- nom : nom de famille
- prenom : prénom
- sexe : civilité (M ou F)
- date : date de naissance au format `jjmmaaaa` ou `jj/mm/aaaa`

Champs facultatifs

- login : login forcé
- password : mot de passe forcé

2.3.2. Importation par l'EAD

L'outil d'importation est accessible par le menu `Outils/Importation` de l'EAD.

2.3.2.a. Types d'importation

La première chose à faire est de choisir son type d'importation :

- *Mise à jour des bases* : ajoute les utilisateurs et groupes manquants sans modifier les groupes existants ;
- *Importation annuelle des bases* : ajoute les utilisateurs et groupes manquants après avoir purgé les options (import des élèves) ou les équipes pédagogiques (import des professeurs).



Choix du type d'importation

Dans le cas où l'import initial doit être réalisé en plusieurs passes (cités scolaires...), l'option *importation annuelle* ne doit être utilisée qu'au premier tour.

Il est tout à fait possible de relancer des importations annuelles en cours d'année afin que la prise en compte des changements d'options et des modifications d'équipes pédagogiques soient complètes.

Par contre, cela peut venir en contradiction avec des modifications "manuelles" non répercutées dans les données utilisées pour mettre à jour les comptes.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.3.2.b. Sources de données

La seconde étape de l'importation est le choix de la source de données à utiliser.

Ce choix dépend du format des fichiers préparés pour l'importation.



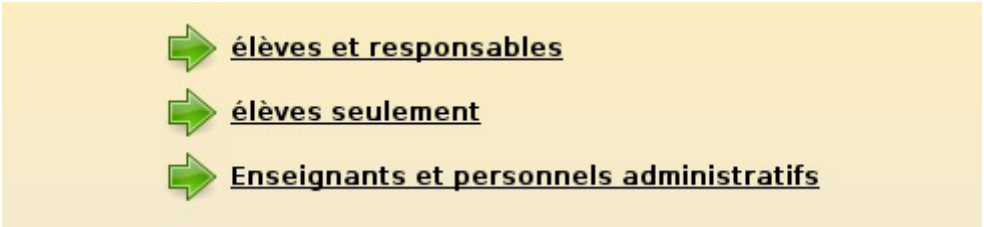
Choix de la source de données

2.3.2.c. Données à importer

La troisième étape de l'importation est le choix des données (types de comptes) à importer.

Les choix proposés à cette étape dépendent de la source de données sélectionnée à l'étape précédente.

Le choix doit généralement être fait entre les élèves (avec ou sans responsables) et les enseignants (avec ou sans personnels administratifs).



Choix des données à importer

2.3.2.d. Préférences pour la création des comptes

La quatrième étape de l'importation consiste à renseigner les options à utiliser pour créer les nouveaux comptes utilisateurs.

Les préférences se paramètrent par type d'utilisateur.

Le nombre de formulaires à valider dépendra donc des choix réalisés lors des 2 étapes précédentes.

Les préférences sont conservées d'une importation à l'autre.

Génération des identifiants

Dans le cas où c'est le format `prenom.nom` qui a été choisi, si le login généré dépasse les

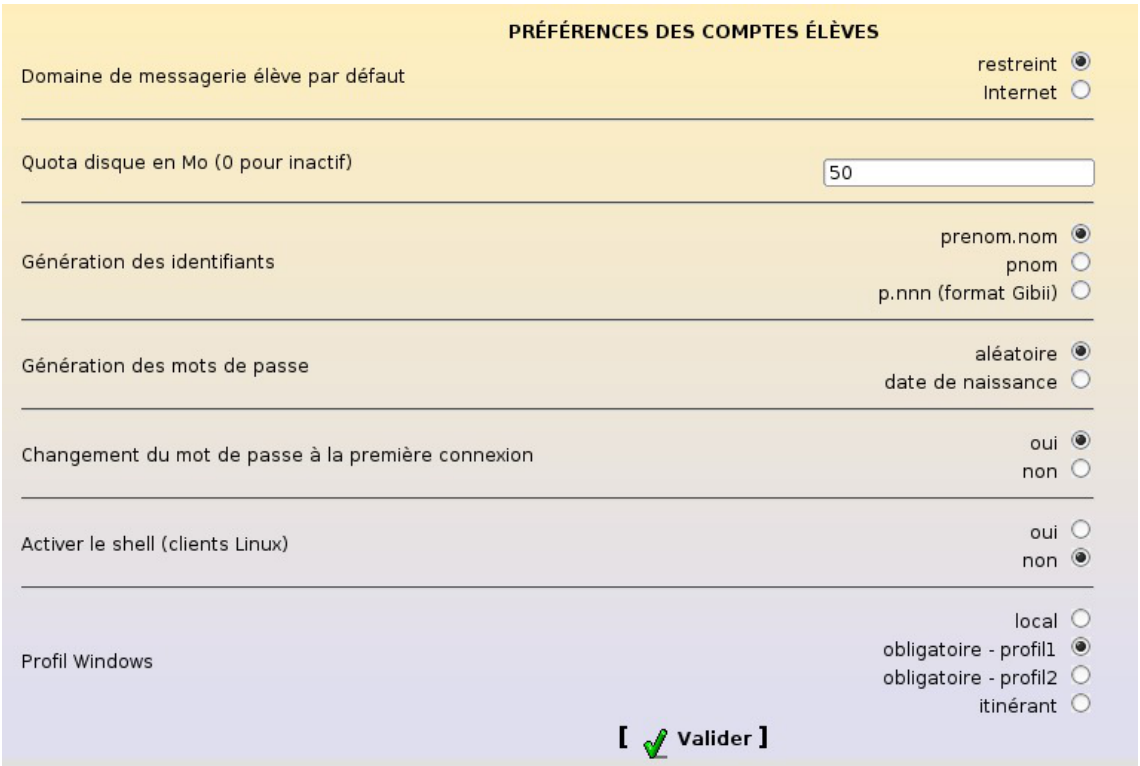
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 19 caractères, alors c'est le format `p.nom` qui est utilisé à la place.
>
> Ceci s'explique par des raisons historiques : la fenêtre de login *Windows 98* n'acceptait que 20 caractères, mais également pratiques : peu d'utilisateurs accepteraient d'entrer un login de plus de 20 caractères !

Préférences des comptes élèves

Les choix proposés sont les suivants :

- *Domaine de messagerie par défaut* : les adresses mail des nouveaux élèves peuvent être générées soit dans le domaine restreint soit dans le domaine Internet (modifiable par la suite) ;
- *Quota disque* : ce quota disque sera appliqué à tous les nouveaux élèves ; il pourra ensuite être personnalisé pour chaque classe, chaque utilisateur ;
- *Génération des identifiants* : format de création des logins pour les nouveaux élèves ;
- *Génération des mots de passe* : façon dont sont générés les mots de passe des nouveaux élèves ; l'utilisation de la date de naissance (format jjmmaaaa) permet d'éviter d'avoir à distribuer les mots de passe, mais peut poser des problèmes de sécurité ;
- *Changement du mot de passe à la première connexion* : permet d'obliger les nouveaux élèves à changer leur mot de passe lors de leur première connexion Samba ;
- *Activer le shell* : permet d'attribuer un shell valide aux nouveaux élèves (modifiable par la suite) ;
- *Profil Windows* : choix du profil Windows à appliquer aux nouveaux élèves (modifiable par la suite).

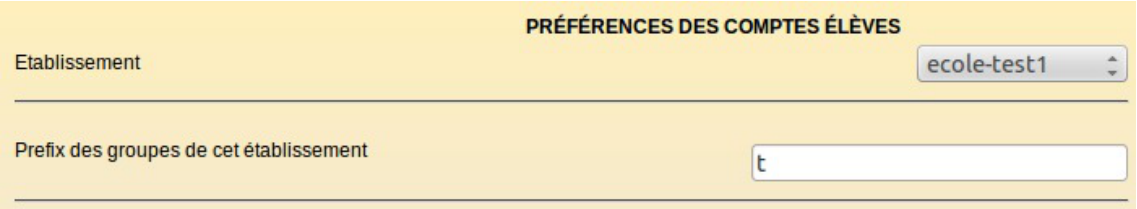


Préférences pour les élèves

> Il existe un mode multi-établissement qui permet de n'avoir qu'un seul module Scribe pour gérer plusieurs établissements. Dans ce mode, deux options supplémentaires apparaissent :
>
> - le choix de l'établissement ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le choix d'un préfixe à appliquer sur les noms des groupes rattachés à l'établissement.

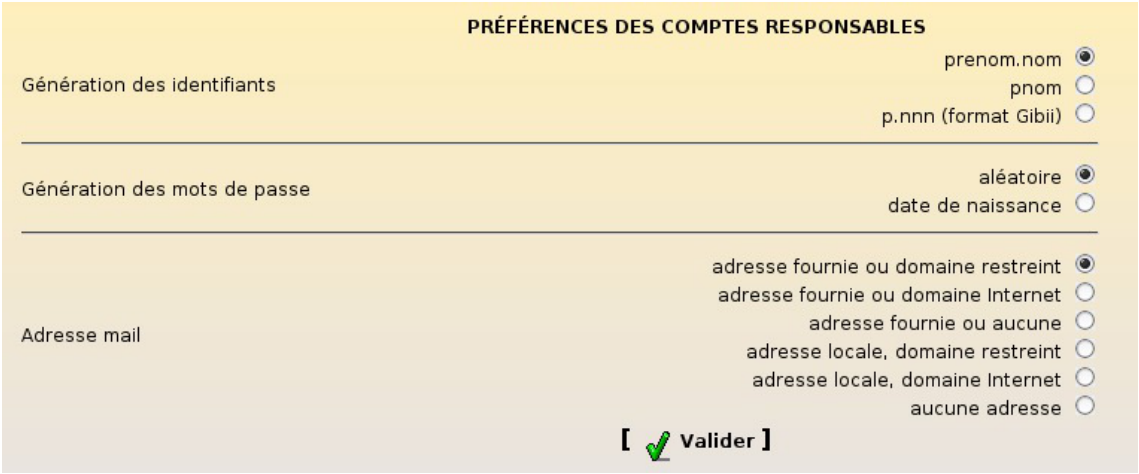


Préférences supplémentaires élèves en mode multi-établissement

Préférences des comptes responsables

Les choix proposés sont les suivants :

- *Génération des identifiants* : format de création des logins pour les nouveaux responsables légaux ;
- *Génération des mots de passe* : façon dont sont générés les mots de passe des nouveaux responsables ;
- *Adresse mail* : façon dont est attribuée l'adresse mail aux nouveaux responsables (modifiable par la suite).



Préférences pour les responsables légaux

La date de naissance des responsables légaux n'est pas forcément renseignée dans les fichiers utilisés pour l'importation.

Si la date de naissance a été choisie pour initialiser le mot de passe mais qu'elle n'est pas renseignée, un mot de passe généré aléatoirement sera affecté à l'utilisateur.

Préférences des comptes enseignants

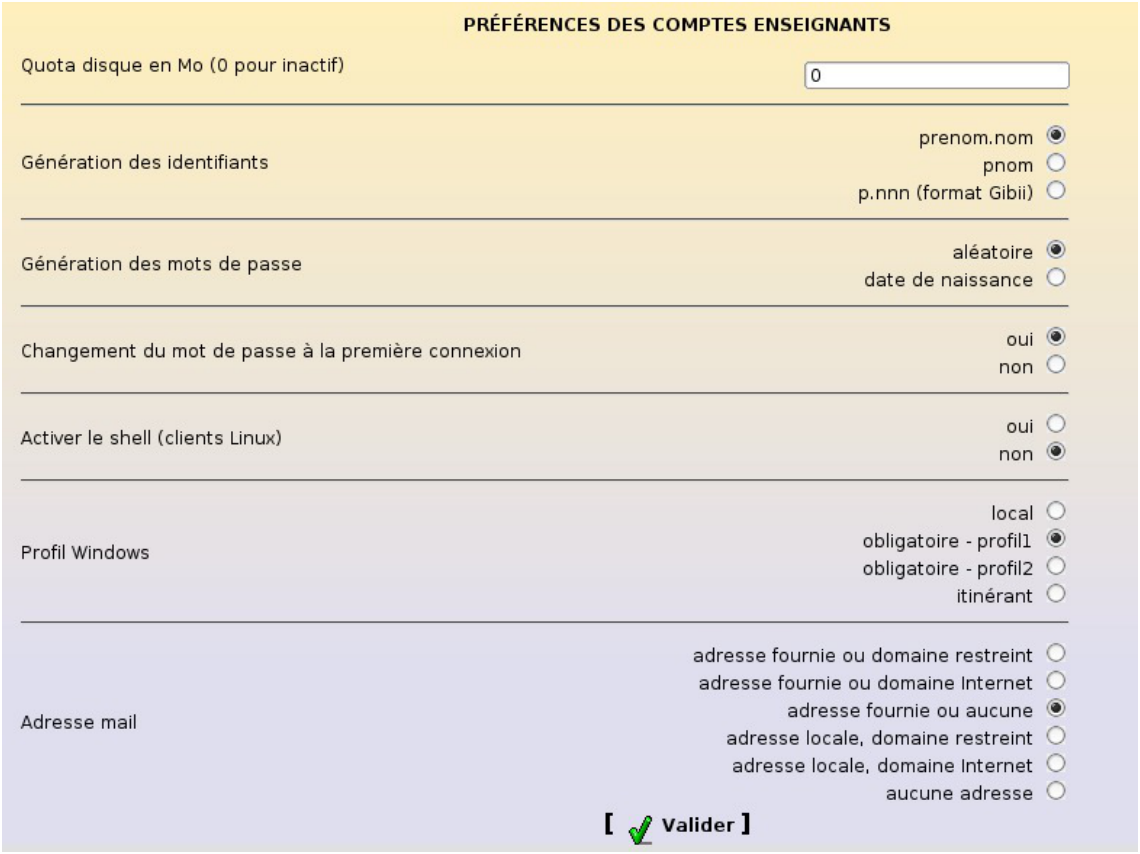
Les choix proposés sont les suivants :

- *Quota disque* : ce quota disque sera appliqué à tous les nouveaux enseignants ; il pourra ensuite être personnalisé pour chaque professeur si nécessaire ;
- *Génération des identifiants* : format de création des logins pour les nouveaux enseignants ;
- *Génération des mots de passe* : façon dont sont générés les mots de passe des nouveaux enseignants ;
- *Changement du mot de passe à la première connexion* : permet d'obliger les nouveaux enseignants à

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

changer leur mot de passe lors de leur première connexion Samba ;

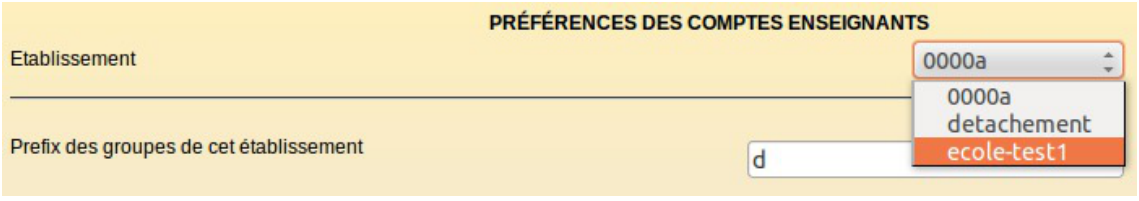
- *Activer le shell* : permet d'attribuer un shell valide aux nouveaux enseignants (modifiable par la suite) ;
- *Profil Windows* : choix du profil Windows à appliquer aux nouveaux enseignants (modifiable par la suite) ;
- *Adresse mail* : façon dont est attribuée l'adresse mail aux nouveaux enseignants (modifiable par la suite).



Préférences pour les enseignants

En mode multi-établissement, deux options supplémentaires apparaissent :

- le choix de l'établissement
- le choix d'un préfixe à appliquer sur les noms des groupes rattachés à l'établissement



Préférences supplémentaires enseignants en mode multi-établissement

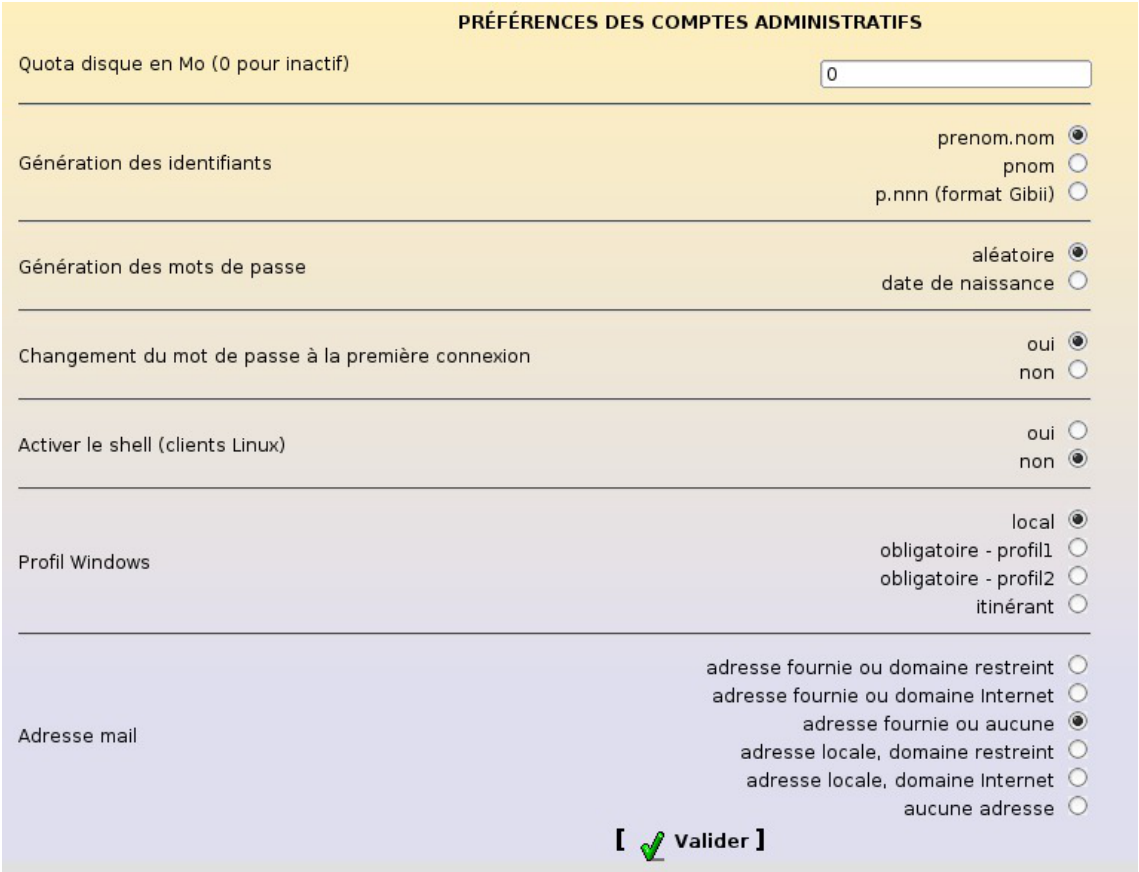
Préférences des comptes administratifs

Les choix proposés sont les suivants :

- *Quota disque* : ce quota disque sera appliqué à tous les nouveaux personnels (modifiable par la suite) ;
- *Génération des identifiants* : format de création des logins pour les nouveaux personnels ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- *Génération des mots de passe* : façon dont sont générés les mots de passe des nouveaux personnels ;
- *Changement du mot de passe à la première connexion* : permet d'obliger les nouveaux personnels à changer leur mot de passe lors de leur première connexion Samba ;
- *Activer le shell* : permet d'attribuer un shell valide aux nouveaux personnels (modifiable par la suite) ;
- *Profil Windows* : choix du profil Windows à appliquer aux nouveaux personnels (modifiable par la suite) ;
- *Adresse mail* : façon dont est attribuée l'adresse mail aux nouveaux personnels (modifiable par la suite).



Préférences pour les personnels administratifs

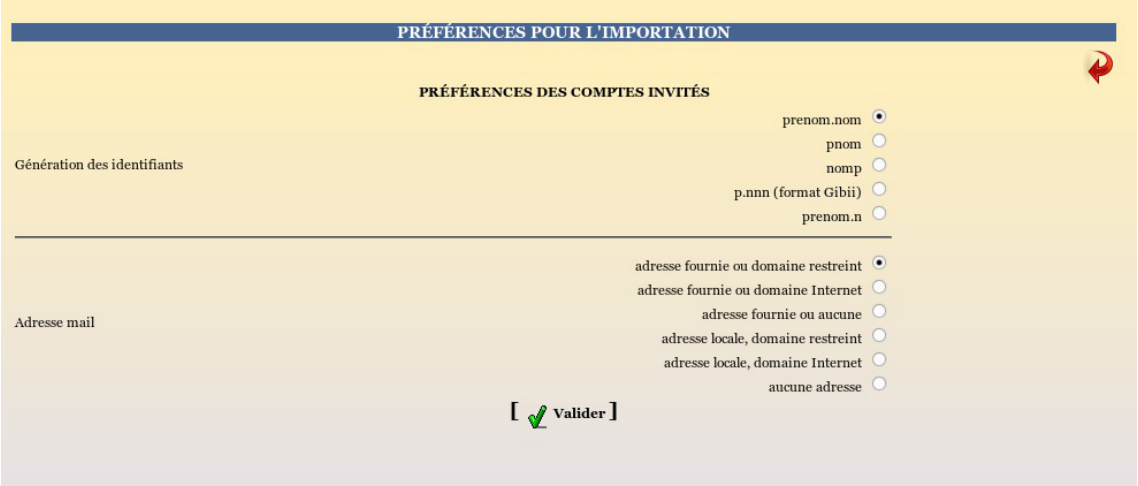
En mode multi-établissement, les personnels administratifs sont automatiquement rattachés à l'établissement choisi au niveau des préférences des enseignants.

Préférences des comptes invités

Les choix proposés sont les suivants :

- *Génération des identifiants* : format de création des logins pour les nouveaux comptes invités ;
- *Adresse mail* : façon dont est attribuée l'adresse mail aux nouveaux comptes invités (modifiable par la suite).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

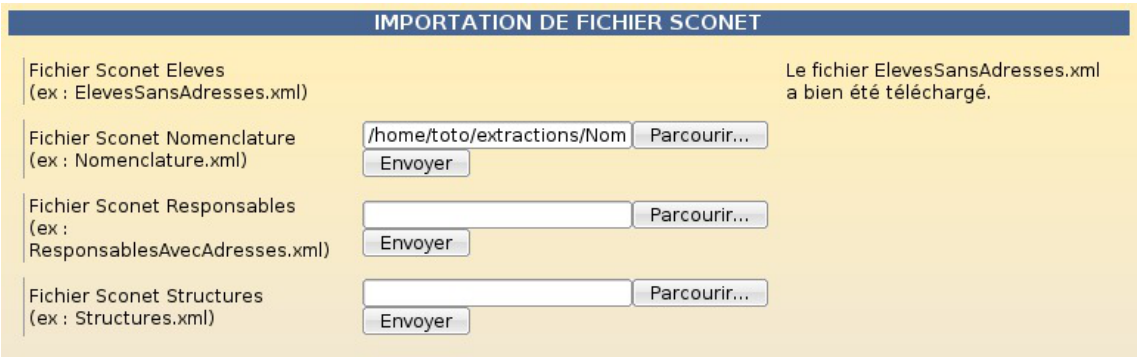


Préférences pour les responsables légaux

2.3.2.e. Téléchargement des fichiers

La cinquième étape de l'importation consiste à télécharger les fichiers contenant les données à importer.

Le nombre de fichiers à télécharger dépendra donc de la source et des données définies dans les étapes précédentes.



Téléchargement des fichiers

2.3.2.f. Lecture des fichiers

Les fichiers téléchargés doivent ensuite être traités.

Pour lancer le traitement, il faut cliquer sur le lien Lancer la lecture des fichiers.

La lecture s'effectue ensuite étape par étape.

Elle est terminée lorsque le mot **FIN** apparait.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Lecture des fichiers

Il est toujours possible d'annuler le processus d'importation tant que le traitement final n'a pas été lancé.

2.3.2.g. Importation des comptes

Une fois les fichiers lus, il n'y a plus qu'à créer effectivement les comptes utilisateurs et les groupes.

Pour lancer le traitement final, il faut cliquer sur le lien `Lancer l'importation`.

Le traitement s'effectue ensuite étape par étape.

Il est terminé lorsque la phrase **FIN DE L'IMPORTATION DE COMPTES** apparait.

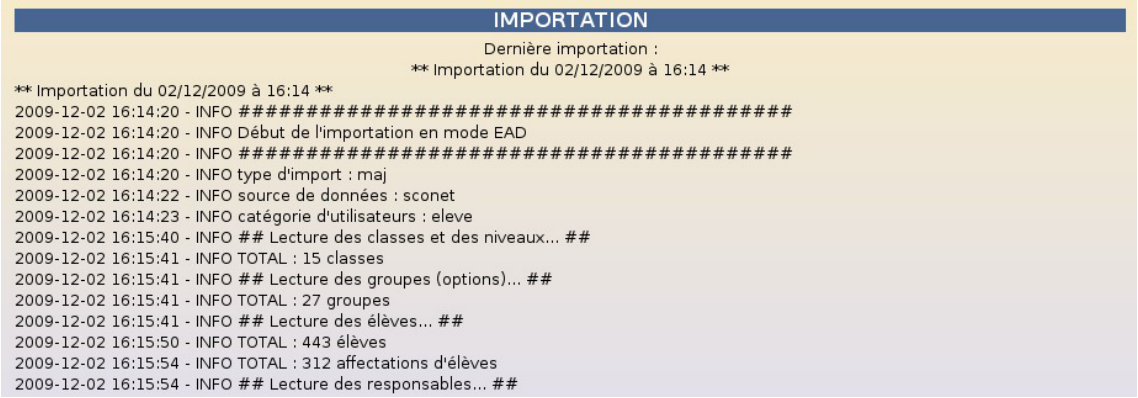


Importation des comptes

2.3.2.h. Rapport d'importation et liste des comptes

Une fois l'importation terminée, le rapport d'importation est disponible sur la page d'accueil de l'EAD.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Affichage du rapport d'importation sur la page d'accueil de l'EAD

Une copie horodatée de ce rapport est également disponible dans le dossier `importation` du répertoire personnel de l'utilisateur *admin*. Le nom exact de ce fichier (de la forme : *rapport_<date>_<heure>.txt*) est indiqué tout en bas du rapport visible par l'EAD.

Le dossier `importation` contient également la liste des comptes créés/retrouvés lors de l'importation est disponible au format CSV. Un fichier CSV horodaté est généré par type d'utilisateur créé (exemple : responsables_20091225_0001.csv).

Le nom exact de ces fichiers est indiqué dans le rapport visible par l'EAD.

Les mots de passe des utilisateurs retrouvés lors de l'importation ne sont pas modifiés.

Dans les fichiers de liste des comptes, il sont représentés par le mot clé : *(déjà attribué)*.

Les fichiers de liste des compte des importations précédentes sont toujours disponibles grâce à l'horodatage des fichiers.

Après plusieurs importations, il est tout de même conseillé de nettoyer le dossier `importation` .

En cas d'erreur durant l'importation, il peut également être utile de consulter le fichier : `/var/log/ead/ead-server.log` .

Après l'importation, il est conseillé d'utiliser l'outil de purge des compte pour supprimer facilement les compte des utilisateurs n'ayant plus de lien avec l'établissement

Lors d'une importation, les élèves sont retrouvés grâce aux nom, prénom, date de naissance et numéro élève.

Une différence, même minime, risque d'entraîner la création d'un doublon.

2.3.3. Importation en mode console

Il est également possible de réaliser une importation en mode console en utilisant le compte root.

Cette version de l'outil d'importation est plutôt réservée au développement et au débogage.

Elle se lance en utilisant la commande : `importation_scribe`

Elle s'utilise soit directement sur le serveur, soit *via* SSH (en activant, de préférence, le transfert X11).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les fichiers utilisés pour l'importation doivent, bien sûr, être présents sur le serveur.

```
root@scribe:~# importation_scribe
INFO:scribe.importation:########################################
INFO:scribe.importation: Début de l'importation en mode console
INFO:scribe.importation:########################################
Type d'importation à réaliser
0 : Mise à jour de comptes
1 : Importation annuelle

Choisissez un nombre dans la liste [0] : 0

INFO:scribe.importation:type d'import : maj
Quelle source de données voulez-vous utiliser ?
0 : Sconet
1 : AAF
2 : ONDE/BE1D
3 : Texte

Choisissez un nombre dans la liste [0] :

INFO:scribe.importation:source de données : sconet
Quelles données voulez-vous importer ?
0 : élèves et responsables
1 : élèves seulement
2 : enseignants et personnels administratifs

Choisissez un nombre dans la liste [0] :
```

Importation en mode console

2.3.4. Informations complémentaires

Rapport complet

Un rapport d'importation complet est disponible sous forme de fichier journal du système.

Ce fichier est disponible dans `/var/log/eole/importation.log` .

Il contient la trace détaillée de toutes les importations réalisées.

```
root@scribe:~# tail -n10 /var/log/eole/importation.log
2009-12-02 16:40:39 - INFO TOTAL : 588 responsables
2009-12-02 16:40:39 - INFO fichier des comptes copié dans :
2009-12-02 16:40:39 - INFO /home/a/admin/perso/importation/responsables_20091202_164039.csv
2009-12-02 16:40:40 - DEBUG Démarrage de nscd...
2009-12-02 16:40:40 - DEBUG suppression du lock eoleimport
2009-12-02 16:40:40 - INFO ########################################
2009-12-02 16:40:40 - INFO  Fin de l'importation en mode EAD
2009-12-02 16:40:40 - INFO ########################################
2009-12-02 16:40:40 - INFO fichier rapport_20091202_164040.txt copié dans :
2009-12-02 16:40:40 - INFO /home/a/admin/perso/importation/rapport_20091202_164040.txt
```

Affichage d'un extrait du fichier de log des importations

Ordre d'importation

L'ordre d'importation recommandé est le suivant : d'abord les élèves puis les enseignants.

En effet, un enseignant est affecté à ses équipes pédagogiques uniquement si celles-ci existent et que la classe ou le groupe associé comporte des élèves. En important les enseignants en premier, il y a un risque pour que ceux-ci ne soient pas affectés aux équipes pédagogiques.

Cette situation peut se vérifier par la présence des lignes suivantes dans le fichier journal `/var/log/eole/importation.log`

`DEBUG Option <option> non trouvée (sans élèves ?)`

Renommage de groupes

Dans certaines situations, il peut arriver que des groupes (principalement les classes) soient renommées

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

par le mécanisme d'importation.

Ce renommage consiste en l'ajout d'un suffixe (la lettre `c` pour les classes) devant le nom original du groupe.

Les causes d'un renommage sont généralement les suivantes :

- le nom du groupe est totalement numérique (ex : `301` pour 3eme1) ;
- il existe une homonymie au niveau des groupes (ex : niveau et classe dénommés `6g`).

2.4. Distribution de documents dans l'EAD

L'EAD offre la possibilité aux enseignants de distribuer des documents et des travaux éducatifs (évaluation, bilan, contrôle ou devoir contrôlé).

Les fonctionnalités sont équivalentes à celles disponibles dans le logiciel `Gestion-postes` mais contrairement à celui-ci, qui n'est accessible que depuis les clients Windows de l'établissement, elles sont disponibles à travers le portail Envole et donc accessibles depuis l'extérieur de l'établissement.



Vue de la distribution de document dans l'EAD

La distribution de documents au travers de l'EAD permet de faire une distribution immédiate ou différée des documents. Dans le cas d'une distribution différée (voir Choix du répertoire de destination), les documents sont préparés avec l'EAD et leur accès sera activé au moment opportun avec `Gestion-Postes`.

La distribution peut être composée de deux éléments :

- le ou les documents sous forme d'un ou plusieurs fichiers. Ils seront copiés dans chacun des dossiers personnels `devoirs` / `nom_de_l'enseignant` / `<nom_du_devoir>` des utilisateurs du groupe sélectionné. Les utilisateurs auront un accès en lecture et en écriture à ces fichiers (modification/suppression) ;
- les données jointes au(x) document(s) qui sont des fichiers supplémentaires dont la modification est impossible. Ils sont copiés une seule fois à un endroit spécifique du serveur. Des liens symbolique vers ces fichiers sont créés dans le sous-répertoire `donnees` du répertoire `devoirs`/

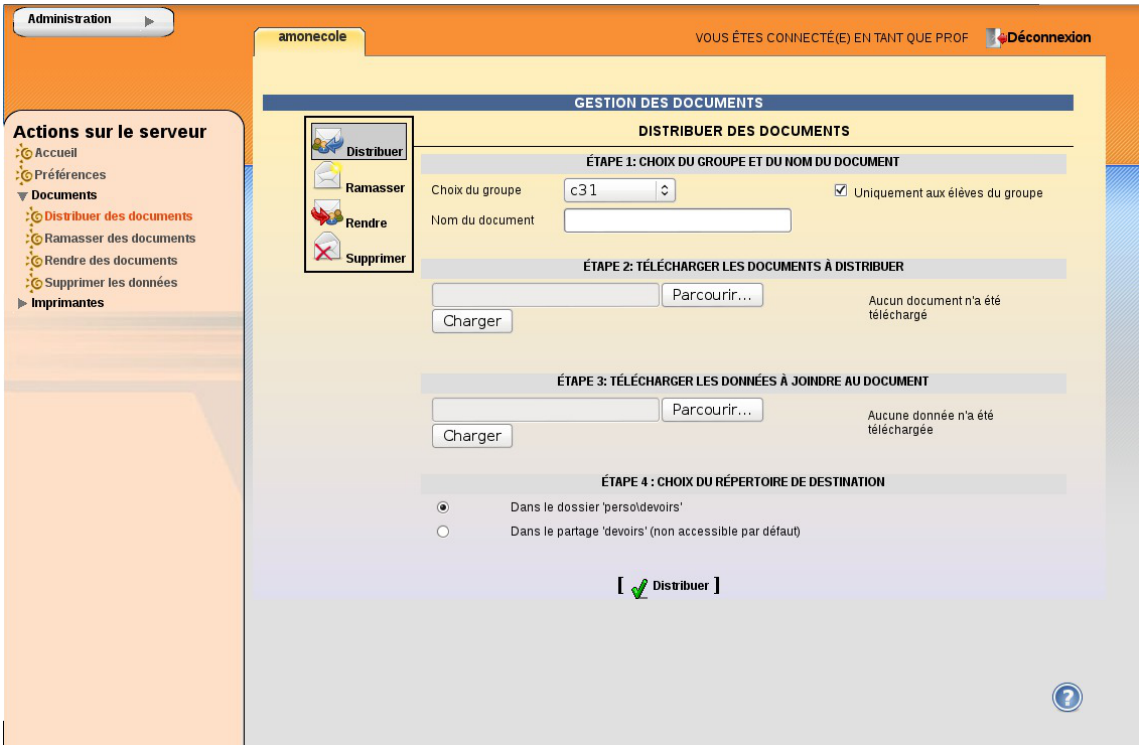
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`nom_de_l'enseignant` / `nom_devoir` de chacun des utilisateurs.

Si la distribution de document est un travail éducatif, la distribution s'effectue en suivant les 4 étapes suivantes :

- distribuer ;
- ramasser ;
- rendre : distribution des devoirs corrigés ;
- supprimer : effacement des fichiers du devoir.

2.4.1. Distribuer des documents



Vue de l'étape 1 : Distribuer

Étape 1 : Choix du groupe et du nom du document

Il faut avant tout choisir, dans le menu déroulant `Choix du groupe`, la classe, la matière ou l'équipe à qui l'ont veut distribuer un ou plusieurs documents. Puis on choisit un nom `Nom du document` pour l'espace de travail. Il apparaîtra dans le répertoire personnel de chacun des utilisateurs sous la forme `devoirs` / `nom_de_l'enseignant` / `<espace_de_travail>` et contiendra les documents de travail et les données.

Le nom du document ne doit comporter ni espace ni caractère accentué.

La case `Uniquement aux élèves du groupe` est cochée par défaut. Décochée, elle permet d'envoyer les documents aux autres membres du groupe, comme par exemple aux enseignants.

Étape 2 : Télécharger les documents à distribuer

Le bouton `Parcourir` permet de choisir un document sur son ordinateur. Après avoir cliqué sur le bouton `Charger`, le document apparaît dans la liste de droite. Il est possible de répéter l'opération pour autant de fichiers que l'on souhaite distribuer.

Étape 3 : Télécharger les données à joindre au document

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le bouton Parcourir permet de choisir un document sur son ordinateur. Après avoir cliqué sur le bouton Charger, le document apparaît dans la liste de droite. Il est possible de répéter l'opération pour autant de fichiers que l'on souhaite distribuer. Cette étape n'est pas obligatoire.

Étape 4 : Choix du répertoire de destination

Par défaut, l'option `Dans le dossier 'perso\devoirs'` étant sélectionnée, les documents seront distribués dans le répertoire personnel des utilisateurs.

L'option `Dans le partage 'devoirs' (non accessible par défaut)` permet de préparer la distribution différée de documents. Ce travail de préparation peut donc se faire aussi bien à l'extérieur qu'à l'intérieur de l'établissement. La distribution ne sera effective qu'au travers du logiciel `Gestion-postes`.

Dernière étape : Distribuer

Valider le bouton Distribuer pour que la distribution soit effective.



Il est possible de distribuer les mêmes documents à plusieurs groupes :

Étape 1 : Choix du groupe et du nom du document

Il faut choisir un autre groupe dans le menu déroulant et obligatoirement changer le nom de l'espace de travail `Nom du document`.

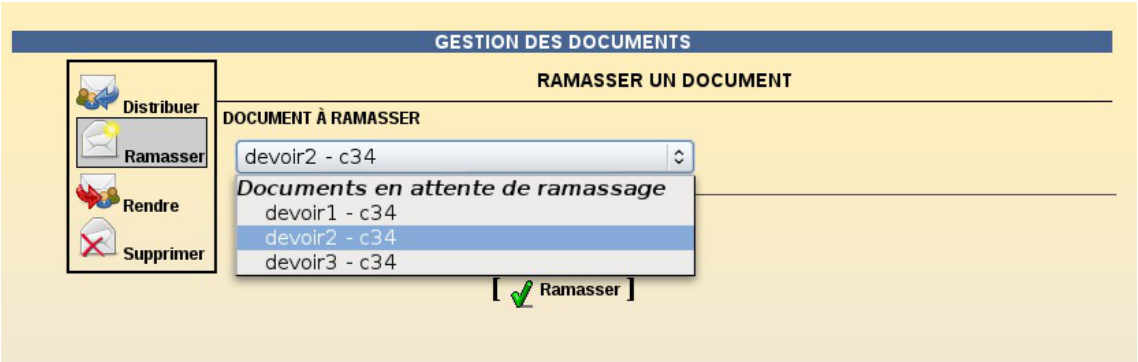
Étape 2 : Télécharger les documents à distribuer

S'il n'y a qu'un document, son chemin est encore dans le champ parcourir. Il suffit alors de cliquer sur le bouton Charger. À défaut, il faut recharger les différents documents à distribuer.

Étape 3 : Télécharger les données à joindre au document

S'il n'y a qu'une donnée, son chemin est encore dans le champ parcourir, il suffit de cliquer sur le bouton Charger. À défaut, il faut recharger les différentes données à distribuer.

2.4.2. Ramasser des documents

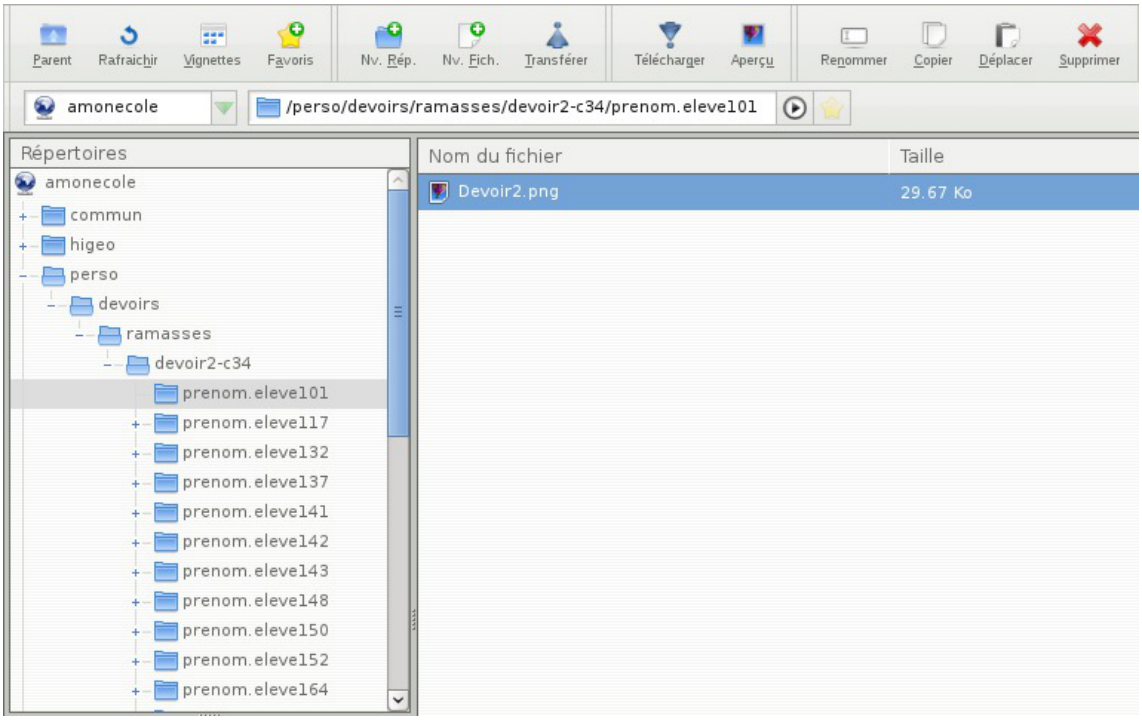


Cette fonctionnalité permet de ramasser les travaux des utilisateurs.

Les documents ramassés se retrouvent dans l'arborescence du dossier personnel de l'utilisateur les ayant ramassés :

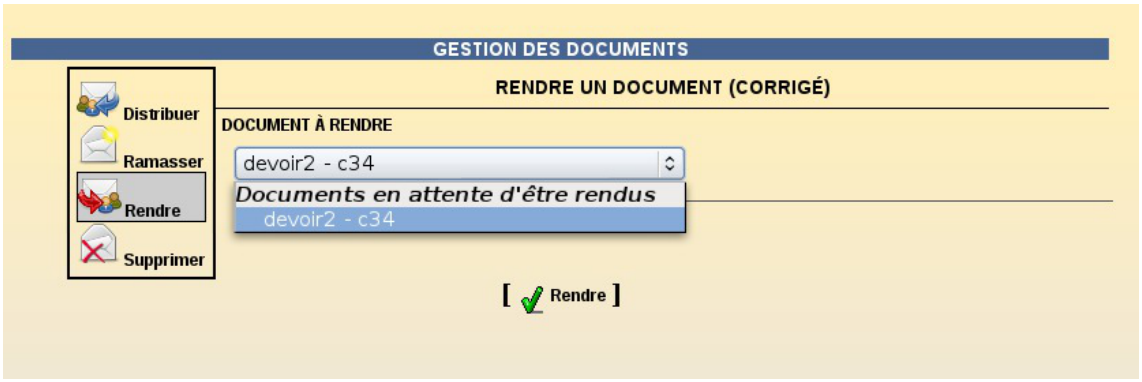
… / perso / devoirs / ramasses / Nom de l'espace de travail (Nom du document) / Identifiant des élèves /

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue des documents ramassés dans Ajaxplorer

2.4.3. Rendre des documents



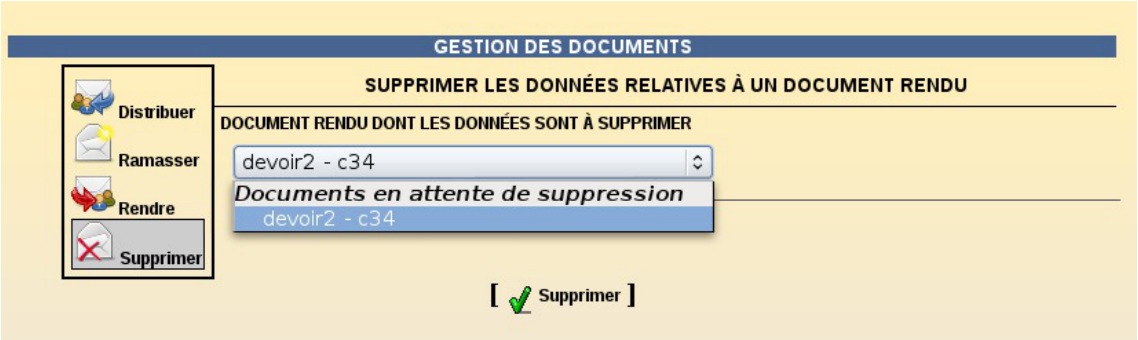
Cette fonctionnalité permet de rendre le travail corrigé. Un document ne peut être rendu que s'il a été auparavant ramassé.

2.4.4. Supprimer les données

Lorsqu'un enseignant distribue des données en plus des documents, elles sont copiées dans `U:\devoirs\.distribues` et des liens vers ces fichiers sont ensuite créés dans le répertoire `nom_du_devoir` \ `donnes` de chacun des destinataires.

Il est possible de supprimer ces fichiers lorsqu'ils sont devenus inutiles.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- La suppression des données entraînera également la suppression du dossier `<nom_du_devoir>` \ `donnees` dans le dossier des destinataires.
- Cette fonctionnalité permet de supprimer les données liées à une distribution de document qui ne seraient plus utiles par la suite. Elle permet donc d'économiser de la place sur le serveur de stockage.

Voir aussi...

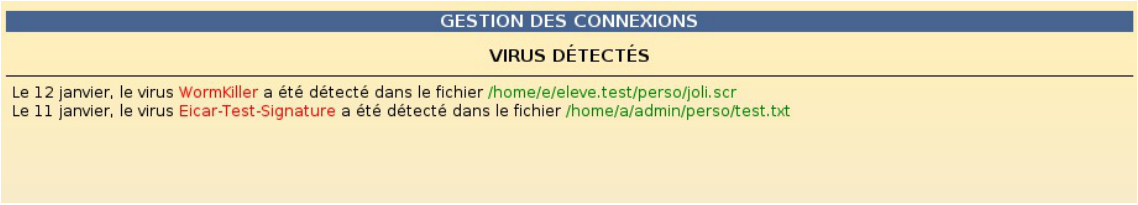
L'application Gestion-postes [p.495]

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 :

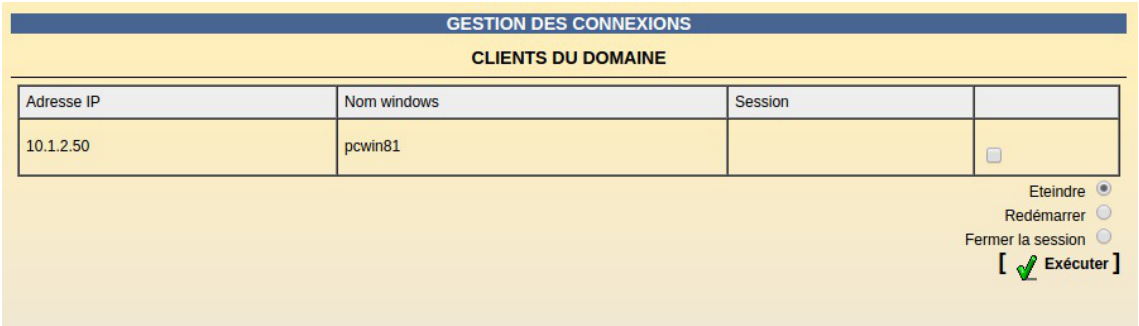
- onglet `Services` : `Activer l'anti-virus ClamAV` à `oui`
- onglet `Clamav` : `Activer l'anti-virus temps réel sur SMB` à `oui`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.6. Gestion des machines

Gestion des clients du domaine

Le menu Outils/Stations/Machines permet d'obtenir la liste des machines démarrées ayant un client Scribe Windows installé et d'agir sur celles-ci.



Les postes de la liste peuvent être éteints ou redémarrés.

Il est également possible de forcer la fermeture de la session de l'utilisateur connecté sur ces postes.

Ces actions sont forcées, si une session est ouverte, le travail de l'utilisateur **NE sera PAS sauvegardé** et la **fermeture des applications forcée**.

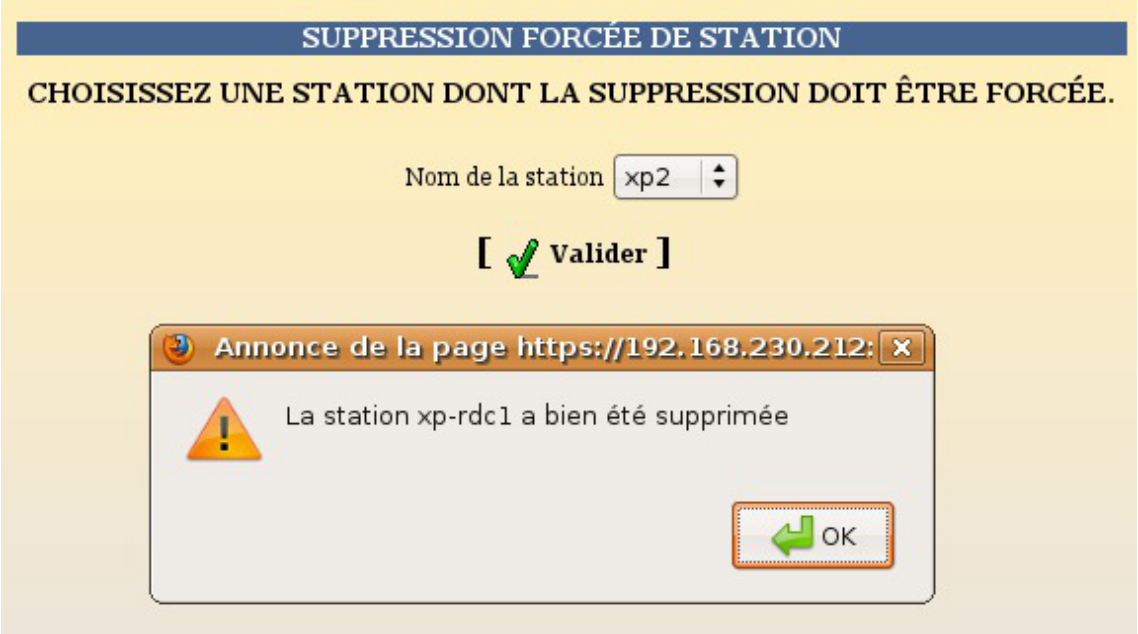
D'autres options d'affichage étaient proposées avant l'arrêt du support de Windows XP. Elles sont incompatibles avec les dernières version de Windows et ont été supprimées à partir de la version 2.5.2 d'EOLE :

- "Maîtres explorateurs" : liste des maîtres explorateurs appartenant à un groupe de travail spécifique ;
- "Contrôleur de domaine" : liste des contrôleurs du domaine avec le nom du domaine qu'il contrôle ;
- "Toutes les stations" : liste toutes les machines présentes dans les propositions précédentes.

Suppression d'une machine

Le menu Outils/Stations/suppression de la station 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)



Suppression d'une machine dans l'EAD Scribe

La ré-inscription d'une station dans le domaine (formatage et réinstallation d'une machine avec un nom identique) peut parfois renvoyer une erreur.

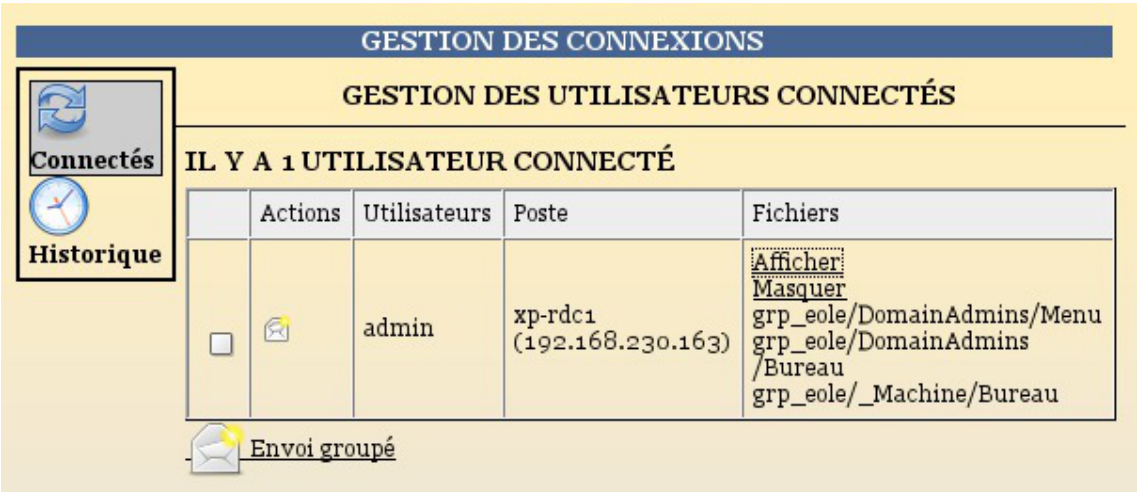
La suppression du compte de la station peut aider à résoudre le problème.

2.7. Gestion des connexions dans l'EAD

Gestion des utilisateurs connectés

Le menu `Outils/Connexion` permet de connaître les utilisateurs connectés, de connaître leurs fichiers ouverts et d'écrire à ces utilisateurs.

En listant les connectés, il est possible de connaître également la liste des fichiers ouvert par l'utilisateur. Pour cela, cliquer sur le bouton "Afficher" dans la colonne "Fichiers" :



Liste des utilisateurs connectés

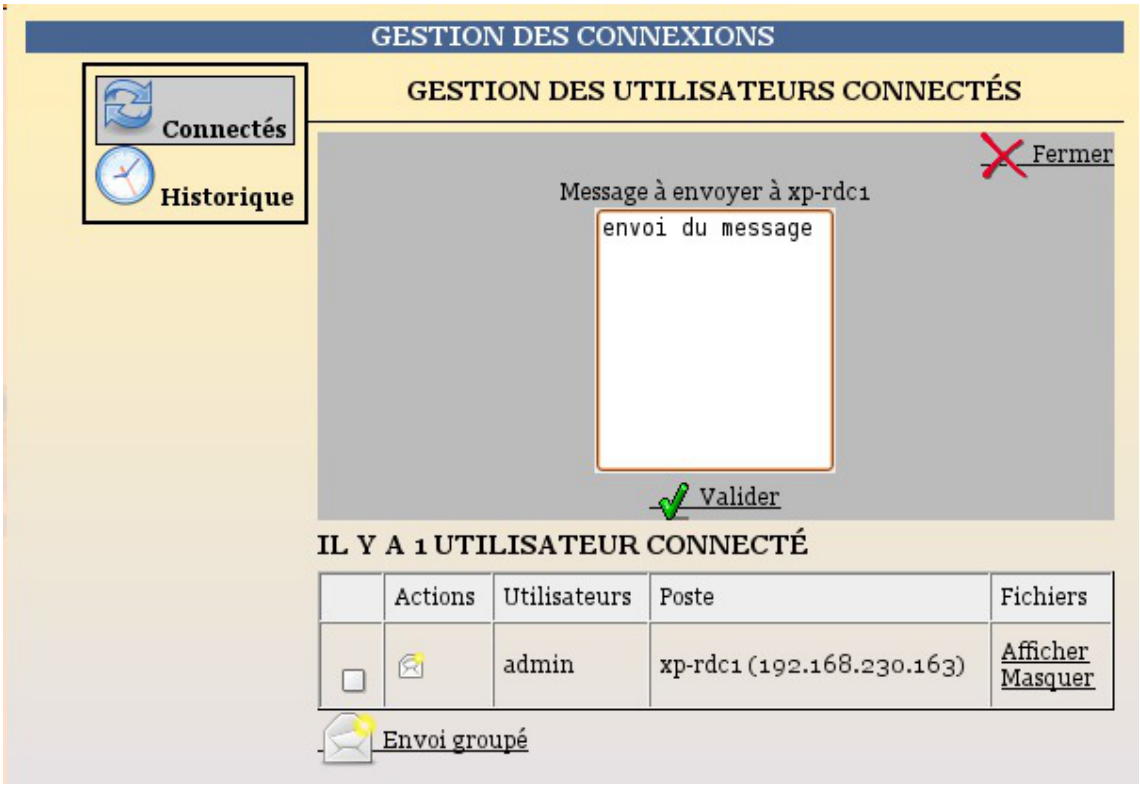
L'envoi de messages aux connectés grâce à *Winpopup* est possible et consiste en un popup s'affichant au premier plan sur l'écran de l'utilisateur. Il permet d'envoyer de courts messages aux utilisateurs ayant

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

une session ouverte sur le domaine. Pour envoyer un message, deux solutions :

- cliquer sur la petite enveloppe de la colonne action ;
- cocher la case à gauche et cliquer sur Envoi groupé.

L'envoi groupé permet d'envoyer le même message aux utilisateurs sélectionnés simultanément.



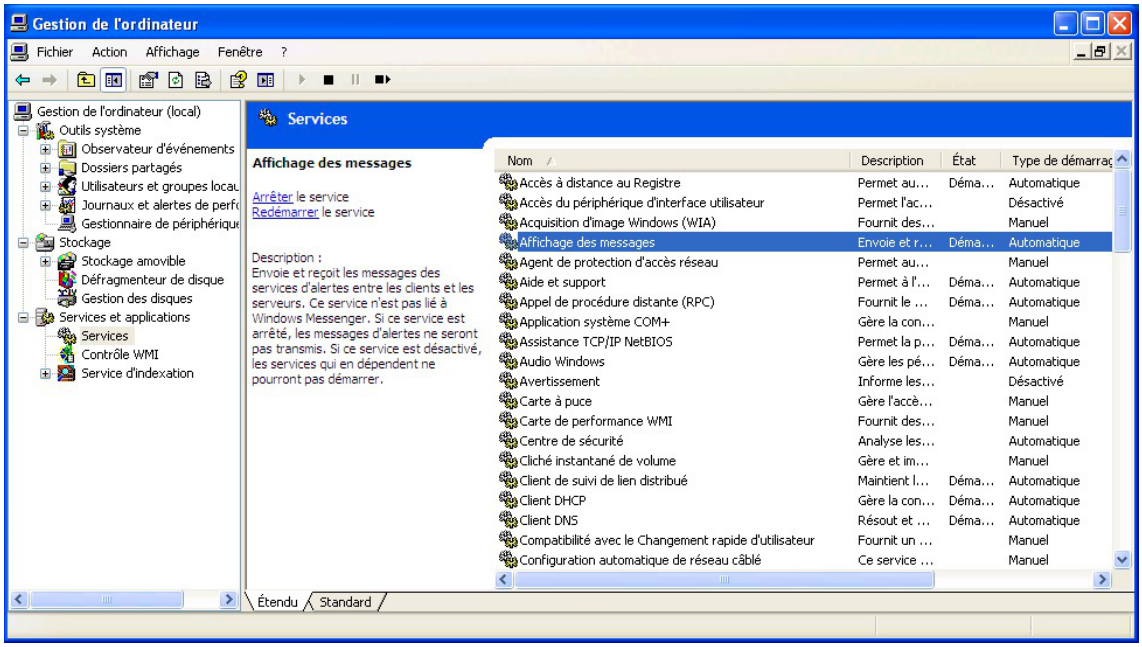
Connexion : envoyer un message à des utilisateurs connectés



Connexion : confirmation de l'envoi d'un message

Afin que les messages puissent être reçus, il est impératif de lancer Winpopup sur les station 98/Me ou que le service **Affichage des messages** *(Messenger)* soit sur démarrage *Automatique*.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Activer le service d'affichage des messages sous Windows XP

L'installeur du client Scribe active automatiquement le service d'affichage des messages. Il n'est donc, en principe, pas nécessaire d'intervenir sur la station.

Historique des connexions

L'historique des connexions affiche les dernières ouvertures de sessions sur le domaine Samba en commençant par la plus récente. L'historique ne concerne que la semaine courante.



Date	Utilisateurs	Ordinateurs	OS
Tue 01 sep 2009 16:40	admin	xp-rdc1 (192.168.230.163)	WinXP
Tue 01 sep 2009 14:44	admin	xp-rdc1 (192.168.230.163)	WinXP
Tue 01 sep 2009 14:31	admin	xp-rdc1 (192.168.230.163)	WinXP
Tue 01 sep 2009 14:10	admin	xp-rdc1 (192.168.230.163)	WinXP

Historique des connexions

Les connexions sont journalisées dans le fichier `/var/log/samba/connexions.log` .

Il est possible de retrouver des connexions plus anciennes en consultant les archives de ce fichier (ex. `/var/log/samba/connexions.log.1.gz`).

Voici comment retrouver l'historique des connexions d'un poste :

```
root@scribe:~# cd /var/log/samba
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
root@scribe:/var/log/samba# ll connexions.*
```

Cette commande renvoi deux types de fichiers :

- `connexions.log` : fichier de journalisation en cours avec les dernières connexions ;
- `connexions.x.gz` : fichier de journalisation compressé avec les connexions les plus anciennes, plus la valeur de x est élevé plus les journaux sont anciens.

```
root@scribe:~# (zcat connexions.x.gz | less) > /root/journauxDeConnexions.log
```

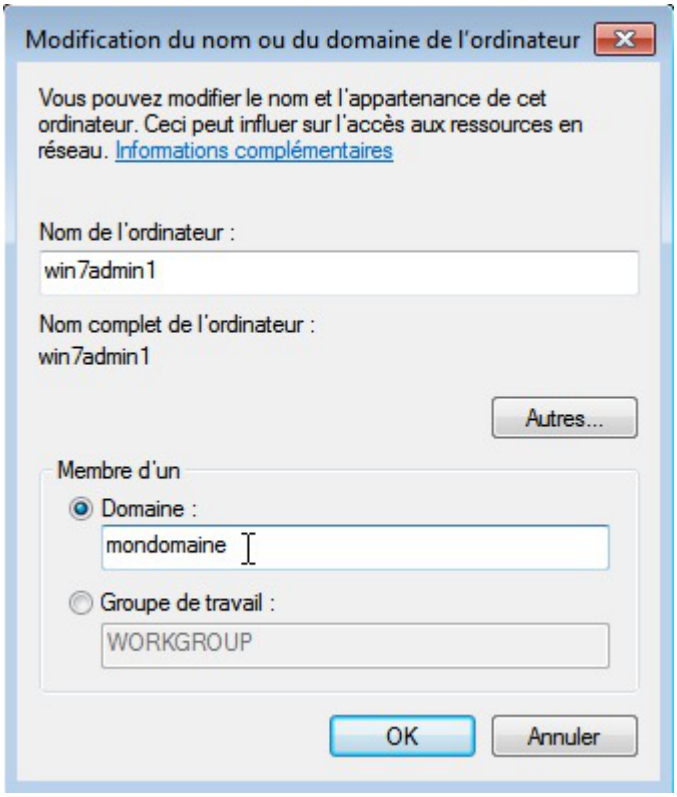
Cette commande permet de créer le fichier `journauxDeConnexions.log` dans `/root/` qui contient les journaux de connexions du fichier `connexions.x.gz`.

Pour chercher toutes les occurrences de connexions du poste pcwin (nom de l'ordinateur) :

```
root@scribe:~# cat /root/journauxDeConnexions.log | grep pcwin
CONNECTION Mon 01 feb 2016 15:08 admin professeurs pcwin Vista 10.1.2.50 31271
CONNECTION Mon 01 feb 2016 17:31 prof1 professeurs pcwin Vista 10.1.2.50 26002
 CONNECTION Mon 01 feb 2016 17:32 prof1 professeurs pcwin Vista 10.1.2.50 26002
CONNECTION Mon 01 feb 2016 17:32 prof1 professeurs pcwin Vista 10.1.2.50 26029
CONNECTION Mon 01 feb 2016 17:32 prof1 professeurs pcwin Vista 10.1.2.50 26002
 CONNECTION Mon 01 feb 2016 17:37 prof1 professeurs pcwin Vista 10.1.2.50 26002
 CONNECTION Mon 01 feb 2016 17:37 c31e1 eleves pcwin Vista 10.1.2.50 26333
CONNECTION Mon 01 feb 2016 17:38 c31e1 eleves pcwin Vista 10.1.2.50 26333
```

Le nom de l'ordinateur est un paramètre Windows.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Pour enregistrer cette liste de connexions du poste `pcwin` dans un fichier :

```
root@scribe:~# ( cat /root/journauxDeConnexions.log | grep pcwin) > /root/journauxDeConnexionsPCWIN.log
```

Toutes sortes de tris (par date, par salle ...) peuvent être effectués en adaptant la commande `grep`. Cette commande est sensible à la casse sauf si l'option `-i` est ajoutée.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

directement réutilisables.

Pour cela, il suffit de sélectionner la machine souhaitée au niveau de la liste déroulante Baux en cours.

2.9. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles[p.887].

Une règle peut être :

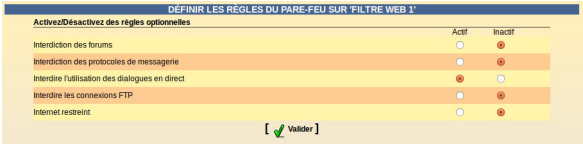
- générale, si elle concerne l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone.

La configuration générale est accessible par le menu EAD : Configuration générale / Règles du pare-feu.

La configuration spécifique est accessible par le menu EAD : Filtre web X / Règles du pare-feu :

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



Activation des directives optionnelles dans l'EAD

Lien entre ERA et les directives optionnelles de l'EAD

Pour les règles optionnelles, l'EAD prime sur l'ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comme étant active par défaut dans ERA et ne pas être active car désactivée dans l'interface EAD.

Voir aussi...

Les directives optionnelles

2.10. Exceptions sur la source ou la destination

Par défaut, tous les accès à des sites nécessitent une authentification (si elle est active) et toutes les machines du réseau doivent s'identifier. Mais certains systèmes ou logiciels doivent pouvoir se mettre à jour de façon transparente.

Par ailleurs, le proxy conserve une version des pages téléchargées en cache pour limiter la consommation réseau. Ce comportement n'est pas adapté à tous les sites.

Pour les sites comportant des données sensibles, il est nécessaire de s'assurer que des données relatives à la navigation sur ce domaine ne soient pas placées dans le cache du serveur.

Certaines machines peuvent également avoir besoin de naviguer avec des données provenant directement du site consulté.

Certains postes clients ou serveurs du réseau ont besoin d'effectuer des mises à jour automatiquement, les sites de mise à jour doivent être accessibles sans authentification.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Certaines machines peuvent également avoir besoin de naviguer sans être authentifiées.
Pour cela, il existe deux mécanismes :

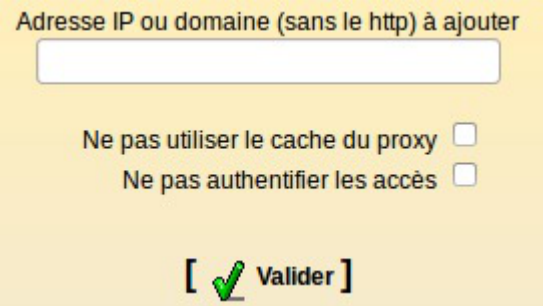
- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

Pour paramétrer les destinations et les sources qui n'utiliseront pas le cache ou l'authentification lors de la navigation il faut se rendre dans `Configuration générale` puis `Cache et Authentification` de l'interface EAD du module.

Cache et authentification de la destination

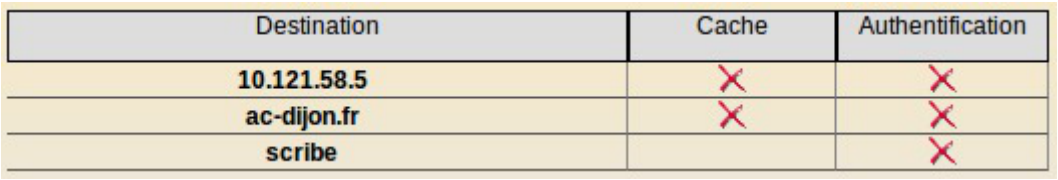
Dans `Configuration générale` / `Cache et Authentification` / `Destinations` :

- entrer l'adresse IP ou le nom du domaine ;
- cocher authentification et/ou cache ;
- valider.



Ajout d'une destination à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :



Destination	Cache	Authentification
10.121.58.5	✗	✗
ac-dijon.fr	✗	✗
scribe		✗

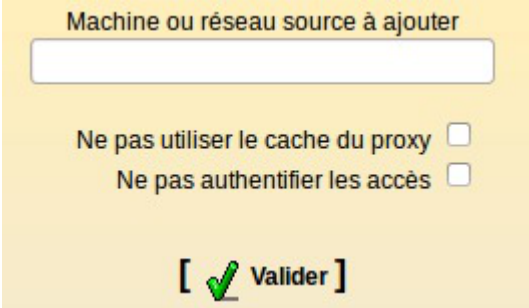
Listes des destinations à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Cache et authentification de la source

Dans `Configuration Générale` / `Cache et Authentification` / `Sources` :

- entrer l'adresse IP ou réseau
- cocher authentification et/ou cache ;
- valider.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ajout d'une source à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

Source	Cache	Authentification
10.121.58.5	✗	✗
10.21.58.10	✗	✗
172.16.0.0/24		✗
172.16.0.6	✗	✗

Listes des sources à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Personnalisations académiques

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid3/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/src_noauth_acad` : liste de sources à ne pas authentifier ;
- `/etc/squid3/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père.



L'utilisation du fichier `/etc/squid3/domaines_noauth_acad` pour gérer la liste de destinations à ne pas authentifier est dépréciée depuis la version 2.5.2. Il faut utiliser la fonctionnalité de l'onglet `Exceptions proxy` de l'interface de configuration du module.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.247]

2.11. Filtrage web

Avec le filtrage web, il est possible :

- de configurer la manière dont le filtrage s'effectue ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des utilisateurs (seulement si l'authentification est activée durant la phase de configuration) ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des machines.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette configuration s'effectue :

- par zone de configuration ;
- de manière plus fine, par politique de filtrage ;
- de façon prioritaire sur les utilisateur puis sur les machines si l'authentification est désactivée sinon de façon prioritaires sur les machines puis sur les utilisateurs.

2.11.1. Filtrage par utilisateur

Si l'authentification a été activée sur la zone durant la phase de configuration, il est possible de définir, pour l'utilisateur, une des politiques de filtrage suivante :

- modérateur (lorsqu'un site est interdit, un lien lui est proposé pour outrepasser l'interdiction) ;
- interdits (aucune navigation web n'est possible pour cet utilisateur) ;
- mode liste blanche (seuls les sites de la liste blanche sont autorisés) ;
- politique de filtrage web spécifique.

Placer un professeur sur la liste des modérateurs pour la zone de filtre web 1

Il est parfois intéressant de voir un site interdit, qui, parfois, empêche l'accès à un contenu pédagogique. En définissant un professeur comme modérateur, on lui permet d'outrepasser l'interdiction de navigation et, le cas échéant, le placer sur la liste des sites autorisés.

Dans `Filtre web 1` / `Utilisateurs` :

- entrer le nom de l'utilisateur ;
- valider ;
- choisir `Modérateur` dans la liste.



Configurer des politiques de filtrage pour un utilisateur sur la zone de filtre web 2

Ces informations sont stockées dans :

`/var/lib/blacklists/dansguardian<num_instance>/common/filtergroupslist`

Sur AmonEcole, ces fichiers sont dans le conteneur ***reseau*** .

Si le menu `Utilisateurs` n'apparaît pas, c'est que la zone n'est pas authentifiée.

2.11.2. Filtrage par machine ou par groupe de machine

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le module Amon propose de gérer des groupes de machine par plage d'adresse IP.

En ajoutant une référence à ce groupe, il est possible :

- de lui interdire l'accès au réseau ;
- de lui interdire la navigation web seulement ;
- de lui autoriser la navigation web selon des horaires ;
- de lui associer une politique de filtrage web spécifique.



Les informations liées aux groupes de machine sont stockées dans :

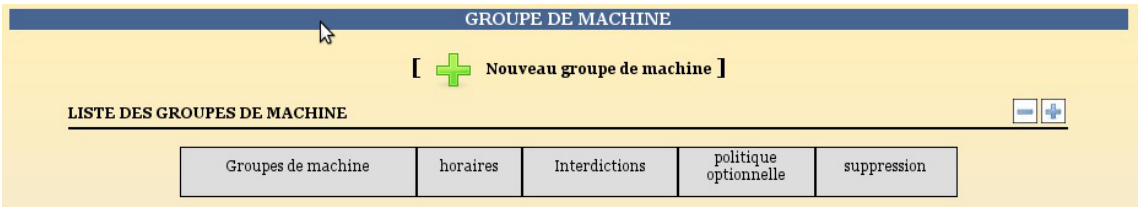
`/usr/share/ead2/backend/tmp/ipset_group<num_instance>.txt`

Les éventuelles plages horaires associées sont dans :

`/usr/share/ead2/backend/tmp/ipset_schedules<num_instance>.pickle`

Créer un groupe de machine

Pour configurer un groupe de machine de la zone 1, aller dans `Filtre web 1` / `Groupe de machine`.



Interface de gestion de groupe de machine

Cliquer sur `Nouveau groupe de machine` et un formulaire de création apparaît.



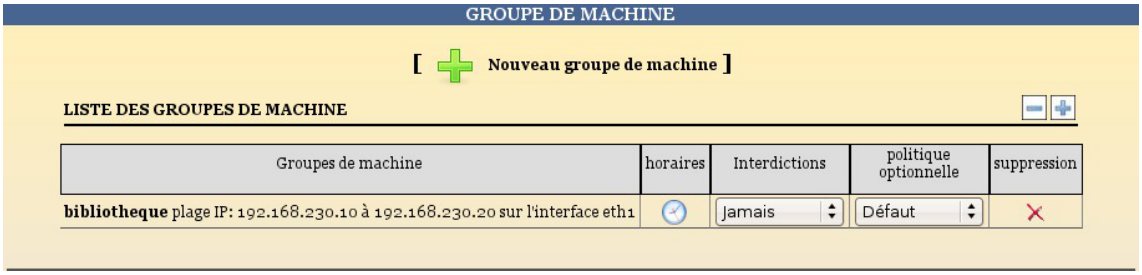
Formulaire de création

Remplir :

- nom pour le groupe de machine (sans accents ni caractères spéciaux) ;
- donner l'adresse IP de début de plage ;
- donner l'adresse IP de fin de plage ;
- si plusieurs interfaces réseau sont associés à cette zone, il vous demandera le nom de l'interface ;
- valider.

Le groupe de machine est dans la liste et peut être géré.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le groupe de machine est ajouté

S'il ne vous est pas possible de choisir l'interface de votre groupe lors de sa création, c'est qu'une seule interface du pare-feu est associée à cette zone.

À partir de la version 2.5.2 d'EOLE, il n'est plus obligatoire que la plage d'adresse du groupe soit de classe C.

Un trop grand nombre d'adresses dans un groupe peut entraîner une baisse de performance.

Limiter l'accès réseau

Dans la colonne `Interdictions`, il est possible de choisir parmi :

- jamais ;
- le web tout le temps ;
- le web selon des horaires (à définir au préalable) ;
- toute activité réseau.

Interdire le groupe de navigation web

Dans la colonne `Interdictions`, choisir `Le web tout le temps`

Le groupe de machine est alors interdit d'accès sur les ports :

- 80 (HTTP)
- 443 (HTTPS)
- 3128 (e2guardian)
- 8080 (Squid)

Si vous désirez faire une interdiction de navigation selon des horaires, il faut :

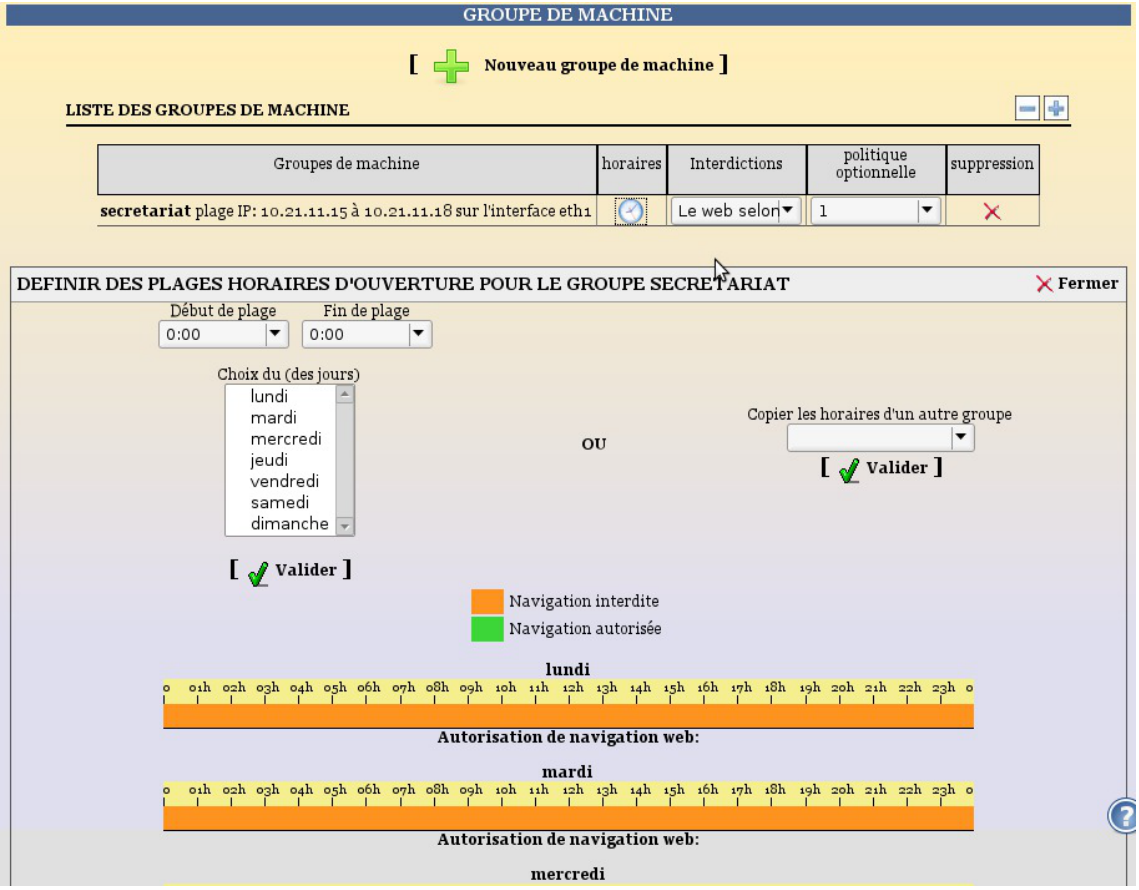
- configurer des horaires ;
- appliquer l'interdiction.

Configuration des horaires

Dans la colonne `Interdictions`, choisir `Le web selon horaires`.

Cliquer sur l'horloge, la gestion des horaires apparaît.

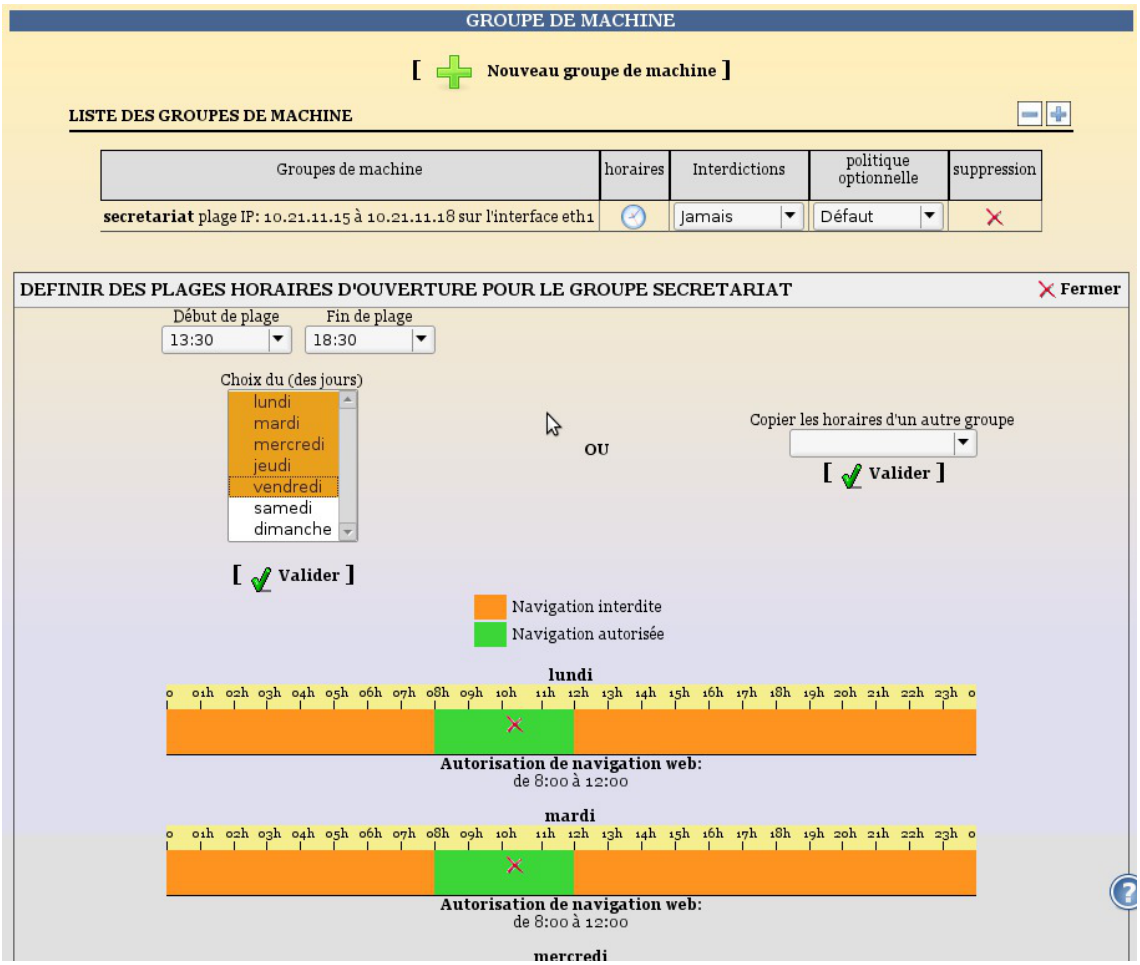
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Gestionnaire d'horaires pour les groupes de machine

- choisir la plage horaire d'autorisation ;
- choisir les jours d'applications ;
- valider.

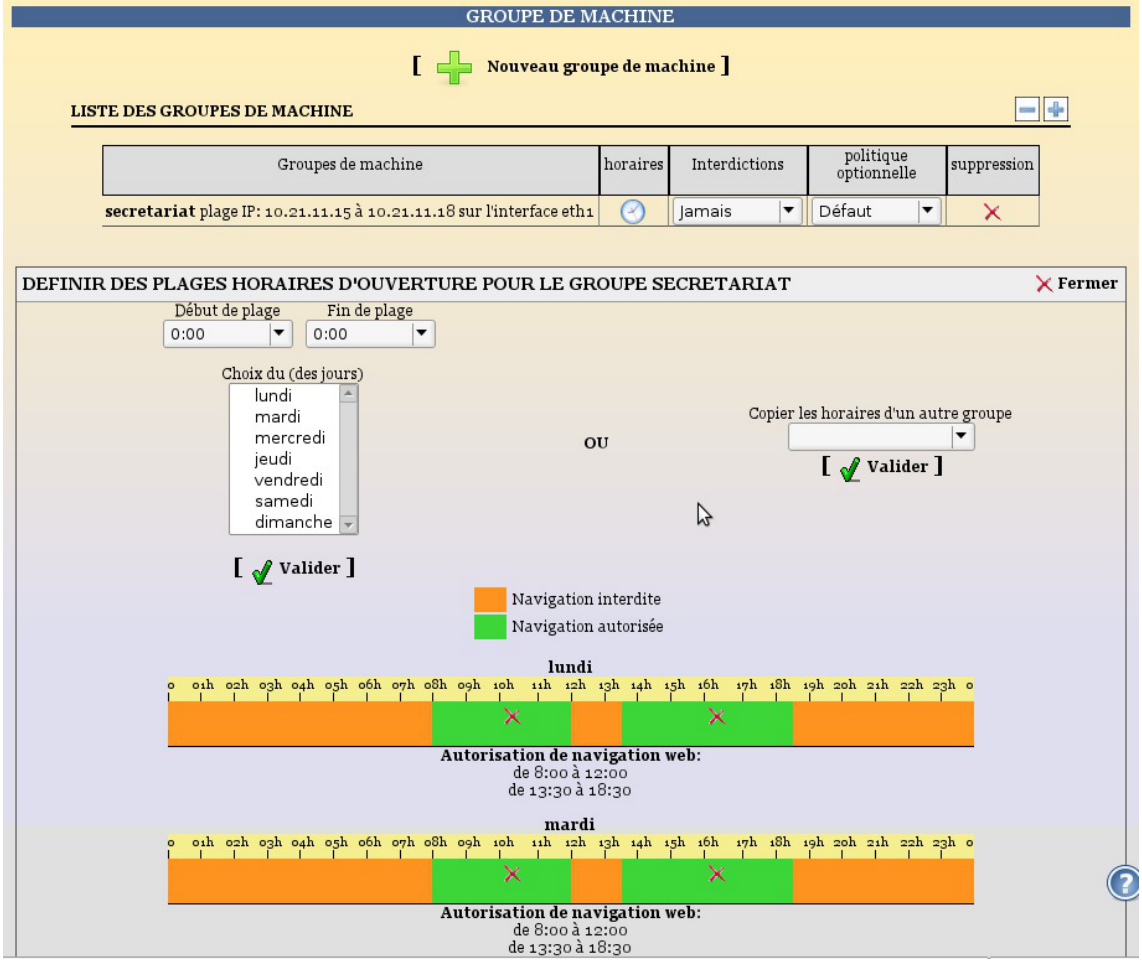
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Remplir le formulaire

Les plages horaires définies s'affichent (la croix permet de supprimer la plage).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Affichage des plages horaires

Sans plage horaire définie, la navigation web est interdite tout le temps

La modification des plages horaires est dynamique.

Si le groupe de machine est interdit de navigation web selon horaires, il est possible de modifier les plages horaires.

Il est aussi possible de copier les horaires depuis un autre groupe de machine.

- choisir le groupe dans la liste ;
- valider.

Interdire l'accès au réseau

Pour interdire tout accès réseau à notre groupe de machine, dans la colonne `Interdictions`, choisir `Toute activité réseau`.

Spécifier une politique de filtrage

Il est possible d'associer une politique de filtrage au groupe de machine. Pour cela choisir la politique dans la colonne `politique optionnelle`.

Certaines politiques de filtrage sont fixes :

- modérateur ;
- interdit ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- mode liste blanche.

D'autres sont configurables :

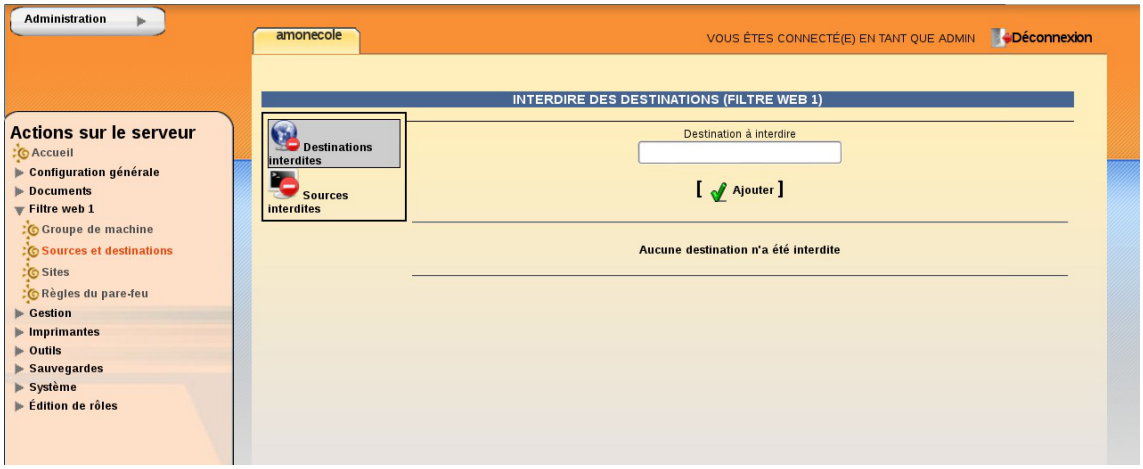
- Défaut ;
- 1 ;
- 2 ;
- 3 ;
- 4.

Supprimer un groupe de machine

Pour supprimer un groupe de machine, cliquez sur la croix en face de votre groupe de machine.

2.11.3. Interdire l'accès à un sous-réseau depuis une interface

Dans l'EAD il est possible d'interdire l'accès à un sous-réseau depuis une interface.



Vue d'ensemble pour l'ajout d'une destination à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Destinations interdites`.

Pour interdire une destination il faut :

- définir le sous-réseau (ou le poste) de destination ;
- choisir l'interface source depuis laquelle interdire l'accès (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné).

Nommage des filtres dans la configuration du filtrage web

> Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.209]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Interdire l'accès au sous-réseau 10.121.11.0/255.255.255.0 depuis l'interface admin (eth1)



Ajout d'une destination à interdire

Soit l'interface eth1 sur la zone de filtre web 1.

- Saisir `10.121.11.0/255.255.255.0` dans `Destinations à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des destinations interdites. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Destinations interdites`.



Suppression d'une destination interdite

- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur `Supprimer`.

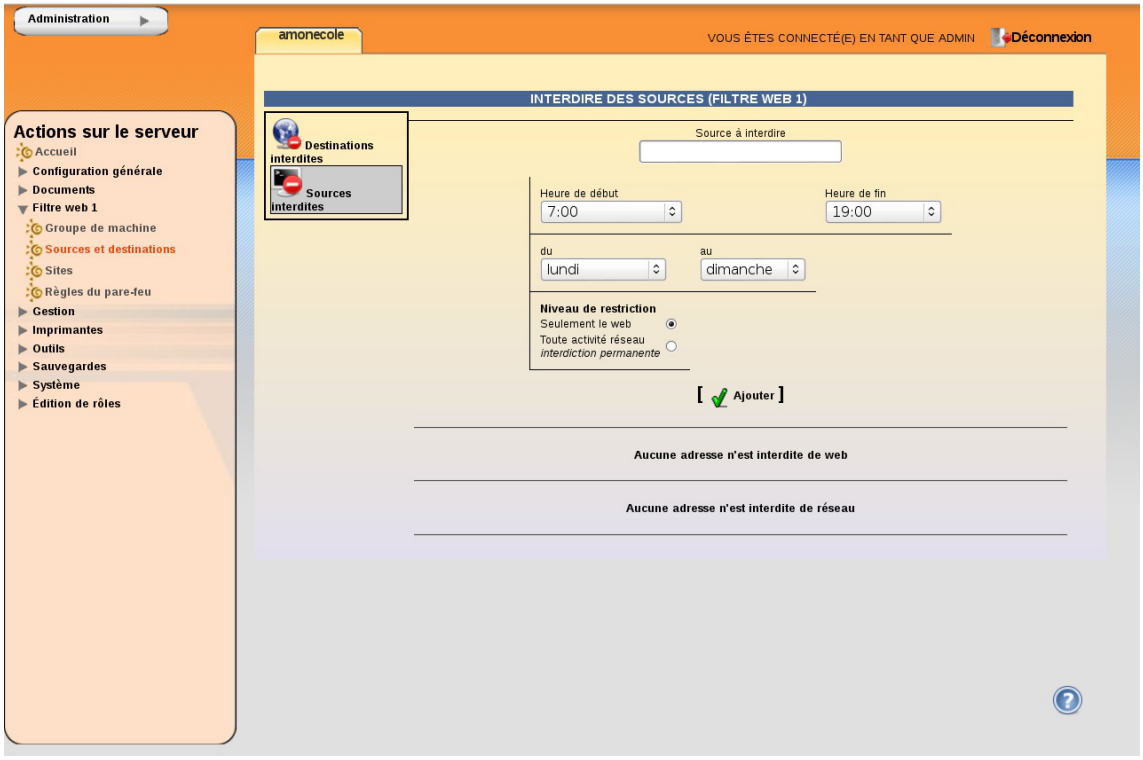
Les destinations interdites sont écrites dans :

`/usr/share/ead2/backend/tmp/dest_interdites<num_instance>.txt`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.11.4. Interdire ou restreindre l'activité d'un sous-réseau

Dans l'EAD il est possible d'interdire l'accès web en fonctions de plages horaires ou d'interdire l'activité à tout un sous-réseau .



Vue d'ensemble pour l'ajout d'une source à interdire

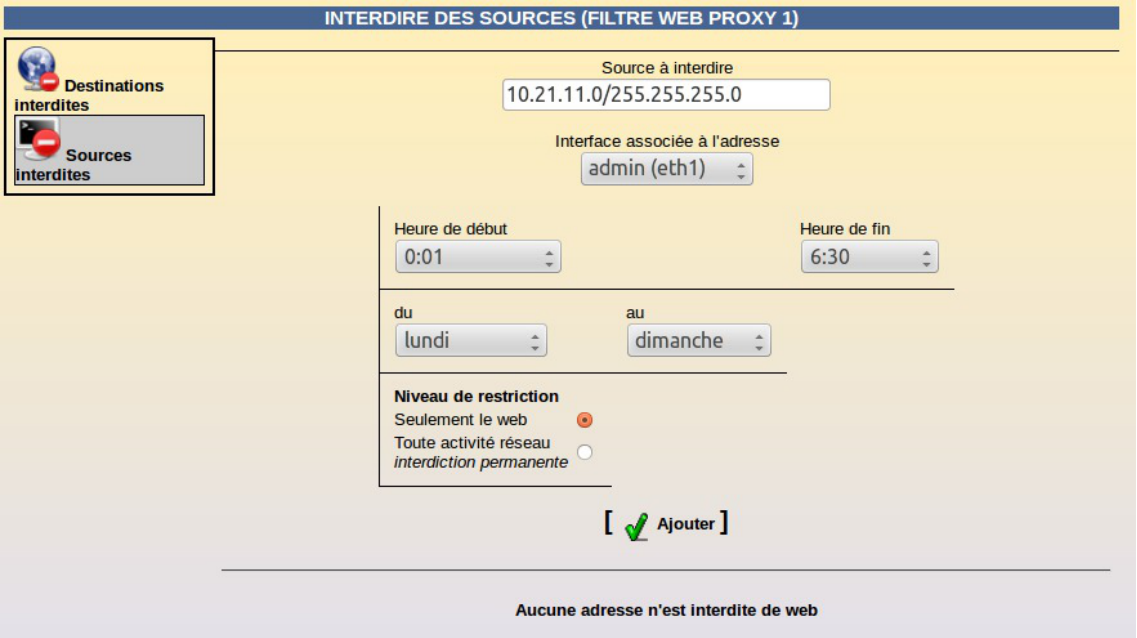
Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.

Les paramètres à saisir sont :

- la `Source à interdire` : le sous-réseau (ou poste) sur lequel les restrictions doivent être appliquées ;
- l'`Interface associée à l'adresse` (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné) ;
- les plages horaires et journalières de la restriction (restriction web uniquement) ;
- le `Niveau de restriction` : web ou réseau.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Interdire l'accès web depuis le sous-réseau 10.21.11.0/255.255.255.0 provenant de l'interface eth1 tous les jours entre minuit et 6 heures du matin



Ajout d'une source à interdire

Soit l'interface eth1 sur la zone de filtre web 1 :

- Saisir `10.121.11.0/255.255.255.0` dans `Source à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Sélectionner `0:01` comme heure de début et `06:30` comme heure de fin ;
- Sélectionner les jours : du lundi au dimanche ;
- Choisir `Seulement le web` comme `Niveau de restriction` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des postes interdits de navigation web. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Suppression d'une source interdite

- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur Supprimer.

Les sources interdites d'accès web sont écrites dans :
/usr/share/ead2/backend/tmp/horaire_ip<num_instance>.txt
Les sources interdites d'accès réseau sont écrites dans :
/usr/share/ead2/backend/tmp/poste_all<num_instance>.txt

Nommage des filtres dans la configuration du filtrage web

Onglet Filtrage web : Configuration du filtrage web [p.209]

2.11.5. Bases de filtres optionnels

Les bases de filtres proposées sur le module Amon sont des copies de celles gérées par l'université de Toulouse 1 Capitole : http://cri.univ-tlse1.fr/blacklists [http://cri.univ-tlse1.fr/blacklists/] .

L'université de Toulouse 1 Capitole diffuse depuis de nombreuses années une liste noire d'URLs, gérée par Fabrice Prigent afin de permettre un meilleur contrôle de l'utilisation d'Internet.

Les bases, publiées sous licence d'utilisation Creative Commons by-sa 4.0 [http://creativecommons.org/licenses/by-sa/4.0/deed.fr] , sont largement utilisées par les écoles et sont également intégrées dans un grand nombre d'outils libres ou commerciaux, en complément d'autres listes.

Les bases sont mises à jour 2 à 3 fois par semaine en fonction des disponibilités du mainteneur, elles peuvent être enrichies grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Ces bases de filtres proposent des catégories avec des listes de domaines et d'URL triés par catégories.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les sites référencés dans les catégories `adult` et `redirector` sont interdits d'office.

Les autres bases de filtres sont activables depuis l'interface EAD.

L'activation se fait :

- par filtre web ;
- par politique de filtrage.

La mise à jour des bases de filtres est lancée automatiquement toutes les nuits

Un rapport de mise à jour est disponible sur la page d'accueil de l'EAD.

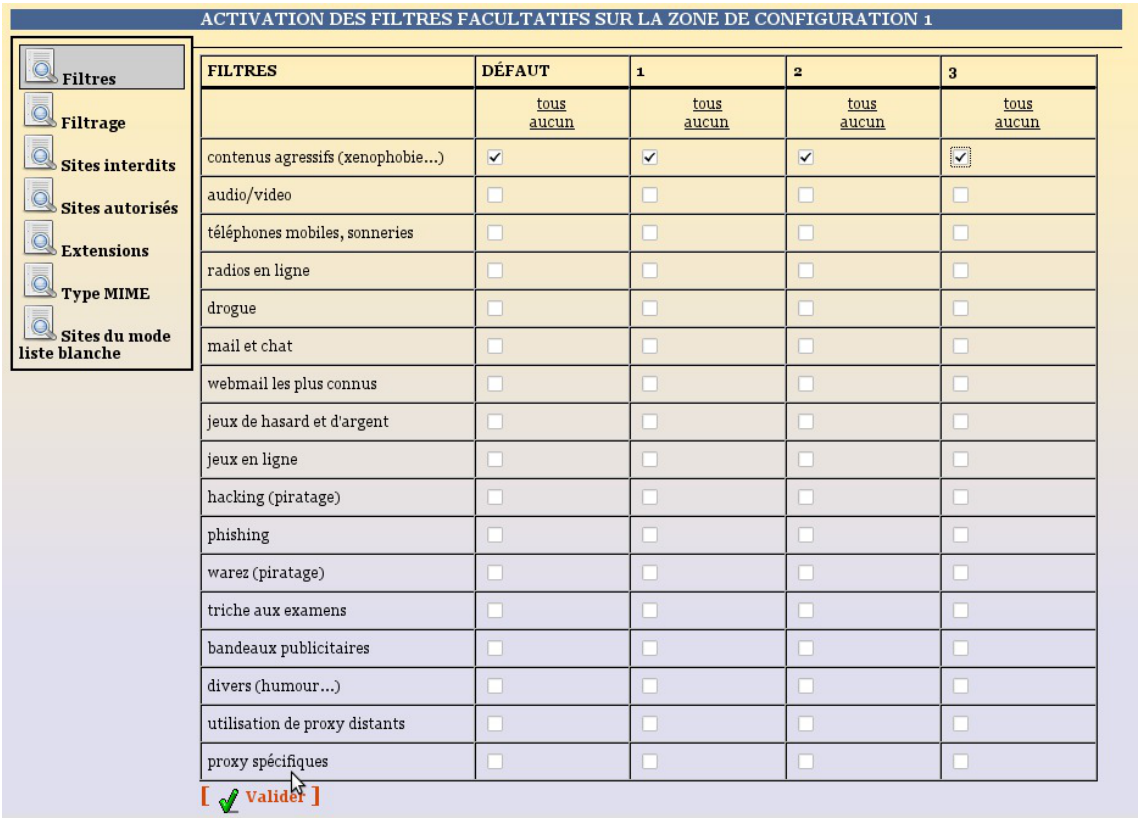


Rapport de mise à jour des bases de filtres

Pour activer la catégorie "agressif" sur toute la zone de configuration 1

Dans `Filtre 1` / `Sites` / `Filtres` :

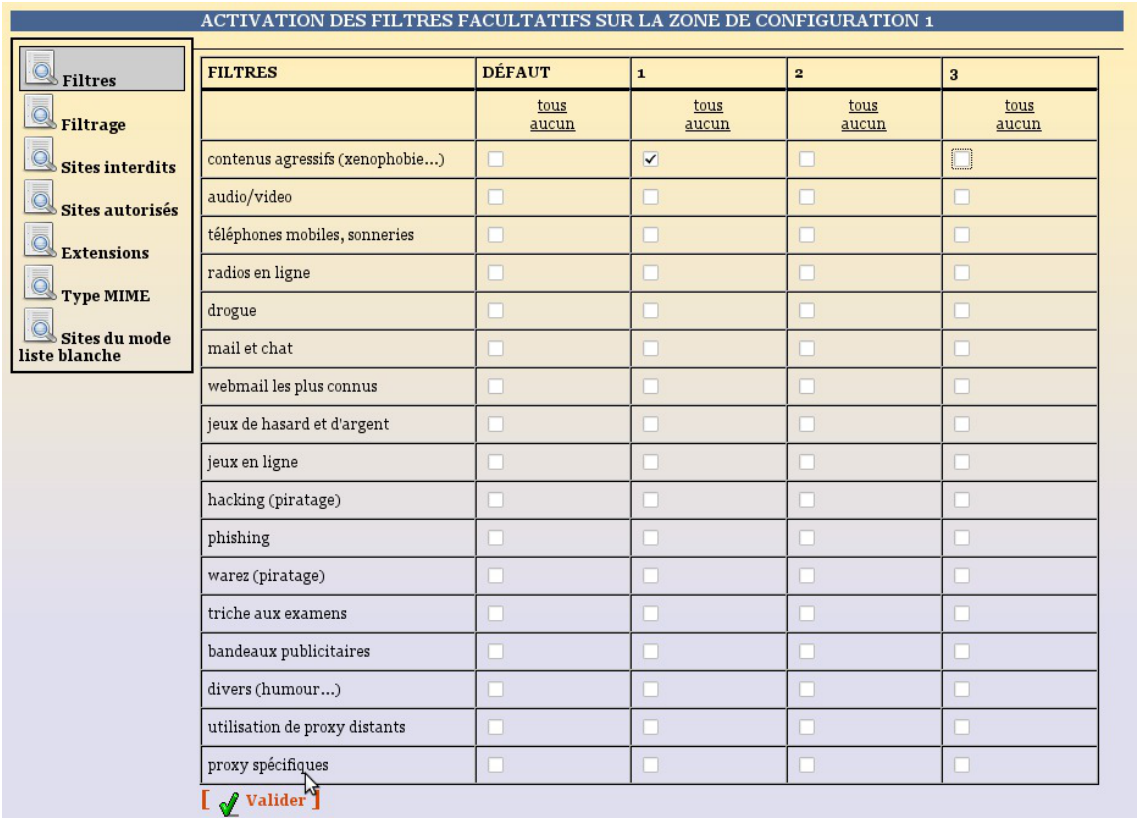
- cocher les quatre cases (pour les quatre politiques de filtrage de la zone 1) ;
- valider.



Activation de filtres optionnels

Pour activer une catégorie seulement pour une politique de filtrage[p.898], seule la case correspondant à la politique doit être cochée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Restreindre l'activation d'un filtre à une politique

La commande suivante permet de forcer la mise à jour les bases de filtrages :

```
/usr/share/eole/Maj-blacklist.sh
```

La liste des bases de filtres d'interdiction gérées sur le module EOLE est fournie par le fichier : /usr/share/ead2/backend/config/filtres-opt.

La modification des filtres optionnels activés impactent les fichiers suivants :

- /var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedsitelist
- /var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedurllist

Sur le module AmonEcole, ces fichiers sont dans le conteneur ***reseau*** .

2.11.6. Filtrage syntaxique

Configuration du filtrage syntaxique

Le module Amon filtre dynamiquement les pages web grâce au filtrage syntaxique[p.890].

Ce système de pondération par mot clef se base sur le fichier /var/lib/blacklists/meta/weighted qui est mis à jour toutes les nuits, à partir des données gracieusement gérées et mises à disposition par l'académie de Rouen.

Dans l'EAD, le filtrage syntaxique peut être :

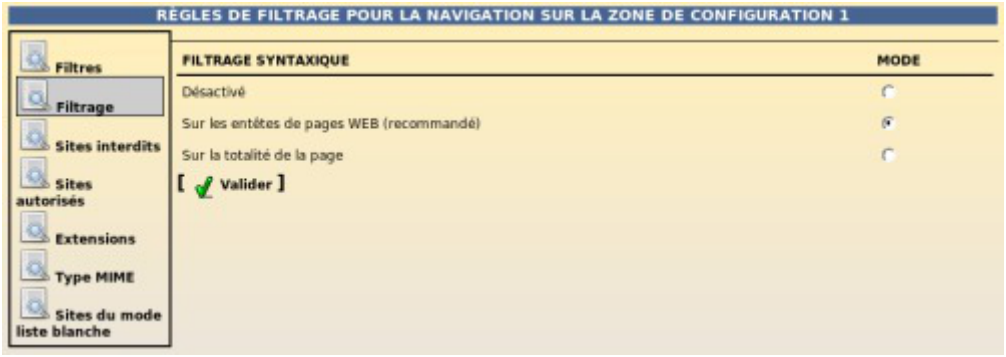
- sur les balises méta[p.884] (par défaut) ;
- sur la page entière ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- désactivé.

Il est possible de régler ce filtrage pour chaque zone de configuration.

Pour modifier la configuration, aller dans Filtre web 1 / Filtrage.



Configuration du mode de filtrage web pour la zone de configuration 1

Le mode de filtrage syntaxique choisi est enregistré dans le fichier :

/var/lib/eole/config/filtrage-contenu<num_instance>

Mode "safe search" dans les moteurs de recherche

Le proxy utilise un système de réécriture des *URL* afin que le mode "safe search" des principaux moteurs de recherche et sites d'hébergement de vidéos soit activé automatiquement.

http://www.google.com/support/websearch/bin/answer.py?answer=510

Certaines fonctionnalités de recherche avancée ont également été désactivées afin de limiter la charge du serveur.

Filtrage PICS

Le filtrage PICS (http://www.w3.org/PICS) ne s'active automatique que si le filtrage syntaxique est configuré `sur la page entière`.

2.11.7. Interdire et autoriser des domaines

Interdire des domaines et des URL

Il est possible de compléter la liste de sites interdits (liste noire[p.892]) en ajoutant des domaines ou des URL sur la liste personnalisée de domaines interdits.

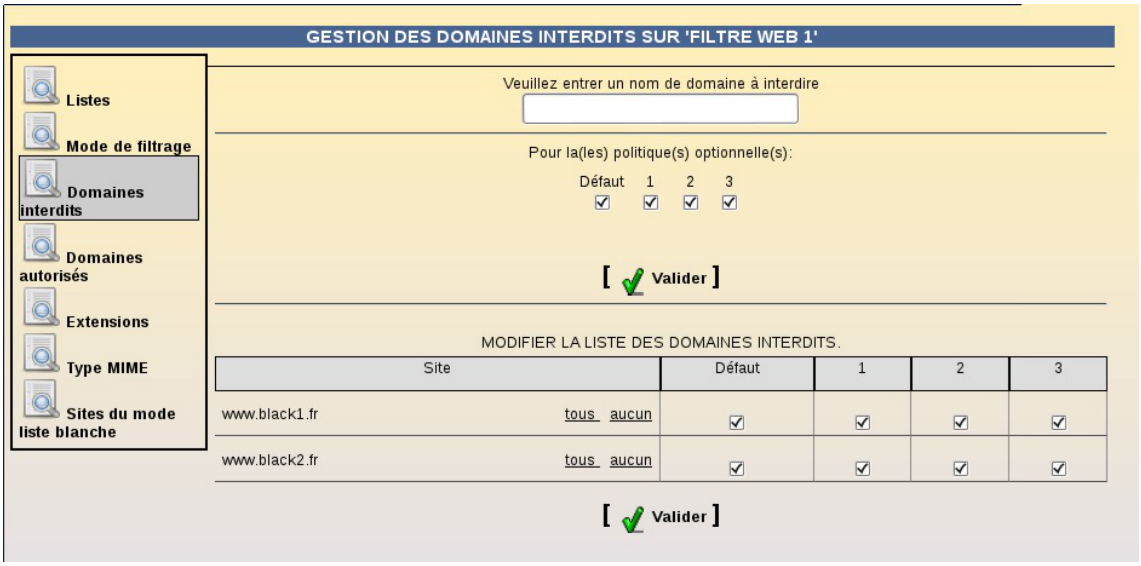
Cette liste est applicable :

- a une zone entière ;
- de manière plus fine sur une seule politique de filtrage.

Le formulaire qui permet d'interdire des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, Filtre web 1 par défaut puis Sites / Domaines interdits.

Nommage des filtres dans la configuration du filtrage web : Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.209]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Interdiction de domaines pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines interdits sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/domains`

Sur un module AmonEcole, ces fichiers sont dans le conteneur `internet`.

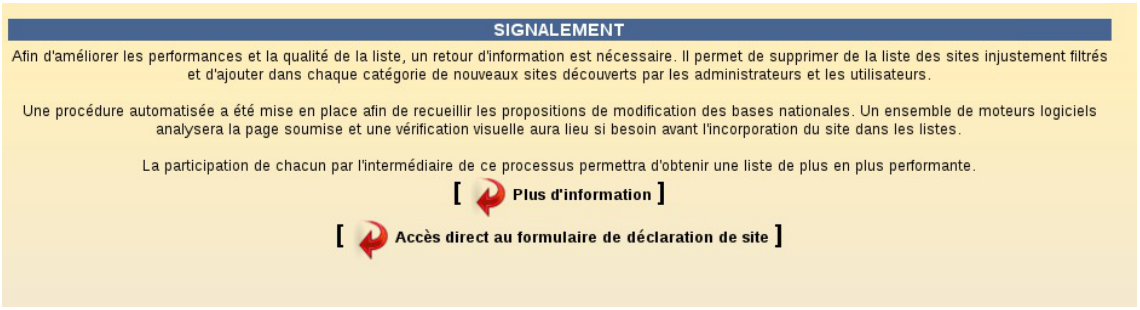
Personnalisations académiques

Des listes de domaines et d'URL peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/var/lib/blacklists/dansguardian<num_instance>/common/domains_acad`
- `/var/lib/blacklists/dansguardian<num_instance>/common/urls_acad`

Il est possible de signaler des domaines à interdire qui amélioreront les performances et la qualité des bases nationales de domaines interdits.

Pour cela, aller dans `Outils` / `Signalements`.



Vue du formulaire de signalement

Une procédure automatisée a été mise en place afin de recueillir les propositions de domaine à interdire dans les bases nationales.

Un ensemble de moteurs logiciels analysera l'URL soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du domaine dans les listes de domaines interdits.

La participation de chacun à ce processus permet d'améliorer les bases nationales et leur performance et ce afin que chacun puisse en bénéficier.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il est également possible de faire une signalement directement auprès de l'université de Toulouse 1 Capitole grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Autoriser des domaines et des URL

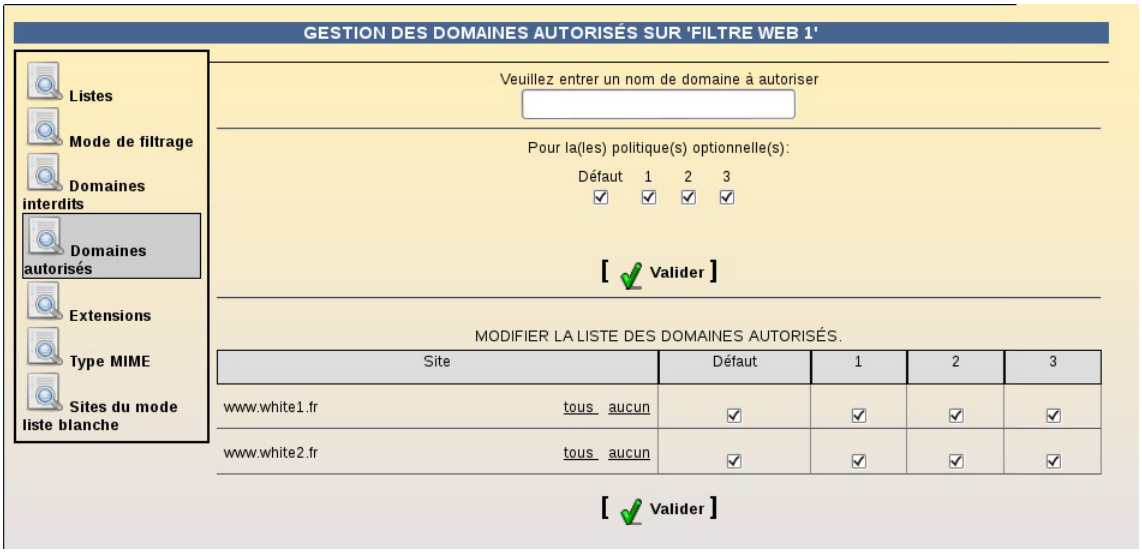
Il est possible de forcer l'autorisation de domaines ou d'URL (liste blanche[p.892]) en les ajoutant à la liste des domaines autorisés.

Cette liste de domaines s'applique :

- sur une zone de filtre web portant le nom du filtre choisi dans l'interface de configuration du module ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans `Filtre web 1` / `Sites` / `Sites autorisés`

Le formulaire qui permet d'autoriser des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, `Filtre web 1` par défaut puis `Sites` / `Domaines autorisés`.



Autorisation de sites pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines autorisés sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/whites`

Sur le module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

2.11.8. Interdire des extensions et des types MIME

Interdire des extensions

Il est possible d'interdire des extensions, ainsi si l'URL de navigation pointe vers un fichier portant cette extension, l'accès sera interdit.

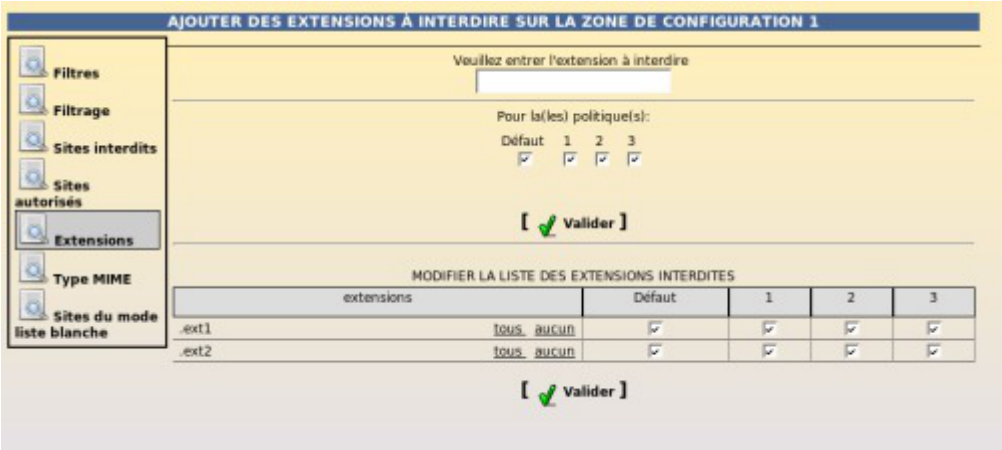
Cette interdiction s'applique :

- sur une zone de configuration ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans Filtre web 1 / Sites / Extensions.



Interdiction d'extensions pour les quatre politiques de la zone de configuration 1

Les extensions interdites sont écrites dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/extensions

Sur AmonEcole, ces fichiers sont dans le conteneur ***reseau***.

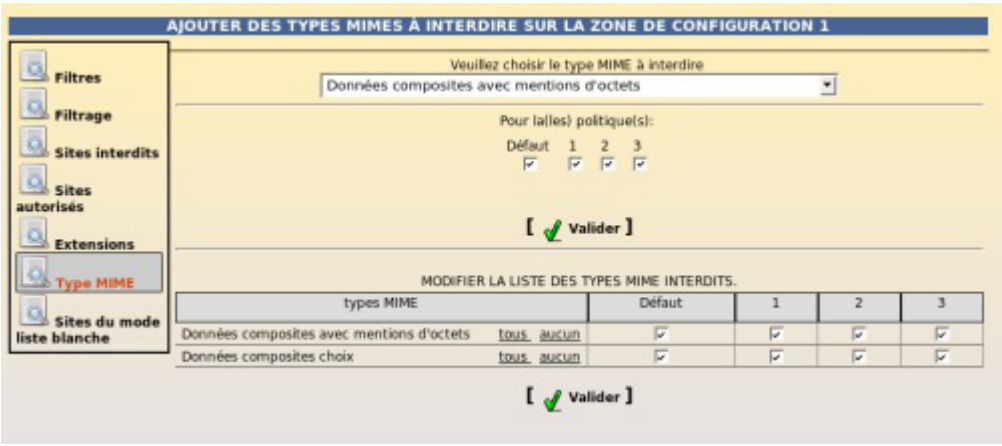
Interdire des types MIME

Il est possible d'interdire des types MIME[p.903]. Cette interdiction fonctionne comme celle des extensions.

Cette interdiction s'applique :

- sur une zone de configuration ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans Filtre web 1 / Sites / type MIME.



Interdiction de types MIME pour les quatre politiques de la zone de configuration 1

Les types MIME interdits sont écrits dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/types_mime

Sur AmonEcole, ces fichiers sont dans le conteneur ***reseau***.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.11.9. Politique liste blanche

Le politique liste blanche[p.892] permet de restreindre la navigation web à une liste de sites.

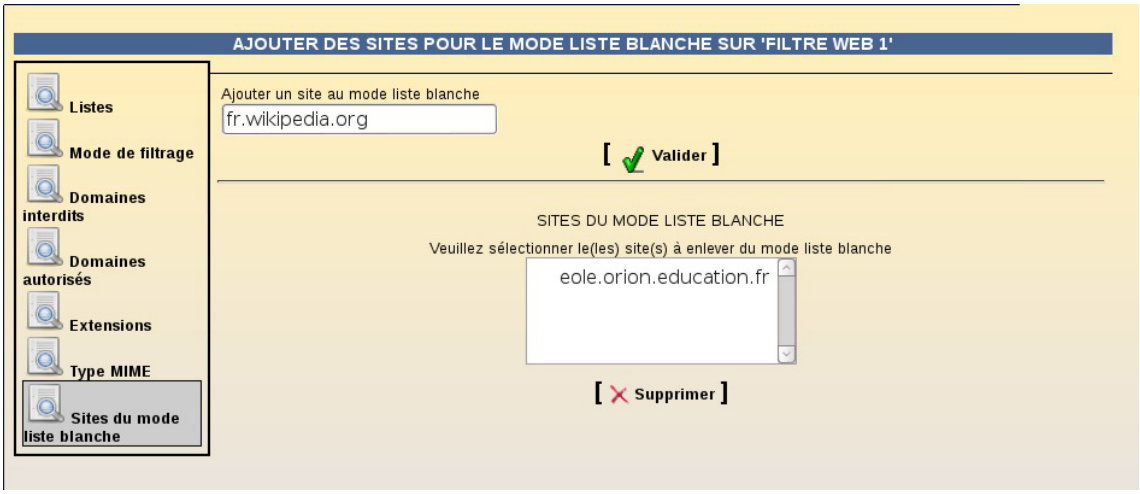
Le principe est "tout est interdit sauf".

Restreindre la navigation au site Wikipédia pour les utilisateurs en mode liste blanche de la zone nommée par défaut "Filtre web 2"

Dans Filtre web 2 / Sites / Sites du mode liste blanche

- ajouter un domaine avec ou sans sous-domaine (exemple fr.wikipedia.org) dans le champ `Ajouter un site au mode liste blanche` ;
- cliquer sur le bouton Valider.

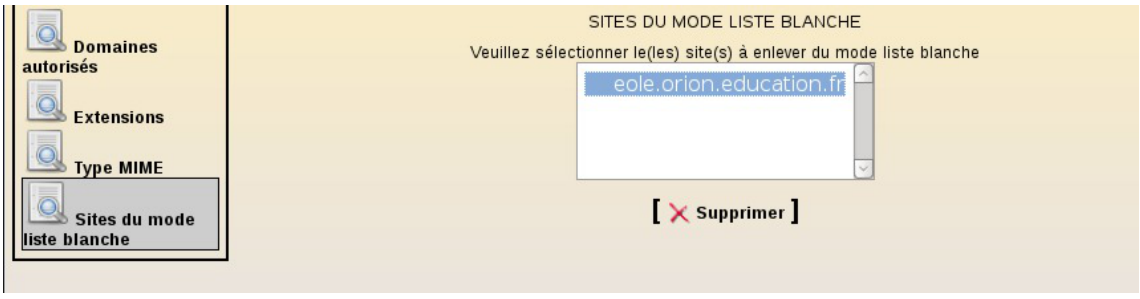
Les utilisateurs et les postes ayant pour politique de filtrage "mode liste blanche" ne pourront naviguer que sur le site ajouté à la liste blanche (exemple Wikipédia).



Ajout d'un site dans la liste blanche

Supprimer un site de la liste blanche

- sélectionner le site dans la liste déroulante `SITES DU MODE LISTE BLANCHE` ;
- cliquer sur la bouton Valider.



Suppression d'un site dans la liste blanche

Les sites de la liste blanche sont écrits dans :

/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/site_liste_blanche

Sur un module AmonEcole, ces fichiers sont dans le conteneur `internet`.

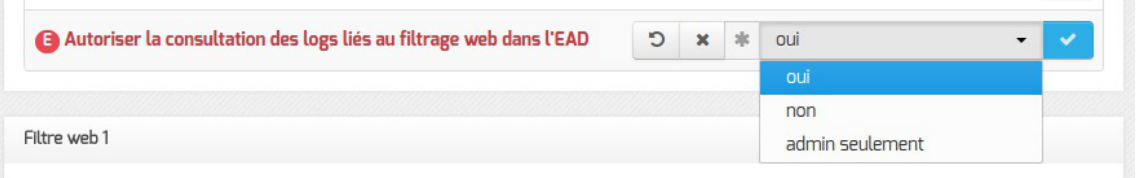
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.12. Observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.888].

Configuration

L'accès à cet outil se paramètre dans l'interface de configuration du module, dans l'onglet expert : `Filtrage web`.

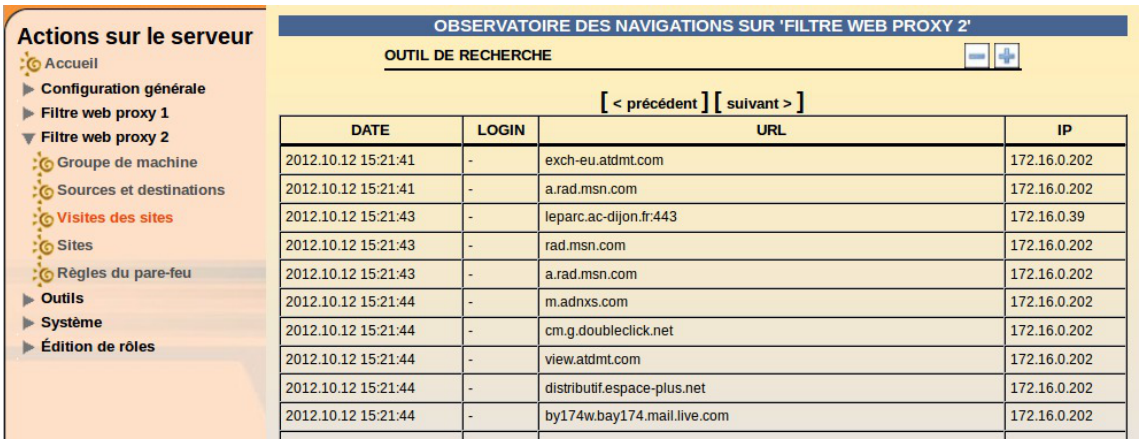


La question `Autoriser la consultation des logs liés au filtrage web dans l'EAD` propose plusieurs options :

- `oui` : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` ;
- `non` : accès interdit pour tout le monde, personne ne voit le lien `Visites des sites` (configuration par défaut) ;
- `admin seulement` : accès autorisé uniquement pour le rôle `admin`.

Consultation

La consultation des visites de sites se fait au travers de l'EAD, menu : `Filtre web X/visites des sites`.



Les noms des menus (ici : `Filtre web proxy` 2) sont modifiables dans l'interface de configuration du module (variables `dansguardian_ead_filtre`1 et `dansguardian_ead_filtre2`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2.13. Outil d'analyse de logs LightSquid

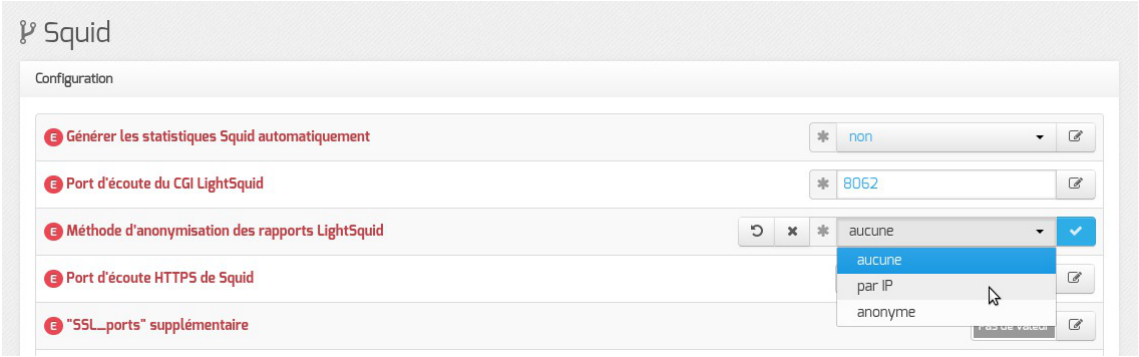
LightSquid est un analyseur de logs pour le proxy/cache Squid[p.902].

Les statistiques générées manuellement ou automatiquement par cet outil sont consultables dans l'interface EAD.

http://lightsquid.sourceforge.net/

Configuration

LightSquid se paramètre dans l'interface de configuration du module, dans l'onglet expert `Squid`. Pour activer la génération automatique des statistiques (toutes les nuits) il faut passer la variable `Générer les statistiques Squid automatiquement` à `oui`. Le port par défaut est 8062.



Paramétrage de Lightsquid

La génération des statistiques proxy peut se faire manuellement, en exécutant la commande `squid_parselogs.sh`.

La méthode d'anonymisation des statistiques générées est également paramétrable :

- `aucune` : aucune anonymisation ;
- `par IP` : n'affiche que les adresses IP ;
- `anonyme` : entièrement anonyme (remplace par un tiret).

Suite à un incident, les statistiques sont celles de la veille, il faut penser à forcer la génération manuellement.

Techniquement, LightSquid fonctionne en mode *cgi* sur un port local (8062 par défaut).

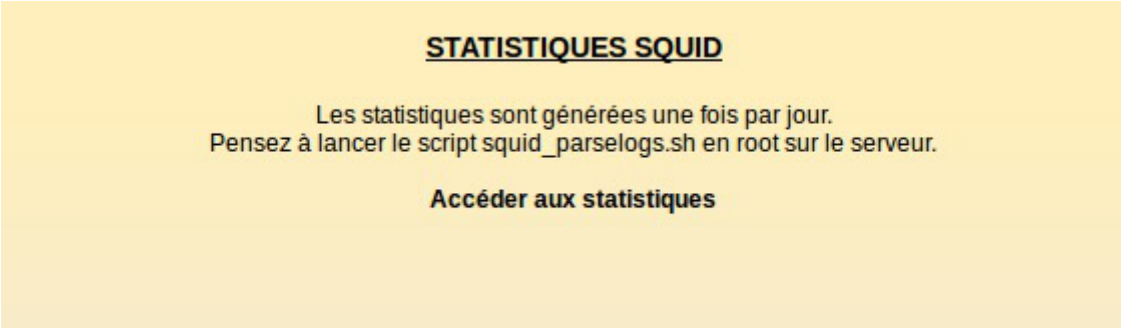
Cela entraîne certaines limitations :

- la ré-authentification nécessaire en mode "pam" ;
- l'accès aux statistiques est impossible depuis un frontend EAD distant.

Consultation

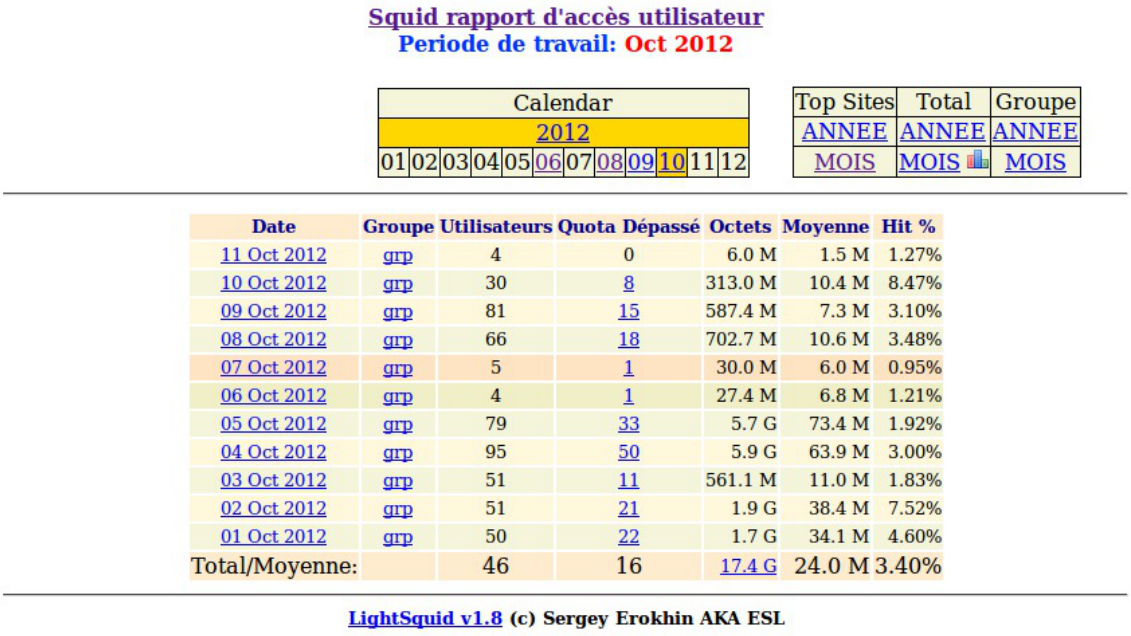
La consultation des statistiques LightSquid se fait au travers de l'EAD, dans le menu `Outils` / `Statistiques proxy`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Pour afficher les statistiques il faut cliquer sur le lien `Accéder aux statistiques`. La navigation se fait dans une nouvelle fenêtre qui demande une authentification. Par défaut, ces statistiques ne sont accessibles que pour le rôle `admin`, un clic sur le bouton `Connexion` sans mot de passe permet de passer à la demande d'authentification pour le compte `root`.

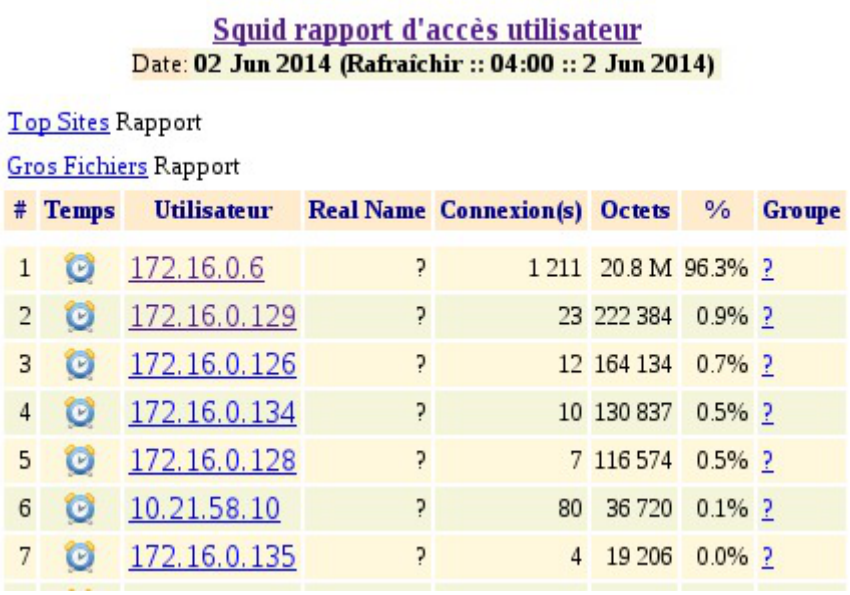
Une fois connecté la vue initiale propose de naviguer dans les statistiques par date (année, jour, mois), par groupe, par quota dépassé.



Consultation au travers de l'EAD

Dans la vue journalière, si la méthode d'anonymisation choisie est par IP, LightSquid n'affiche que les adresses IP utilisées lors de la navigation. Il affiche également le nombre de connexions et le nombre d'octets utilisés. Il est possible d'afficher un rapport sur le top des sites visités et le top des gros fichiers téléchargés dans la journée. Il est possible de repasser à des statistiques journalières par IP.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Squid rapport d'accès utilisateur

Date: 02 Jun 2014 (Rafraîchir :: 04:00 :: 2 Jun 2014)

Top Sites Rapport

Gros Fichiers Rapport

#	Temps	Utilisateur	Real Name	Connexion(s)	Octets	%	Groupe
1		172.16.0.6	?	1 211	20.8 M	96.3%	?
2		172.16.0.129	?	23	222 384	0.9%	?
3		172.16.0.126	?	12	164 134	0.7%	?
4		172.16.0.134	?	10	130 837	0.5%	?
5		172.16.0.128	?	7	116 574	0.5%	?
6		10.21.58.10	?	80	36 720	0.1%	?
7		172.16.0.135	?	4	19 206	0.0%	?

Vue journalière des statistiques

Dans la vue des statistiques journalières par IP, toutes les adresses visitées par l'utilisateur s'affichent avec le nombre de connexions et les octets consommés.



Squid rapport d'accès utilisateur

Utilisateur: 172.16.0.6 (?)

Groupe: ?

Date: 02 Jun 2014

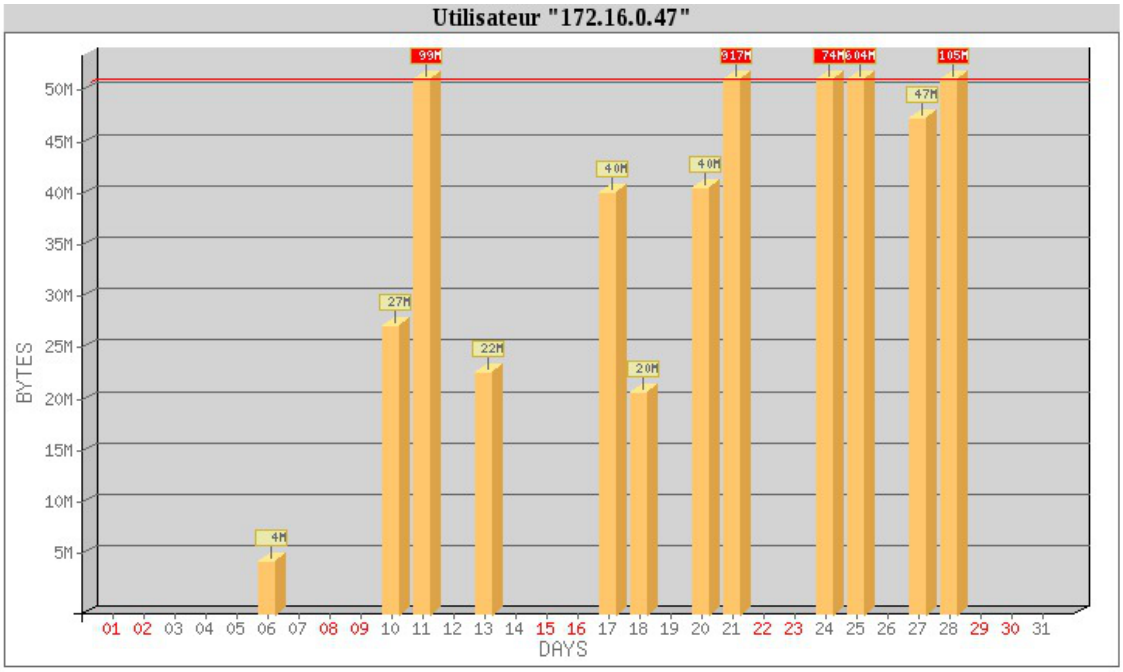
User download "Big Files"

Total					
			20.8 M		
#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	osce106-ilspn25-p.activeupdate.trendmicro.com	28	19.6 M	19.6 M	94.3%
2	osce106-ilspn25wr-p.activeupdate.trendmicro.com	16	869 227	20.5 M	3.9%
3	92.51.156.70	1 152	340 194	20.8 M	1.5%
4	cyberlib.crdp-poitiers.org:443	14	25 142	20.8 M	0.1%
5	ctldl.windowsupdate.com	1	337	20.8 M	0.0%
Total			20.8 M		

Vue journalière par IP des statistiques

Dans la vue par mois, un clic sur la consommation total des Octets donne un classement de la consommation d'octets par adresse IP. Dans le tableau affiché, un graphe mensuel de la consommation d'octets par adresse IP est disponible.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Graphe mensuel de la consommation d'octets pour une adresse IP

3. Les clients GNU/Linux

3.1. Principe du client GNU / Linux

L'objectif est d'obtenir des postes de travail sous GNU / Linux dont l'authentification et le montage des répertoires de travail se fait sur les modules Scribe ou Horus.

Authentification PAM / LDAP

Un système GNU / Linux peut aller chercher dans différents endroits pour authentifier des utilisateurs. Par défaut il utilise le fichier `/etc/passwd`.

Cependant on peut lui ajouter d'autres sources de données.

Le module PAM[p.897] va permettre de vérifier, à la demande d'un service, la validité d'une authentification à un service d'authentification tel que LDAP[p.892] ou Kerberos[p.892].

Aussi, il ne suffit pas de modifier la configuration de PAM pour que cela fonctionne. En général, il faut également installer un service qui va pouvoir activer ce pont entre PAM et le service d'authentification :

- `libpam-ldap` permet à PAM d'utiliser LDAP pour l'authentification
- `libpam-krb5` permet de faire le pont entre PAM et Kerberos pour l'authentification

L'authentification sur les postes clients GNU / Linux va principalement se baser sur 2 services :

- NSS (Name Service Switch, NS Switch) est une bibliothèque générique de résolution de nom.
  Elle permet :
  - d'authentifier les utilisateurs via le LDAP ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

  - d'obtenir les informations des utilisateurs à travers le LDAP.
- nslcd est utilisé pour lier l'authentification LDAP et de récupérer ses informations

  nslcd est un démon qui va faire des requêtes LDAP pour les processus locaux qui veulent faire utilisateur, groupe et autres recherches de nommage (NSS) ou de faire l'authentification des utilisateurs, d'autorisation ou de modification de mot de passe (PAM)
- nscd qui fera un cache et vous évitera des problèmes liés à la performance et au coupure du réseau.

NSS

Les informations telles que les noms d'utilisateurs, groupes et autres, stockées dans des fichiers situés dans `/etc/`, vont être fournies grâce à NSS (Name Service Switch) à l'aide du serveur LDAP du module Scribe.

Un serveur LDAP peut gérer les bases de données suivantes :

- aliases (alias de messagerie, ignoré par la plupart des démons de courrier) ;
- ethers (adresses Ethernet) ;
- group (groupes d'utilisateurs) ;
- hosts (noms et adresses d'hôte) ;
- netgroup (groupes d'hôtes et d'utilisateurs pour le contrôle d'accès) ;
- networks (informations concernant le réseau) ;
- passwd (comptes des utilisateurs) ;
- protocols (protocoles réseau) ;
- rpc (base de données des numéros de programmes rpc) ;
- services (liste des services réseau Internet) ;
- shadow (informations sécurisées sur les comptes utilisateurs).

Les données gérer dans l'annuaire LDAP du module Scribe sont :

- passwd (comptes des utilisateurs) ;
- group (groupes d'utilisateurs) ;
- shadow (informations sécurisées sur les comptes utilisateurs).

#fixme : à compléter

Il existe actuellement deux paquets disponibles pour configurer les requêtes NSS via LDAP :

- `libnss-ldap`

  plus mature mais plus complexe, `libnss-ldap` a quelques problèmes connus au démarrage
- `libnss-ldapd`

  plus simple, amélioré, mais moins mature

Le choix entre les deux dépend des besoins, ici `libnss-ldapd` a été retenu.

nslcd

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

nslcd (local LDAP name service daemon) est un démon qui va faire des requêtes LDAP pour les processus locaux basés sur un fichier de configuration simple.

nslcd utilise nscd pour mettre en cache les informations et permet de limiter les requêtes au serveur LDAP.



Le durée du cache peut être réglé en modifiant les valeurs `xxx-time-to-live` dans le fichier `/etc/nscd.conf`, les valeurs par défaut suffise dans la plupart des cas.

Montage des répertoires partagés

Il existe actuellement 2 méthodes pour mettre en place des montages distants depuis le client GNU/Linux ver le module Scribe :

- méthode basée sur NFS ;
- méthode basée sur les montages Samba.

Méthode basée sur NFS

La méthode basée sur le partage de fichiers NFS[p.894] est valable aussi bien pour des clients GNU/Linux existants que pour la mise en œuvre des clients légers Eclair (serveur de clients légers).

Pour fonctionner, le client GNU/Linux a besoin que le service NFS soit installé et activé sur le module Scribe.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.



Tous les comptes locaux ont un accès au module Scribe.

#fixme

Méthode basée sur Samba

Cette solution basée sur SMB[p.901] est valable pour des clients GNU/Linux.

Un fichier de configuration doit être ajouté sur le module Scribe pour la prise en charge des partages.

Pour fonctionner, le client GNU/Linux doit pouvoir monter des partitions distante par SMB avec l'utilitaire `cifs-utils.`

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.



Cette méthode crée autant de comptes sur l'ordinateur client qu'il y a de comptes dans l'annuaire du module Scribe.

#fixme

Intégration dans l'environnement graphique

Un certains nombres de modification permette une intégration plus forte dans l'environnement graphique.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Appliquer des règles

Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil.

3.2. Configuration des comptes utilisateurs sur le serveur

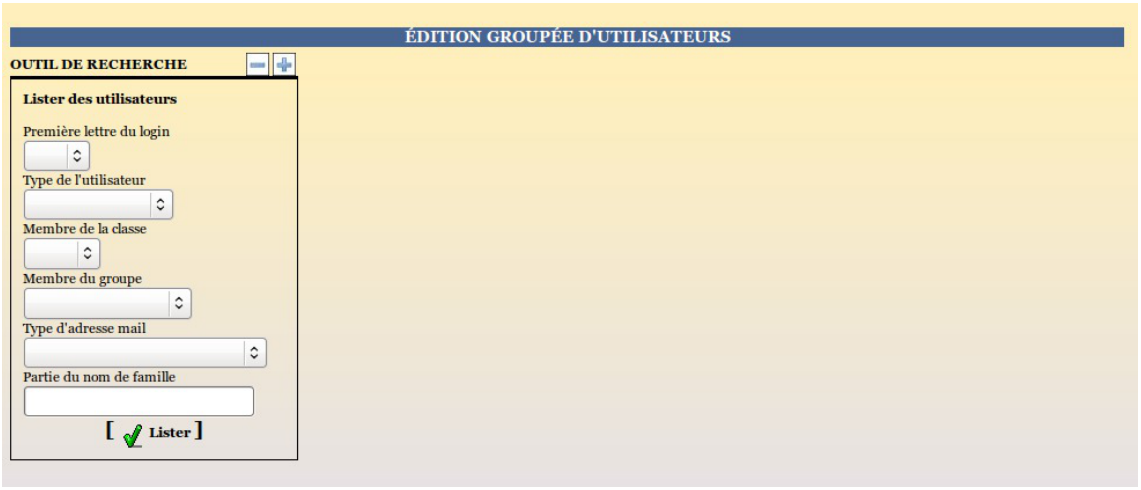
Configuration des comptes utilisateurs

Les utilisateurs du module Scribe doivent avoir l'interpréteur de commande activé.

Cette manipulation se fait au moment de l'importation des utilisateurs sur le module Scribe.

Si l'importation a été faite, il est possible de faire une édition groupée des utilisateurs devant avoir un interpréteur de commande activé.

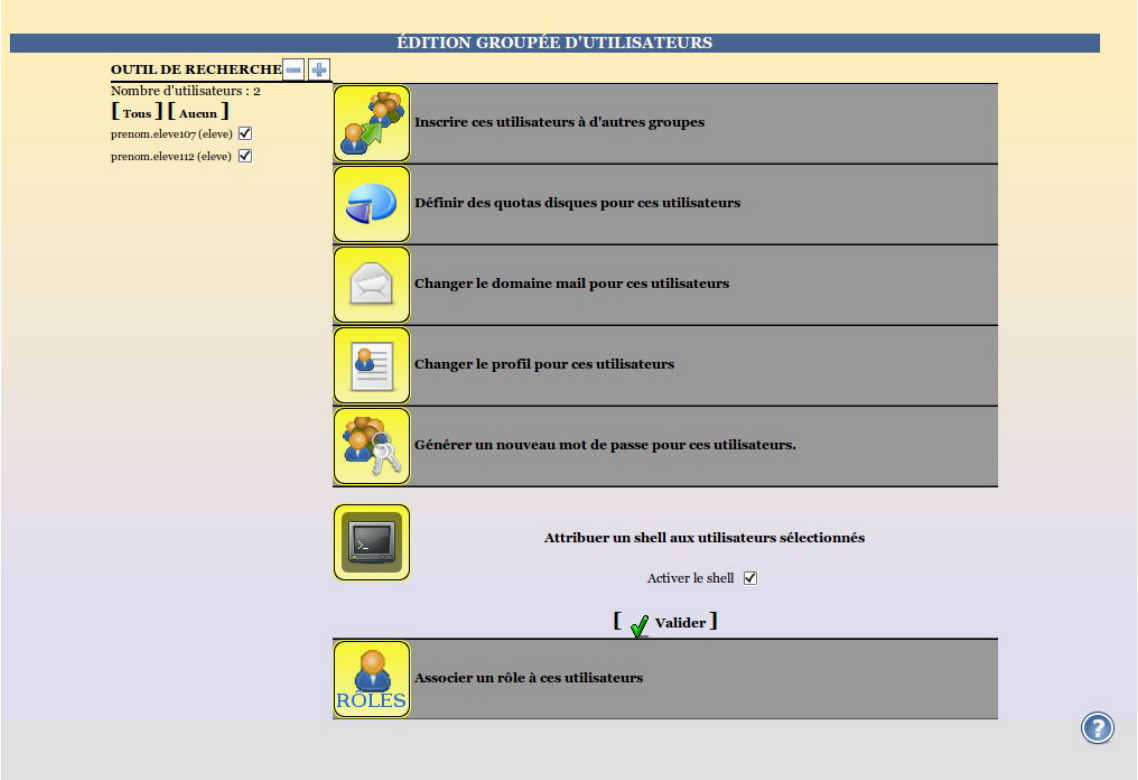
Dans l'EAD → Gestion → Édition groupée.



Sélectionner les critères de recherche et cliquer sur le bouton Lister.

Décocher les utilisateurs en trop si besoin et cliquer sur Modifier le shell associé à ces utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'option ☑ Activer le shell est cochée, cliquer alors sur le bouton Valider.

Une fenêtre affiche `Le shell des utilisateurs sélectionnés a bien été modifié`.

Activation massive du shell en ligne de commande

La commande suivante permet d'activer le shell de tous les utilisateurs en une seule fois :

```
# ldapsearch -x cn=DomainUsers|grep memberUid:|awk '{print $2}' | while read i
> do
> echo "mise en place du shell pour $i"
> smbldap-usermod -s /bin/bash $i
> done
```



Commande en une seule ligne :

```
# ldapsearch -x cn=DomainUsers|grep memberUid:|awk '{print $2}' | while read i ; do echo "mise en place du shell pour $i"; smbldap-usermod -s /bin/bash $i; done
```

Ne pas forcer le changement de mot de passe

Dans le cas d'une création de nouveaux comptes utilisateurs, il ne faut pas utiliser la fonctionnalité `forcer le changement de mot de passe à la première connexion` se trouvant dans les outils d'importation des comptes et de l'édition groupée de l'EAD. La connexion du client serait impossible car il ne gère pas le changement de mot de passe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

#fixme

Si vous utilisez l'authentification par proxy dans votre établissement il faut obligatoirement spécifier l'utilisateur/mot de passe sous GNU/Linux (L'authentification transparente du proxy utilise un mécanisme interne de Microsoft).

3.3. Authentification LDAP depuis le client GNU / Linux

La procédure suivante propose l'intégration d'un client Ubuntu 15.04 vivid à jour :

```
root@pclinux:/home/eole# apt-get update && apt-get upgrade
```

L'adresse du poste client est obtenu par DHCP et le nom de machine du module Scribe est résolue.

Configuration de l'authentification LDAP

http://wiki.debian.org/fr/LDAP/NSS

Installation de libnss-ldapd

L'installation de libnss-ldapd se fait à l'aide de la commande `apt-get install` :

```
root@pclinux:/home/eole# apt-get install libnss-ldapd
```

Des paquets supplémentaires seront installés : `ldap-utils` `libpam-ldapd` `nscd` `nslcd` `nslcd-utils`



La configuration de `libnss-ldapd` et `nslcd` est interactive en fin d'installation.

Pour une configuration manuelle avec édition des fichiers de configuration il faut ajouter l'option -y à la commande `apt-get install` :

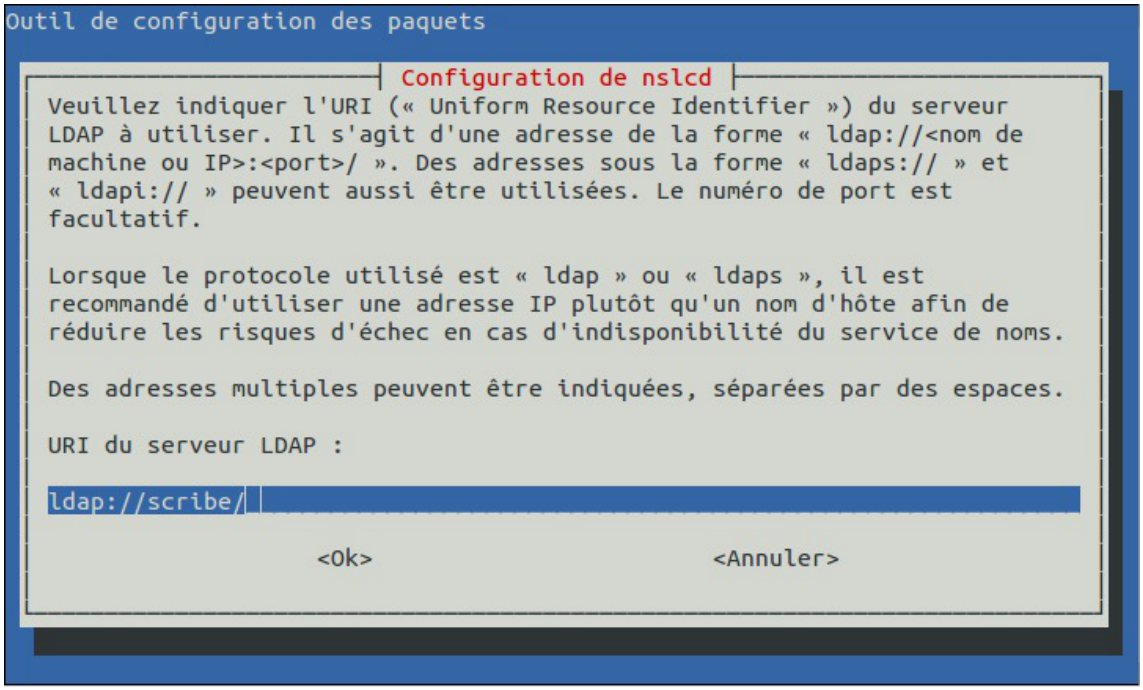
```
root@pclinux:/home/eole# apt-get -y install libnss-ldapd
```

Configuration interactive

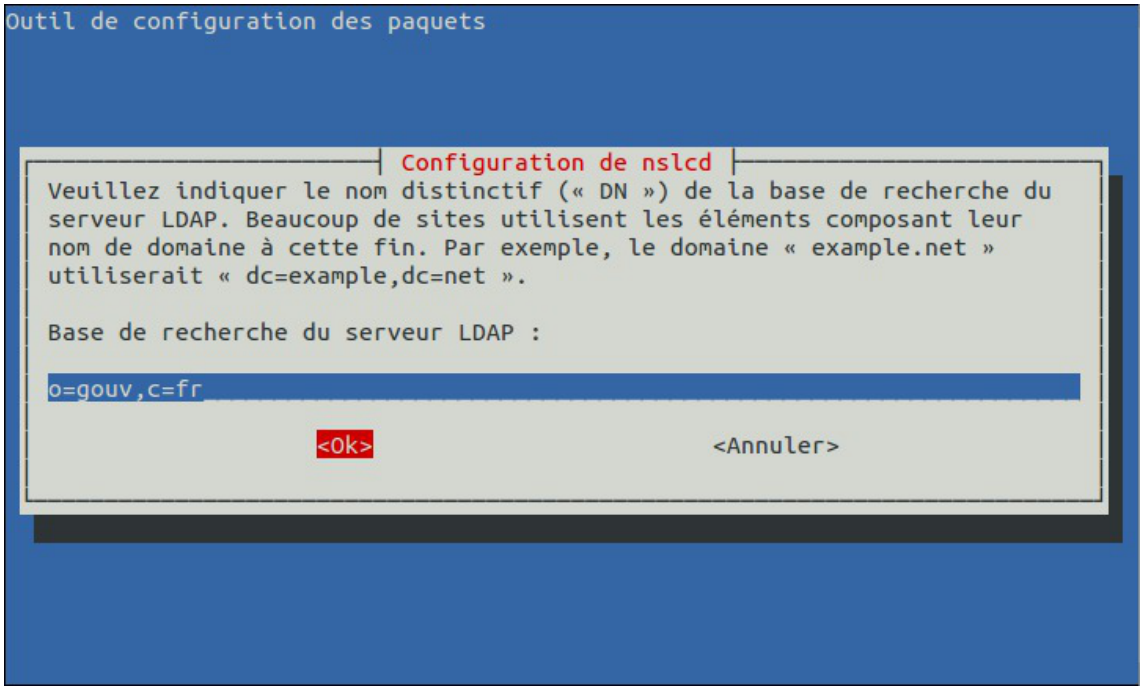
Si l'installation 0 question n'a pas été adoptée 3 écrans permettent, à la fin de l'installation , de configurer le service :

- configuration de `nslcd` : saisir l'adresse ou le nom de machine du module Scribe, il ne faut pas omettre le / à la fin, le port peut être spécifié ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

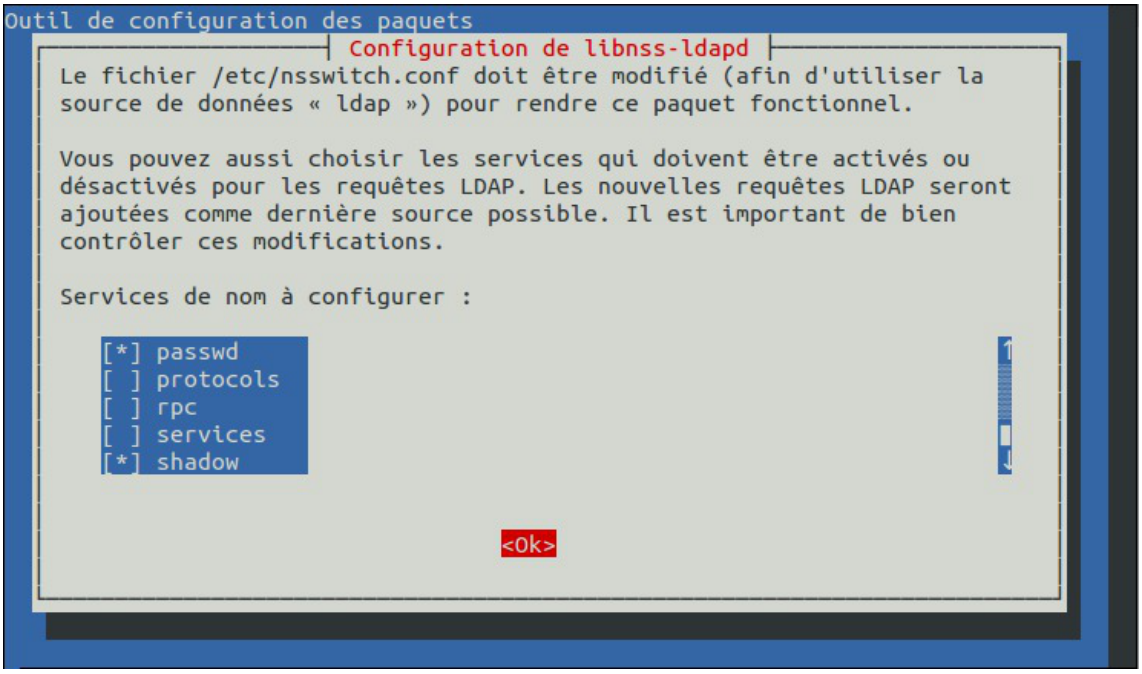


- configuration de `nslcd` : saisir le nom distinctif de la base de recherche, saisir `o=gouv, c=fr` ;



- configuration `nsswitch` des ressources à chercher dans l'annuaire LDAP : cocher `passwd`, `group` et `shadow` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Configuration manuelle

La configuration peut-être réalisée ou adaptée en éditant les fichiers suivants :

- /etc/nslcd.conf

```
# The location at which the LDAP server(s) should be reachable.
uri ldap://scribe/
# The search base that will be used for all queries.
base o=gouv,c=fr
```

- /etc/nsswitch.conf

```
passwd: compat ldap
group: compat ldap
shadow: compat ldap
```

Le mode compat est destiné à travailler avec NIS[p.894].

Test de liaison avec l'annuaire LDAP :

root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr -x uid=utilisateurScribe

```
root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr
-x uid=test.prof
uid: test.prof
uidNumber: 10034
gidNumber: 10001
homeDirectory: /home/t/test.prof
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaSID: S-1-5-21-1756604377-3768680913-3336469871-21068
sambaPrimaryGroupSID: S-1-5-21-1756604377-3768680913-3336469871-21003
sambaProfilePath: \\scribe\netlogon\profil
sambaHomePath: \\scribe\test.prof\perso
sambaHomeDrive: U:
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: administrateur
objectClass: ENTPerson
objectClass: ENTAuxEnseignant
objectClass: radiusprofile
cn: test prof
sn: prof
givenName: test
displayName: test prof
gecos: test prof
LastUpdate: 20151107
ENTPersonLogin: test.prof
ENTPersonJointure: ENT
ENTPersonProfils: enseignant
ENTPersonNomPatro: prof
codecivilite: 1
ENTPersonSexe: M
personalTitle: M.
intid: 12
radiusTunnelType: VLAN
radiusFilterId: Enterasys:version=1:policy=Enterprise User
radiusTunnelMediumType: IEEE-802
mail: test.prof@etb1.ac-test.fr
mailHost: localhost
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
mailDir: /home/mail/test.prof/
typeadmin: 0
loginShell: /bin/bash
sambaAcctFlags: [U]
sambaPwdLastSet: 1447316673
sambaPwdMustChange: 1447316673
shadowLastChange: 16751
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
```

```
root@pclinux:/home/eole# getent passwd utilisateurScribe
utilisateurScribe:x:10034:10001:test prof:/home/u/utilisateurScribe:/bin/bash
root@pclinux:/home/eole#
```



```
root@pclinux:/home/eole# getent passwd test.prof
test.prof:x:10034:10001:test prof:/home/t/test.prof:/bin/bash
root@pclinux:/home/eole#
```

Tester la prise en compte des utilisateurs

ssh test.prof@10.1.2.52

test.prof@10.1.2.52's password:

Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-15-generic x86_64)

3.4. Problèmes d'authentification rencontrés et solutions

Pendant le débogage nscd peut masquer les problèmes en fournissant des entrées de son cache, il est donc préférable de stopper nscd (démon de Name Service Caching) avec la commande suivante :

```
# service nscd stop
```

Reconfigurer libnss-ldapd et nslcd

Si la configuration post installation ne convient pas il est possible de relancer la configuration de `libnss-ldapd` et de `nslcd` avec la commande `dpkg-reconfigure`.

```
# dpkg-reconfigure libnss-ldapd
# dpkg-reconfigure nslcd
```



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Utilisation de la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure libnss-ldapd
```

et

```
# dpkg-reconfigure nslcd
```

Problème de cache

Un ou plusieurs mots de passe de compte utilisateurs ont été changé sur le module Scribe. Il faut rafraîchir le cache de `nscd`.

Nettoyer le cache

Nettoyer le cache avec la commande `nscd` :

```
# nscd -i passwd
# nscd -i group
# nscd -i shadow
```

Relancer le service permet également de vider le cache :

```
# service nscd restart
```

Utiliser l'outil nss-updatedb

Le paquet `nss-updatedb` fourni la commande `nss_updatedb` qui permet de créer des bases de données de type Berkeley DB stockant les données équivalentes aux `passwd` et `group` du NSS. Il faut l'invoquer régulièrement afin de maintenir à jour ces bases de données.

Cela permet à un utilisateur du domaine de se reconnecter à sa session lorsqu'il est hors ligne.

Installer l'outil `nss-updatedb` :

```
root@pclinux:/etc# apt-get install nss-updatedb
Lecture des listes de paquets... Fait
```

Utiliser manuellement l'outil `nss-updatedb` :

```
root@pclinux:/etc# nss_updatedb ldap
passwd... done.
group... done.
```

Il faut informer le système qu'il peut utiliser ces bases de données comme source pour `passwd`, `group` et `shadow` en ajoutant `db` aux entrées respectives du fichier `/etc/nsswitch.conf` :

```
passwd: compat ldap db
group: compat ldap db
shadow: compat ldap db
```

Désactiver le cache de nscd

Il est possible de désactiver le cache dans le fichier de configuration `/etc/nscd.conf` en ajoutant les options désirées :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
enable-cache passwd no
enable-cache group no
enable-cache shadow no
```

Pour en savoir plus, consulter le manuel à l'aide de la commande `man` :

```
# man nscd.conf
```

Perte de l'authentification

Il n'est plus possible de se connecter depuis le poste client ni avec le gestionnaire de connexion (display manager) ni en ligne de commande dans un tty.



Il faut s'assurer du bon fonctionnement du module Scribe avec la commande `diagnose`.

Il faut ensuite tester si le service LDAP distant répond :

```
root@pclinux:/home/eole# ldapsearch -h scribe:389 -b o=gouv,c=fr -x uid=utilisateurScribe
```

la commande `getent` :

```
# getent passwd test.prof
```

Si elle ne renvoie plus rien il faut relancer le service `nscd` avec la commande suivante :

```
# service nscd restart
```

Activer et consulter les logs de nscd

L'activation des logs pour nscd se fait dans le fichier `/etc/nscd.conf`.

Il faut dé-commenter la ligne `logfile /var/log/nscd.log` et passer la variable `debug-level` à `1` ou plus de verbosité.

Pour plus d'information il faut consulter la page de manuel :

```
# man nscd.conf
```

Pour rendre effectif le changement il faut relancer le service :

```
root@pclinux:/home/eole# service nscd restart
```

La consultation des journaux se fait à l'aide de la commande `tail` :

```
root@pclinux:/home/eole# tail -f /var/log/nscd.log
```

Pour lancer le service libnss-ldapd en mode débogage

Arrêter `nscd`

```
# service nscd stop
```

Arrêter le démon de `libnss-ldapd`

```
# service nslcd stop
```

Lancer le démon de `libnss-ldapd` en mode débogage

```
# nslcd -d
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3.5. Partages avec NFS

La méthode basée sur le partage de fichiers NFS[p.894] est valable aussi bien pour des clients GNU/Linux existants que pour la mise en œuvre des clients légers Eclair (serveur de clients légers).

Pour fonctionner, le client GNU/Linux a besoin que le service NFS soit installé et activé sur le module Scribe.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Configuration du partage de fichiers sur le module Scribe

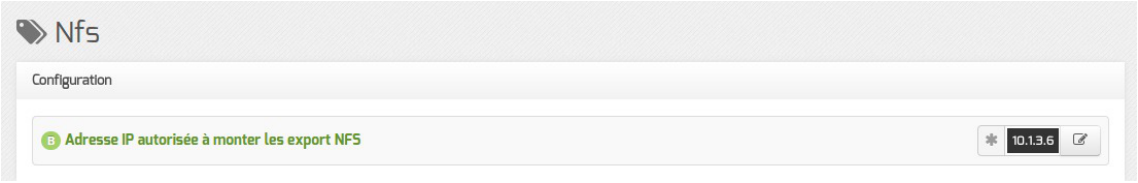
Sur le module Scribe il faut installer le paquet `eole-nfs` :

```
# apt-eole install eole-nfs
```

L'installation du paquet ajoute :

- un nouveau service dans l'onglet `Services` de l'interface de configuration du module `Activer le serveur NFS` est par défaut à `oui`
- et un nouvel onglet nommé `Nfs` est disponible

Il faut ensuite autoriser le module Eclair ou les clients Linux à monter les export NFS du module Scribe. Pour cela, se rendre dans l'interface de configuration du module Scribe, dans l'onglet `Nfs` et saisir l'adresse IP (Interface-0) du module Eclair ou les adresses des clients GNU/Linux dans le champ `Adresse IP autorisée à monter les exports NFS`.



Il faut ensuite procéder à la reconfiguration du module Scribe avec la commande `reconfigure`.

Test manuel de montage

Pour le support du système de fichiers NFS sur le client il faut installer le paquet `nfs-common` :

```
# apt-get install nfs-common
```

Pour tester la prise en charge il est possible de procéder à un montage manuelle d'une partition distante :

```
# mdkir /mnt/montage
# mount -t nfs -o auto,nouser,rsize=8192,wsize=8192,timeo=14,intr,acl,nolock,async scribe:/home/ /mnt/montage
```

Pour démonter la partition :

```
# umount /mnt/montage
```

Si le test de montage renvoie la ligne suivante c'est qu'il faut autoriser l'adresse IP du client dans l'onglet Nfs du module Scribe :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
mount.nfs: access denied by server while mounting scribe:/home/
```

Configuration pour le montage à la connexion

Pour permettre à PAM de monter des volumes pour une session utilisateur il faut installer la bibliothèque libpam-mount :

```
root@pclinux:/home/eole# apt-get install libpam-mount
```

#fixme

Voir aussi...

eole-nfs

3.6. Partages avec Samba

Cette solution basée sur SMB[p.901] est valable pour des clients GNU/Linux.

Un fichier de configuration doit être ajouté sur le module Scribe pour la prise en charge des partages.

Pour fonctionner, le client GNU/Linux doit pouvoir monter des partitions distante par SMB avec l'utilitaire `cifs-utils.`

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Paramétrer le module Scribe

Pour que les partages fonctionnent sur un module Scribe 2.4 il faut ajouter le fichier de configuration `/etc/samba/conf.d/partages-linux.conf` avec le contenu suivant :

```
[eclairng]
path = %H/.ftp
comment = montage linux
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config_eole/
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ce fichier permet de partager le répertoire `.ftp` de l'utilisateur qui lui contient les liens symboliques vers les répertoires de l'utilisateur.

Pour que le changement soit pris en compte sur le module il faut reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Test manuel de montage

Le protocole SMB/CIFS permet un partage de fichiers multiplate-forme avec des systèmes Linux.

Le paquet `cifs-utils` fournit des utilitaires pour gérer les montages des systèmes de fichiers en réseaux CIFS.

```
# apt-get install cifs-utils
```

Pour tester la prise en charge il est possible de procéder à un montage manuelle d'une partition distante :

```
# mdkir /mnt/montage
```

Récupérer l'UID de l'utilisateur

```
root@pclinuxlxde:/home/eole# getent passwd test.prof
test.prof:x:10034:10001:test prof:/home/t/test.prof:/bin/bash
root@pclinuxlxde:/home/eole#
```

Montage manuel

```
root@pclinux:/home/eole# mount -t cifs //scribe/perso /mnt/montage -o noexec,nosetuids,mapchars,cifsacl,serverino,nobrl,iocharset=utf8,user=test.p
Password for test.prof@//scribe/perso: ******
root@pclinux:/home/eole#
```

Pour démonter la partition :

```
# umount /mnt/montage
```

Si le test de montage renvoie la ligne suivante c'est qu'il faut autoriser l'adresse IP du client dans l'onglet Nfs du module Scribe :

```
mount.nfs: access denied by server while mounting scribe:/home/
```

Configuration pour le montage à la connexion

Pour permettre à PAM de monter des volumes pour une session utilisateur il faut installer la bibliothèque `libpam-mount` :

```
root@pclinux:/home/eole# apt-get install libpam-mount
```

Il faut ensuite éditer le fichier de configuration `/etc/security/pam_mount.conf.xml` et ajouter les volumes à monter dans la rubrique `<!-- Volume definitions -->` du fichier.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les points de montage sont créés automatiquement.

```
<volume user="*" fstype="cifs" server="scribe" path="professeurs" mountpoint="/media/professeurs" />
<volume user="*" fstype="cifs" server="scribe" path="perso" mountpoint="~/Documents" />
<volume user="*" fstype="cifs" server="arg1" path="eclairng" mountpoint="/media/serveur-scribe" />
```

```
<volume user="*" fstype="cifs" server="scribe" path="commun" mountpoint="/media/commun" />
<volume user="*" fstype="cifs" server="scribe" path="groupes" mountpoint="/media/groupes" />
```

Il faut également ajouter les paramètres des volumes à monter dans la rubrique `<!-- pam_mount parameters: Volume-related -->` du fichier.

```
<cifsmount>mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o "noexec,nosetuids,mapchars,cifsacl,serverino,nobrl,iocharset=utf8,u
OPTIONS)"</cifsmount>
```

#fixme

Empêcher ou personnaliser la création des dossiers Musique, Vidéo, Téléchargement,...

`xdg-user-dirs` est un outil de gestion qui définit un lot de répertoires standards prêts à l'emploi (Documents, Images, Musique, Téléchargements, Vidéos notamment) dans le répertoire `/home` de l'utilisateur.

Il est possible d'empêcher la création par le système des répertoires par défaut de l'utilisateur (Musique, Vidéo, Téléchargement,...).
Pour cela il faut éditer le fichier `/etc/xdg/user-dirs.conf` et de passer `enabled=True` à `False`.

Il est possible de personnaliser les répertoires par défaut de l'utilisateur (Musique, Vidéo, Téléchargement,...).
Pour cela il faut éditer le fichier `/etc/xdg/user-dirs.defaults` et commenter les répertoires non souhaités et inversement.

Voir aussi...

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

eole-fichier-primaire [p.810]

3.7. Intégration dans un environnement graphique

Le gestionnaire de connexion, DM pour display manager en anglais, peut-être différent d'une distribution GNU / Linux à une autre :

- LightDM pour Unity, qui se lit light display manager ;
- GDM pour GNOME, qui se lit gnome display manager ;
- KDM pour KDE qui se lit KDE display manager ;
- XDM pour X Window qui se lit X display manager ;
- Entrance pour Enlightenment ;
- LDM, gestionnaire d'affichage spécialement écrit pour LTSP.

LightDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir lightdm comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure lightdm
```

Selon la version de la distribution le fichier de configuration qui permet de personnaliser le comportement de LightDM peut être différent :

- `/etc/lightdm/lightdm.conf` sur Ubuntu inférieure à 14.04 ;
- `/usr/share/lightdm/lightdm.conf.d/50-xubuntu.conf` sur Ubuntu supérieure égal 14.04 ;
- `/usr/share/lightdm/lightdm.conf.d/60-xubuntu.conf` sur Ubuntu supérieure à 14.04.



La modification du fichier de configuration nécessite le redémarrage du service :

```
# service lightdm restart
```

Activer la touche NumLock (VerrNum)

Un paquet supplémentaire peut être installé pour gérer la touche NumLock (VerrNum) :

```
# apt-get install numlockx
```

Pour sa prise en charge dans LightDM ajouter la ligne suivante dans la rubrique `[SeatDefaults]` :

```
greeter-setup-script=/usr/bin/numlockx on
```

Exécution d'un script à la déconnexion

Créer un script `/etc/lightdm/logoffscript.sh` avec les actions à réaliser à la déconnexion de l'utilisateur.

Pour sa prise en charge dans LightDM ajouter la ligne suivante dans la rubrique `[SeatDefaults]` :

```
session-cleanup-script=/etc/lightdm/logoffscript.sh
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

démontage et suppression du répertoire personnel

```
umount -f $HOME
# suppression du répertoire personnel local à chaque déconnexion,
# sauf pour le compte administrateur local
# if [ $USER != adminprof ]&&[ $USER != adminskel ]; then
# if [ $USER != adminprof ]&&[ $USER != adminskel ]&&[ $USER != prof ]&&[ $USER != invite ]; then
if [ $USER != adminprof ]; then
# on vérifie qu'il n'y a plus de répertoire monté dans /home/$USER/ mount | grep "/home/"| grep $USER ; if [ $? = 0 ]; then exit 1,; fi
rm -r $HOME
fi
exit 0
```

Autres possibilités

Il est également possible de :

- masquer tous les utilisateurs
  `greeter-hide-users=true`
- permettre la saisie manuelle
  `greeter-show-manual-login=true`

Documentation LightDM

- http://wiki.ubuntu.com/LightDM
- http://doc.ubuntu-fr.org/lightdm

KDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir KDM comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure kdm
```

GDM

Si plusieurs gestionnaire de connexion sont installés il est possible de choisir GDM comme celui par défaut avec la commande `dpkg-reconfigure` :

```
# dpkg-reconfigure gdm
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

3.8. Installation de Gaspacho

Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil.

Installation

Pour installer le service Gaspacho sur le module Scribe il faut installer le paquet `eole-gaspacho` :

```
# apt-eole install eole-gaspacho
```

L'installation du paquet ajoute un nouveau service dans l'onglet `Services` de l'interface de configuration du module. `Activer Gaspacho` est par défaut à `oui` et un nouvel onglet nommé `Gaspacho` est disponible en mode expert.

Celui-ci vous permet de choisir qui détermine les entrées DNS via la variable `Utiliser des entrées DNS des clients plutôt que le nom fourni par l'agent` qui par défaut est à `non`. Par défaut, les entrées DNS sont donc imposées par l'agent Gaspacho.



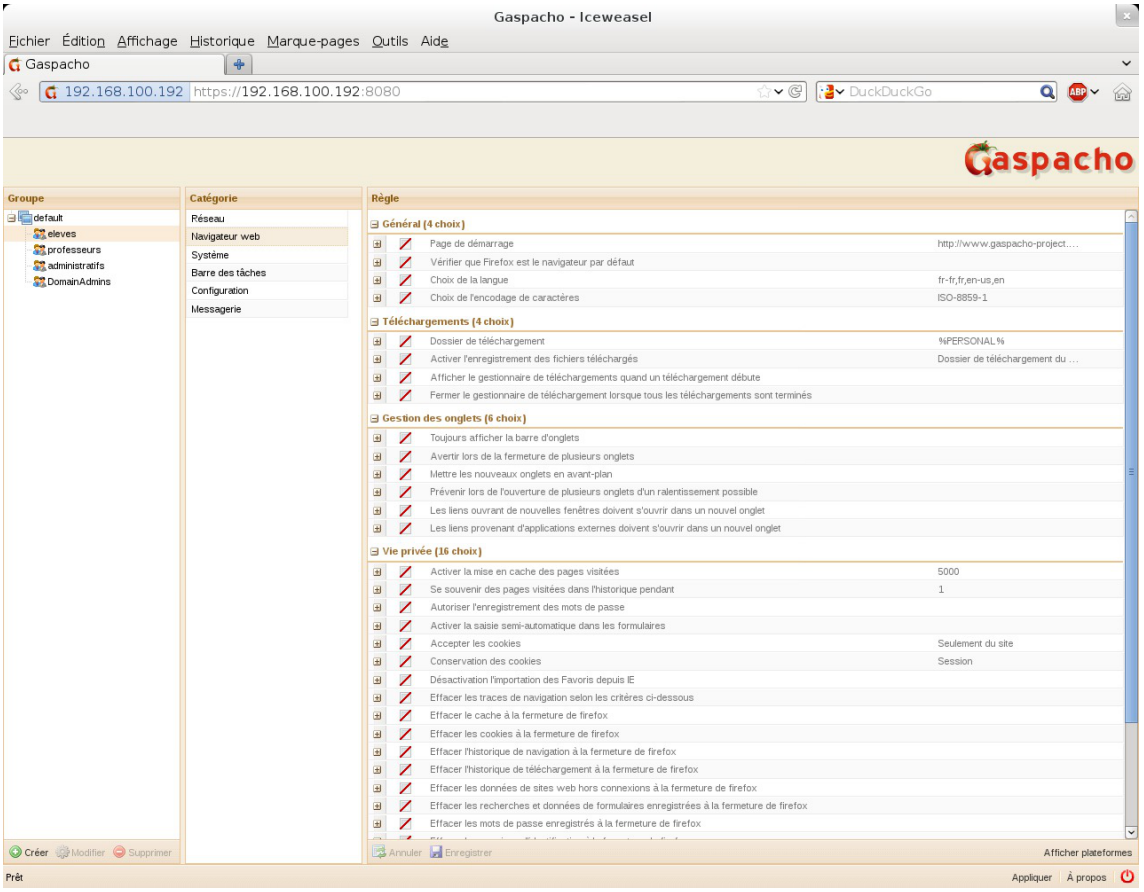
Les changement des paramètres de configuration nécessite la reconfiguration du module à l'aide de la commande `reconfigure`.

Accès à l'application

Gaspacho est accessible sur le module à l'adresse `https://<adresse_serveur>:8080`.

Le compte à utiliser est le compte `admin` du module Scribe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue d'ensemble de l'application Gaspacho

Plus d'informations sur Gaspacho sont disponibles dans la documentation dédiée et sur le site du projet : http://www.gaspacho-project.net/.

Gaspacho côté client

#fixme

3.9. Scripts d'intégration pour GNU / Linux

Des scripts utilisant Samba permettent d'intégrer des clients GNU/Linux au domaine Scribe, ils sont à installer sur chacun des clients.

Une adaptation sur le module Scribe en version supérieure ou égale à 2.4 est nécessaire pour le bon fonctionnement des partages.

Le logiciel Gaspacho permet d'appliquer des configurations sur les postes clients.

Les scripts d'intégration

Les scripts et leurs adaptations sont le résultat du travail de plusieurs personnes :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

Deux méthodes sont possibles pour récupérer les scripts :

- scripts versionnés ;
- archive par version de GNU/Linux.

Dans les deux cas les scripts seront à personnaliser et à modifier en fonction du contexte et de la version GNU/Linux des clients.

Scripts versionnés avec Git

Les scripts versionnés sont mis à disposition par la Délégation Académique au Numérique Éducatif de Lyon à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Ces scripts permettent d'intégrer des clients Gnu/Linux dans un environnement EOLE Scribe.

Les clients supportés sont les suivants :

- Ubuntu (Environnement Unity) 12.04 et 14.04
- Xubuntu (Environnement XFCE) 14.04
- Lubuntu (Environnement LXDE) 14.04
- Linux (Environnement Mate ou Cinammon) Mint 17 ou 17.1 ou 17.2

Pour récupérer l'ensemble du projet versionnés, il faut avoir Git d'installer sur son poste :

```
$ git clone https://github.com/dane-lyon/clients-linux-scribe.git
$ cd clients-linux-scribe/
```

La procédure d'utilisation est disponible dans le fichier `README.md` du projet ou à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Scripts archivés

Les différentes archives de scripts d'intégration proposées par les contributeurs concernent des versions de GNU/Linux et des environnements de bureau différents.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Exemple d'intégration avec les scripts archivés

La procédure d'écrite ci-dessous a été testée avec un poste client Xubuntu

Elle utilise l'archive qui concerne l'intégration d'une station Debian 8 proposée par par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

La procédure pour Debian 8 est entièrement décrite et mise à disposition :
http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_debian_scribe-1.pdf

Installer les scripts sur le poste GNU/Linux

#fixme

Paramétrer le module Scribe

Pour que les partages fonctionnent sur un module Scribe 2.4 il faut ajouter le fichier de configuration `/etc/samba/conf.d/partages-linux.conf` avec le contenu suivant :



```
[eclairng]
path = %H/.ftp
comment = montage linux
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config eole/
```


Ce fichier permet de partager le répertoire `.ftp` de l'utilisateur qui lui contient les liens symboliques vers les répertoires de l'utilisateur.



Pour que le changement soit pris en compte sur le module il faut reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Résolution de problème

La commande `getent passwd` permet de savoir si les utilisateurs LDAP ont été ajouté aux utilisateurs

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

locaux :

```
root@ejabber:~# getent passwd prenom.prof26
prenom.prof26:x:10437:10000:Prenom PROF26:/home/p/prenom.prof26:/bin/false
root@ejabber:~#
```

3.9.1. Paramétrage des clients GNU/Linux

3.9.1.a. Clients Debian

Client Jessie (Debian 8)

Pour l'intégration d'une station Debian 8 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_debian_scribe-1.pdf

Scripts d'intégration

Des scripts d'intégration sont mis à disposition à l'adresse suivante par Jean-François Mai, du collège République de Cholet : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Le script suivant s'occupe uniquement de l'intégration : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-v1.0c.tar.gz

Le script suivant installe un système avec un environnement minimal MATE et enfin s'occupe de l'intégration : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-mate-core-v1.0b.

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom du script.sh
```



Beaucoup d'informations sont présentes dans le fichier `readme.txt` de l'archive.

Problème des partages sur un serveur EOLE Scribe 2.4

Pour avoir les partages avec un client GNU/Linux et un serveur Scribe 2.4, il suffit d'ajouter le fichier `partages-linux.conf` de configuration dans `/etc/samba/conf.d/`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le fichier doit contenir :

```
[eclairng]
path = %H/.ftp
comment = disque personnel pour 98 et 95
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config_eole/
```

Pour rendre le changement opérant il faut procéder à la reconfiguration du module :

```
# reconfigure
```

Client Wheezy (Debian 7)

Pour l'intégration d'une station Debian 7 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Jean-François Mai, du collège République de Cholet et basé sur le travail de :

- Christophe Dezé (Rectorat de Nantes)
- Cédric Frayssinet (Mission Tice Académie de Lyon)
- Xavier Garel (Mission Tice Académie Lyon)
- Simon Bernard (Dane Reseau Lyon)
- Kalai Mehdi (Académie de Poitiers)

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_wheezy_in_EOLE_scribe-v1.0.pdf (37Mo)

Scripts d'intégration

Des scripts d'intégration sont mis à disposition à l'adresse suivante par Jean-François Mai, du collège République de Cholet : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Le script suivant installe un système avec un environnement minimal MATE et enfin s'occupe de l'intégration :

http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_wheezy_in_scribe-v1.0h.tar.gz [http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/debian_gnu_linux_jessie_in_scribe2.4-mate-core-v1.0b.tar.gz]

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom_du_script.sh
```



Beaucoup d'informations sont présentes dans le fichier `readme.txt` de l'archive.

Problème des partages sur un serveur EOLE Scribe 2.4

Pour avoir les partages avec un client GNU/Linux et un serveur Scribe 2.4, il suffit d'ajouter le fichier `partages-linux.conf` de configuration dans `/etc/samba/conf.d/`.

Le fichier doit contenir :

```
[eclairng]
path = %H/.ftp
comment = disque personnel pour 98 et 95
read only = no
browseable = no
invalid users = nobody guest
inherit permissions = yes
inherit acls = yes
create mask = 0664
directory mask = 0775
valid users = %U
write list = %U
guest ok = no
hide files = /config eole/
```

Pour rendre le changement opérant il faut procéder à la reconfiguration du module :

```
# reconfigure
```

3.9.1.b. Clients Ubuntu

Client Hardy Heron (8.10)

Pour l'intégration d'une station Ubuntu 8.10 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Mehdi Kalai, de l'académie de Poitiers :

http://www.m-k.cc/spip.php?article1

Scripts d'intégration

Des scripts d'intégration ont été développés par Christophe Dezé de l'académie de Nantes.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Ces scripts sont disponibles pour plusieurs versions de GNU/Linux Ubuntu :

- Ubuntu 8.04 **LTS** (Hardy Heron)
- Ubuntu 8.10 (Intrepid Ibex)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Ubuntu 9.04 (Jaunty Jackalope)
- Ubuntu 9.10 (Karmic Koala)
- Ubuntu 10.04 **LTS** (Lucid Lynx)
- Ubuntu 10.10 (Maverick Meerkat)
- Ubuntu 11.04 (Natty Narwhal)
- Ubuntu 12.04 (The Precise Pangolin)

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom_du_script.sh
```

3.9.1.c. Clients Mandriva

Client Mandriva 2010

Pour l'intégration d'une station Mandriva 2010 à un serveur Scribe, vous pouvez vous reporter à la procédure décrite par notre collègue Mehdi Kalaï, de l'académie de Poitiers :

http://www.m-k.cc/spip.php?article2

3.9.1.d. Clients Mageia

Scripts d'intégration

Un script d'intégration a été développés par Mehdi Kalaï de l'académie de Poitiers.

Il est mis à disposition dans : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

Ce script n'est disponible que pour la version 2 de Mageia.

Pour utiliser un des scripts proposés en téléchargement, vous devez le rendre exécutable.

Si vous n'êtes pas à l'aise avec la ligne de commande clic droit → Propriétés → permettre l'exécution du programme.

Sinon lancez un terminal et tapez la commande suivante :

```
$ chmod +x nom_du_script.sh
```

3.10. Liens vers des contributions externes

Installation de postes clients GNU/Linux Ubuntu par Cédric Frayssinet.

L'objectif de ce guide est d'obtenir des postes de travail prêts à l'utilisation et qui peuvent être restaurés dans leur état initial en quelques minutes par une personne sans compétence informatique particulière à partir d'une image OSCAR.

OSCAR permettra également de déployer rapidement un ensemble de postes identiques à partir d'un

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

poste modèle.

Ce guide fait parti des ressources technico-pédagogiques accessibles publiquement sur le site de la Délégation Académique au Numérique Éducatif et du CRDP de l'académie de LYON.

Il est mis à mis à disposition selon les termes de la licence Creative Commons Paternité-Pas d'Utilisation Commerciale-Partage des Conditions Initiales à l'Identique 2.0 France.

http://nefertiti.crdp.ac-lyon.fr/wk/cdch/postes_clients_ubuntu_32_64_bits

http://www2.ac-lyon.fr/wiki-dane/mardi/integration_poste_x_ubuntu_sur_scribe

Scripts d'intégration des clients Gnu/Linux dans un environnement EOLE Scribe

Les scripts versionnés sont mis à disposition par la Délégation Académique au Numérique Éducatif de Lyon à l'adresse suivante :

https://github.com/dane-lyon/clients-linux-scribe

Archives de scripts d'intégration

Les différentes archives de scripts d'intégration proposées par les contributeurs concernent des versions de GNU/Linux et des environnements de bureau différents.

Ils sont mis à disposition à l'adresse suivante : http://eole.ac-dijon.fr/pub/Contribs/Clients_Linux/

4. Les clients Windows

4.1. Installation et configuration des clients Windows

4.1.1. Principe

Scribe agissant comme un contrôleur de domaine, les stations Windows doivent dans un premier temps être intégrées dans le domaine.

Afin d'interagir davantage avec Scribe, un programme client a été développé pour les stations Windows.

Il doit être installé sur chaque station intégrée au 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.1.2. Configuration réseau

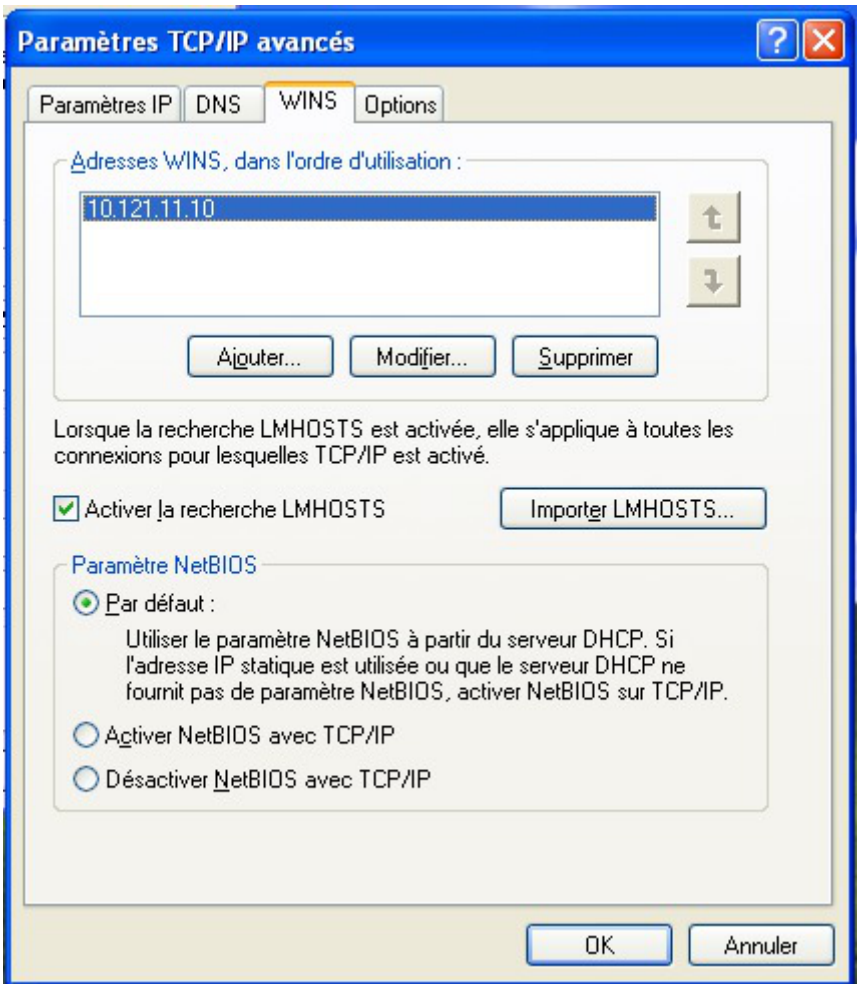
Avant l'intégration au domaine, il est indispensable de s'assurer que les paramètres réseau de la station soient corrects (adresse IP, passerelle, DNS, WINS).

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.905] ;
- 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 .



Configuration du serveur WINS dans Windows XP

4.1.3. Intégration et installation du client Scribe automatique

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

4.1.3.a. JoinEOLE pour 2.5.2

Préparation de 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(

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

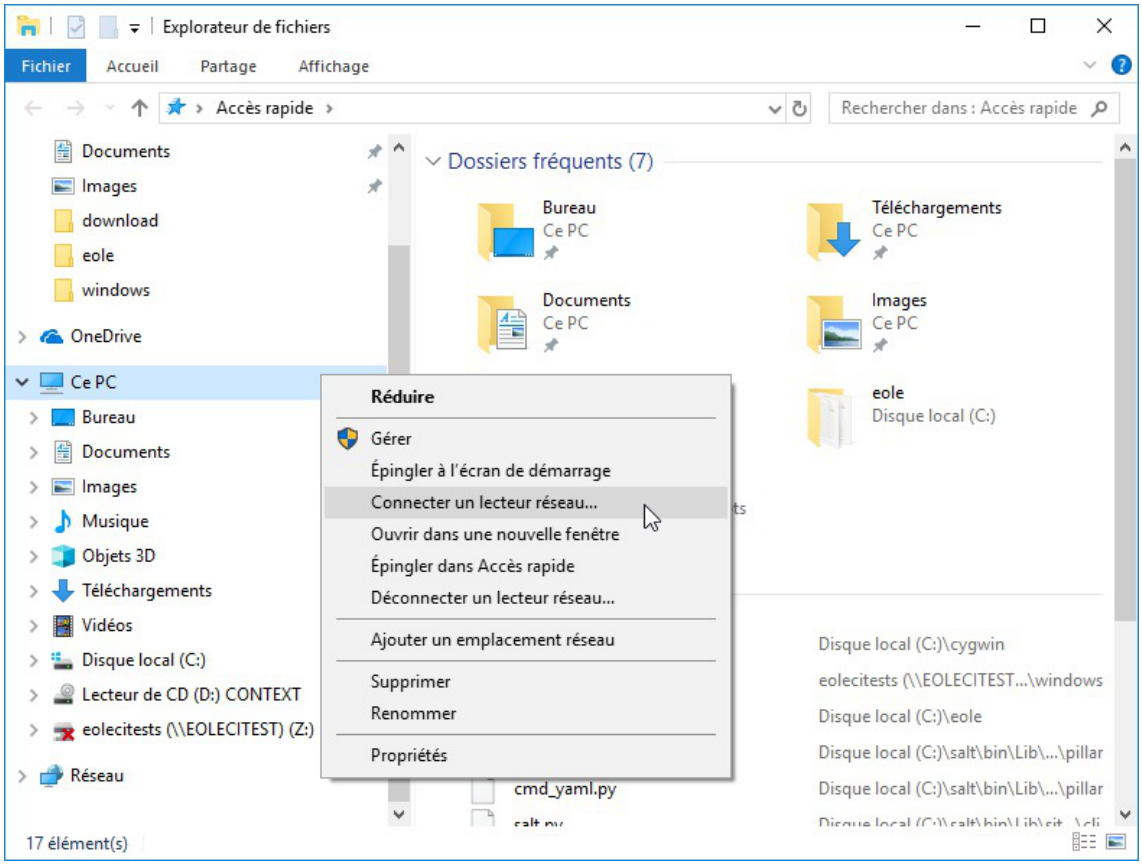
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

Monter un répertoire en spécifiant les identifiants de connexion

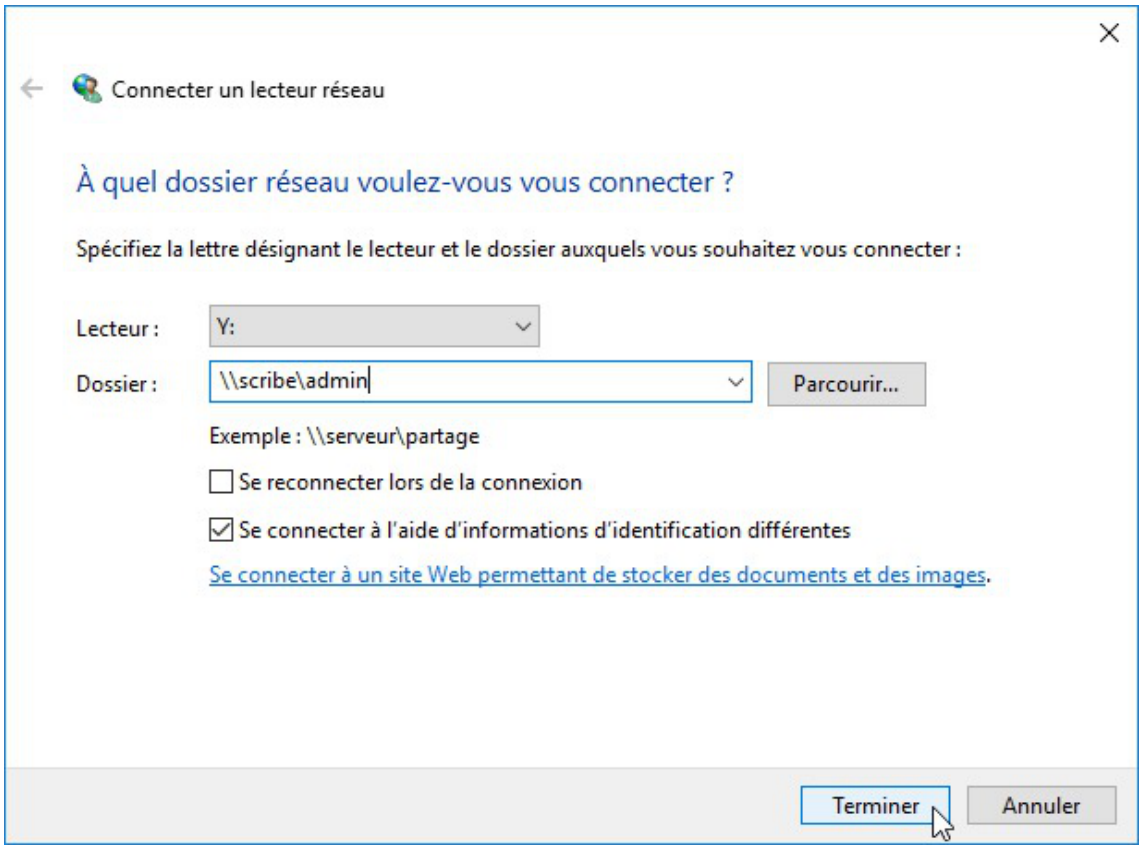
Pour accéder au répertoire personnel de l'administrateur :

- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

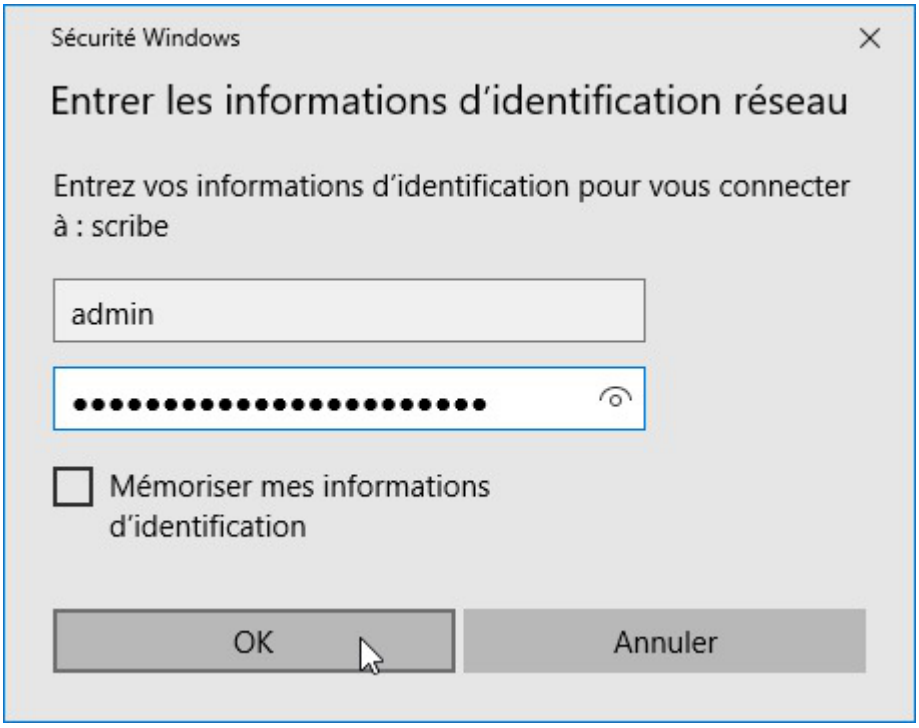


- Faire un clique droit sur `Ce PC` ;

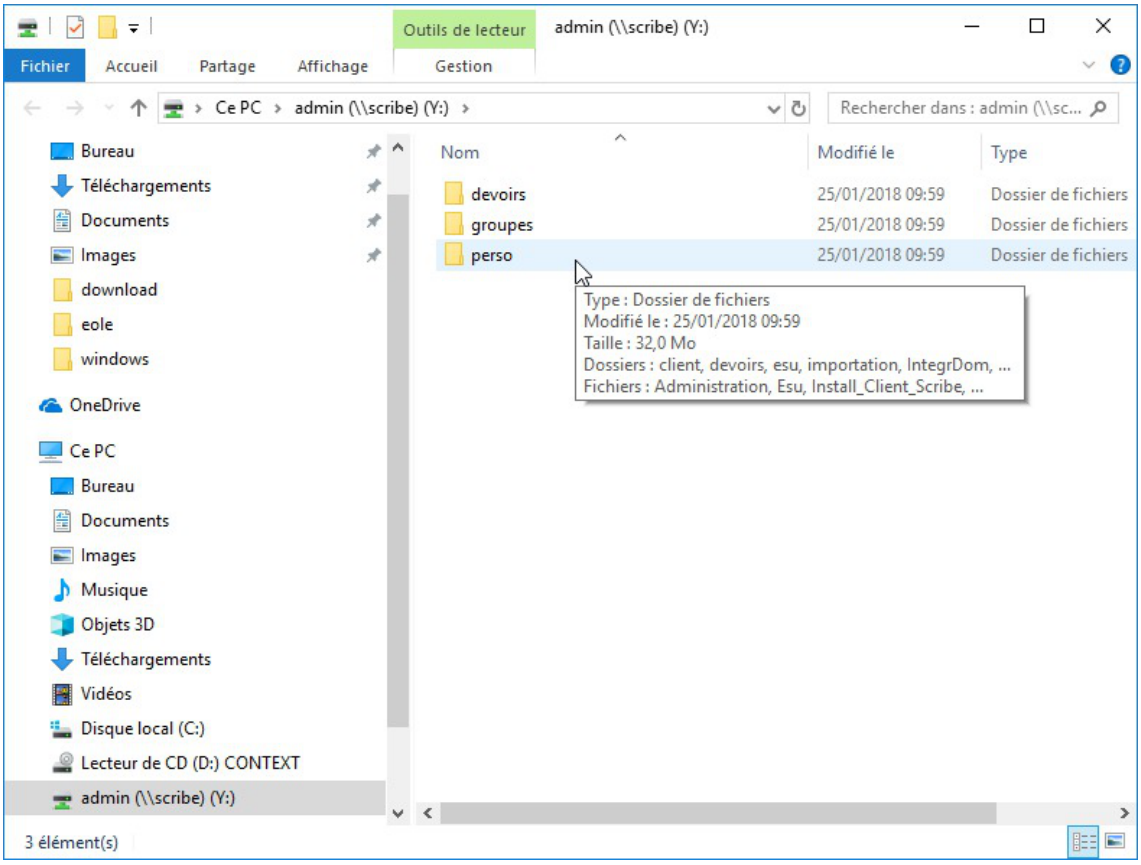


- Saisir `\\scribe\admin` dans le champ `Dossier`, décocher `☑ Se reconnecter lors de la connexion`, cocher `☑ Se connecter à l'aide d'informations d'identification différentes` et cliquer sur le bouton `Terminer` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton OK ;



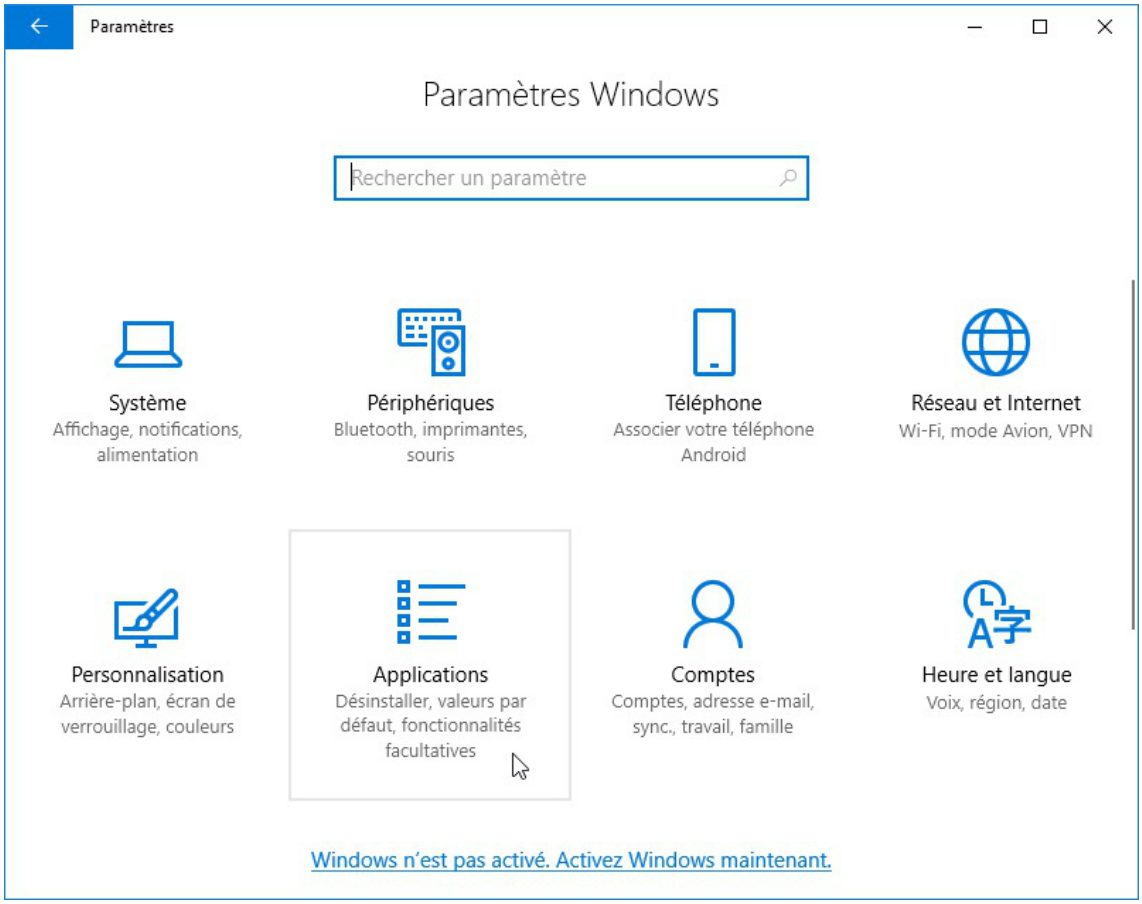
Activer le support de partage de fichiers SMB 1.0/CIFS

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

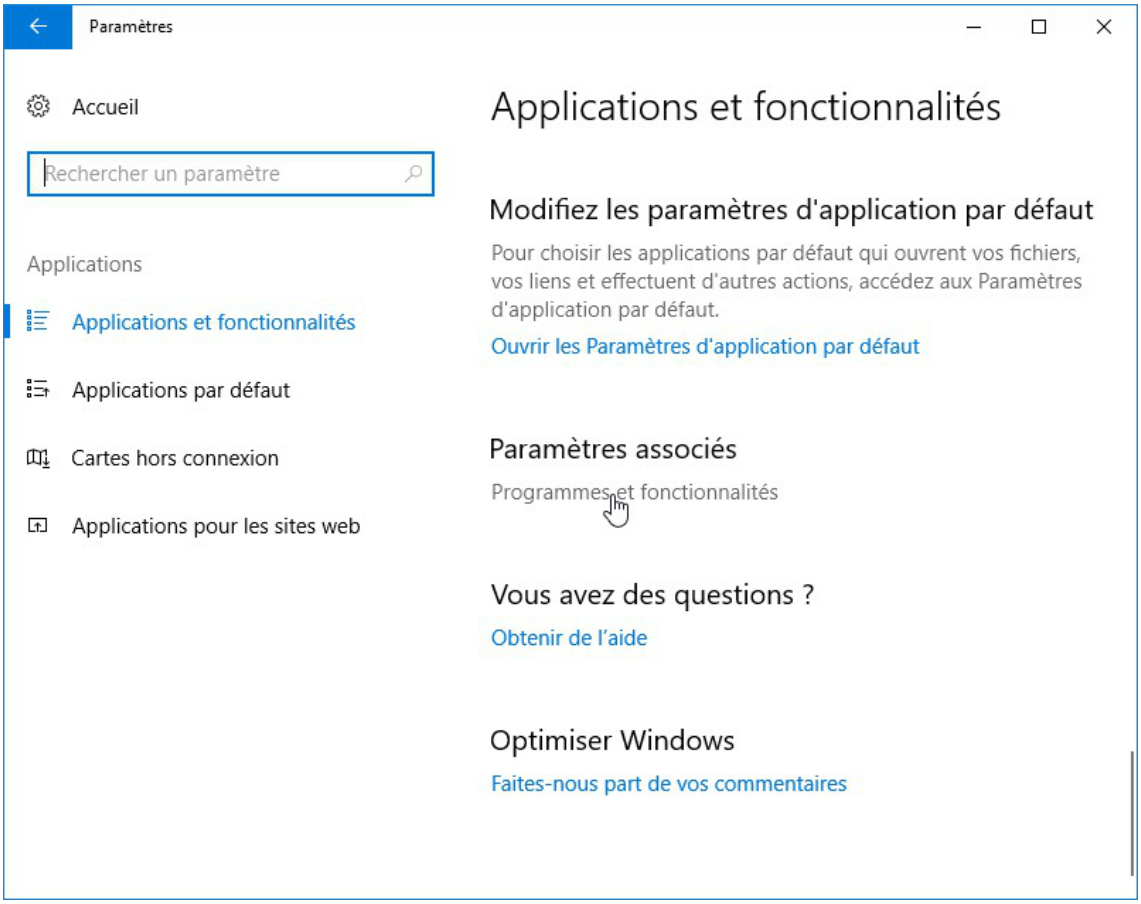
Paramétrer Windows de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

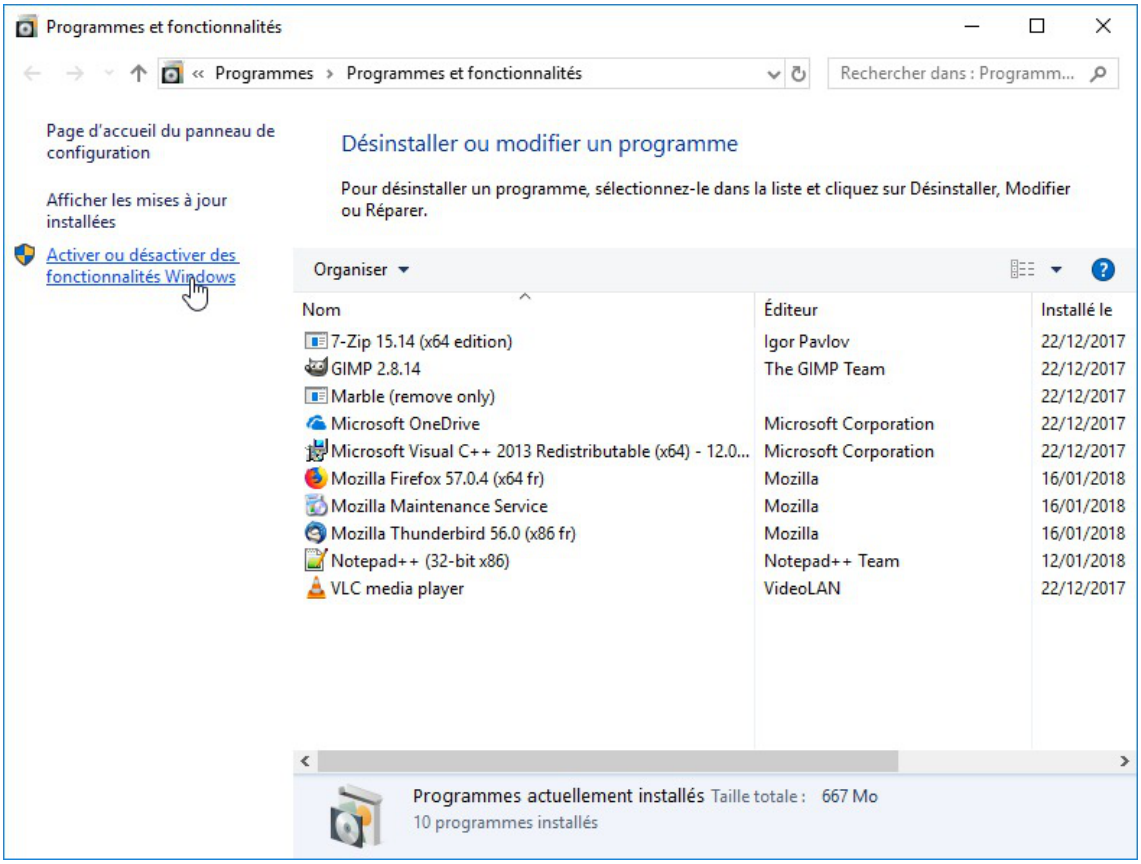


- Cliquer sur `Applications` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

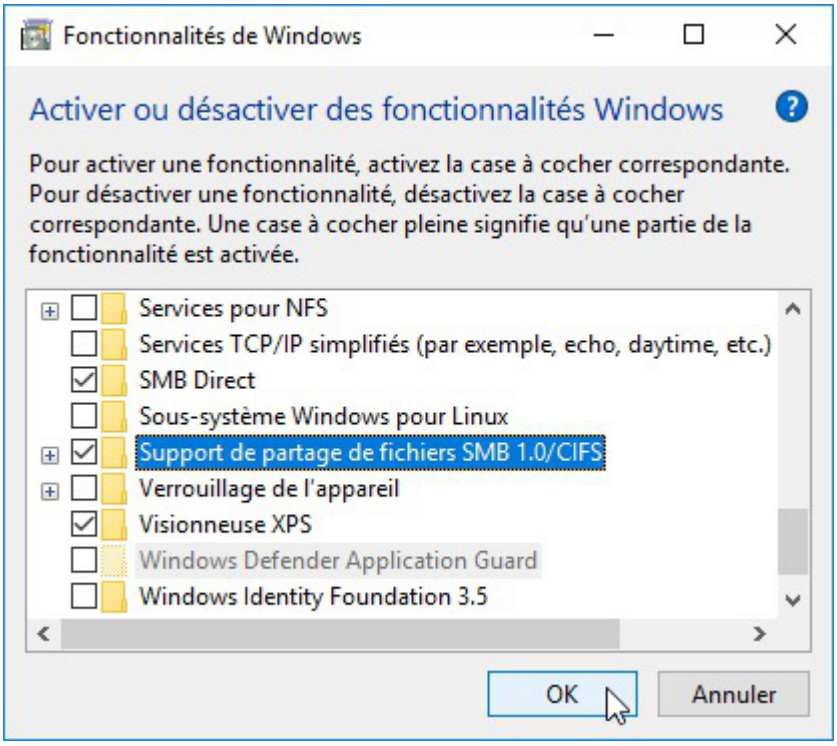


- Descendre et cliquer sur `Programmes et fonctionnalités` ;

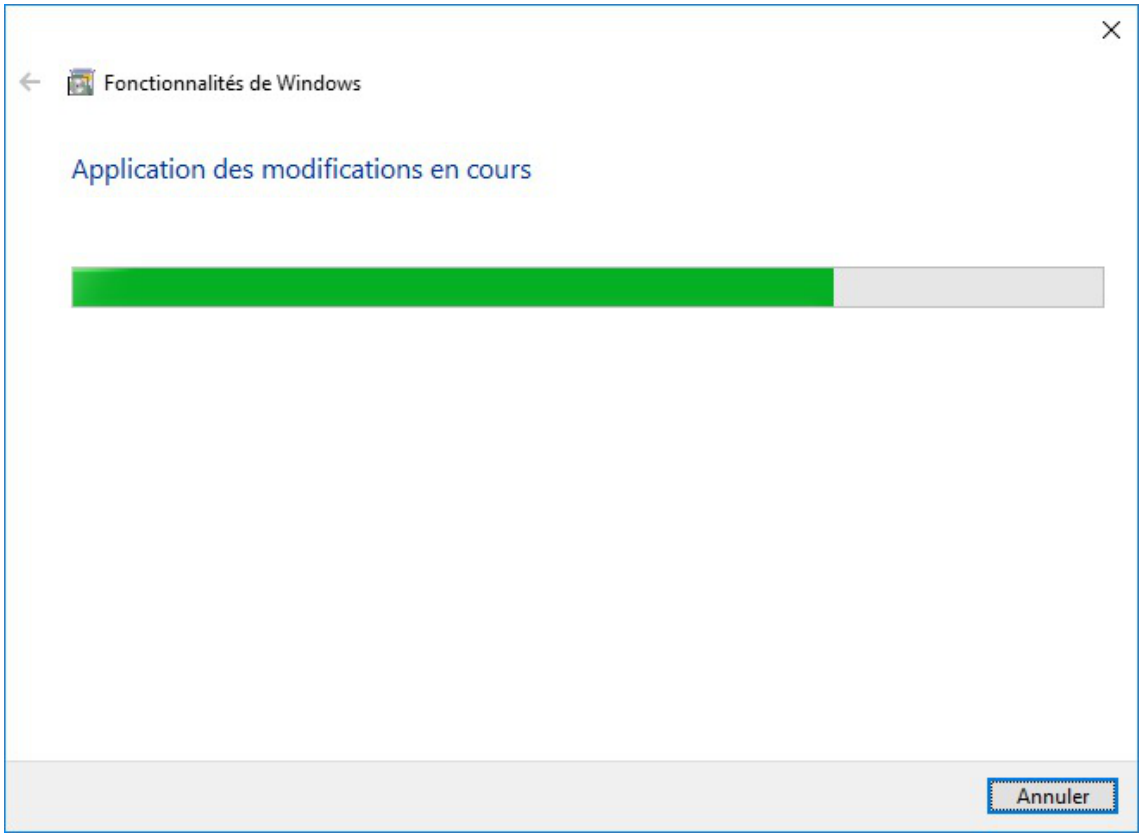


- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Descendre dans la liste et cocher ☑ Support de partage de fichiers SMB 1.0/CIFS , cliquer sur OK, les modifications s'appliquent ;



Préparation de Windows 7

Les stations Windows 7 ne nécessitent aucune action préalable à l'utilisation de JoinEOLE.

Utilisation de JoinEOLE

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

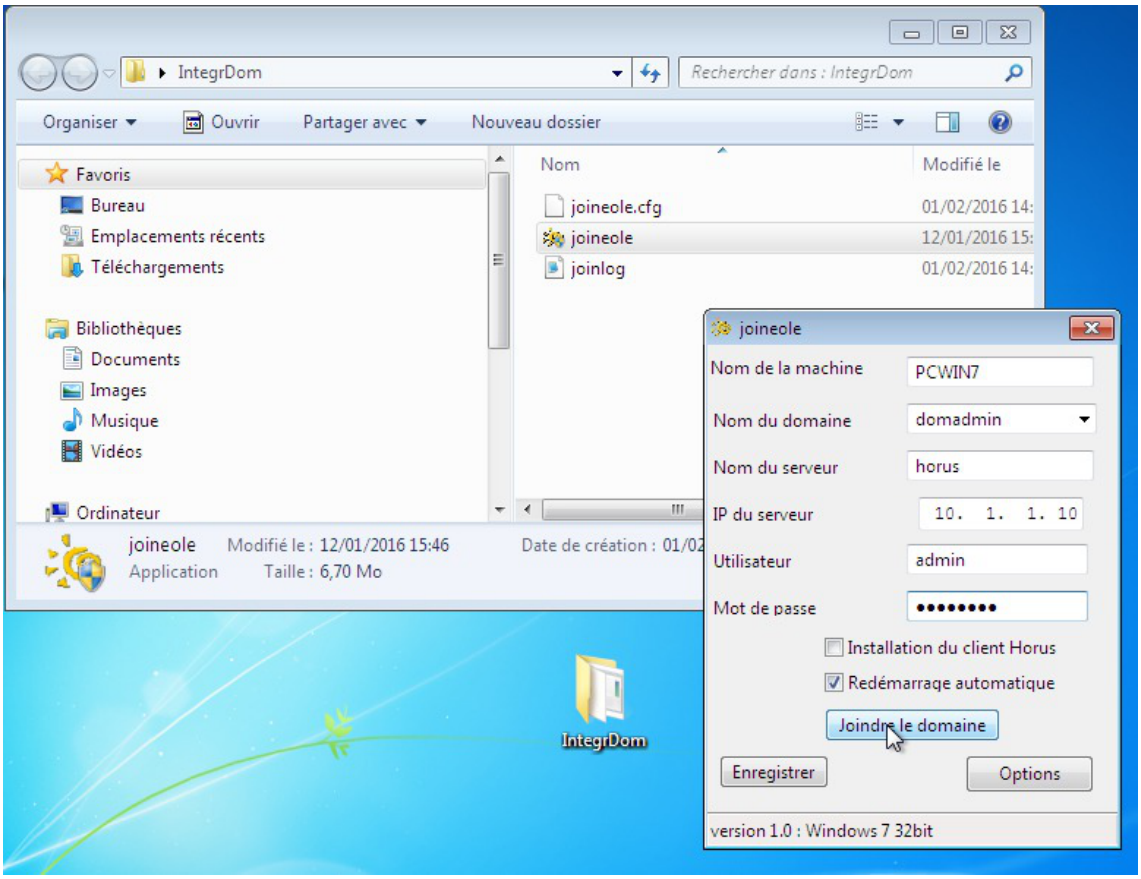
L'outil JoinEOLE prépare la station, la joint au domaine et installe de façon optionnelle le client pour Scribe ou Horus. De ce fait, il peut également être utilisé pour joindre les postes à un domaine Horus sur lequel le logiciel ESU n'est pas activé.

Le logiciel JoinEOLE est une contribution de Christophe Dezé de l'académie de Nantes.



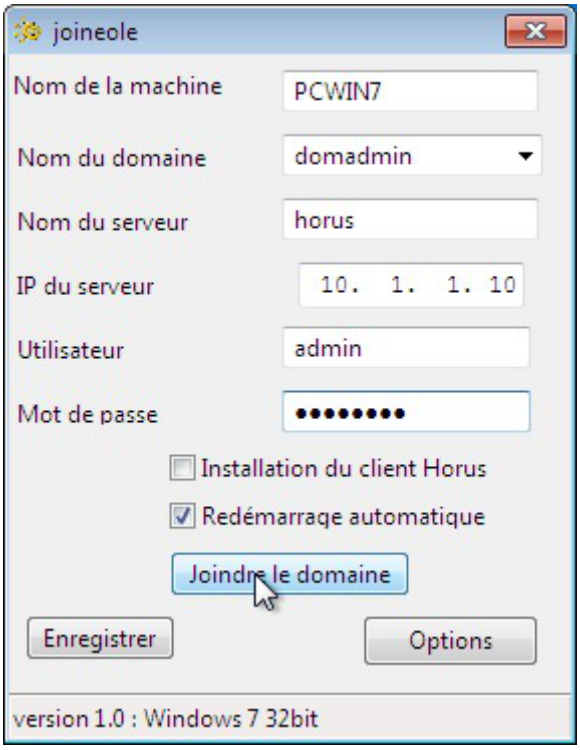
Il n'est pas possible de lancer l'exécution de JoinEOLE directement depuis le lecteur réseau car l'utilitaire ne gère par les chemins UNC[p.904].

Il faut donc copier l'utilitaire en copiant le répertoire `IntegrDom` sur la machine cliente et lancer son exécution.



Il faut préciser le nom de la machine à intégrer, le nom du domaine auquel la machine doit être raccrochée, le nom netbios du serveur ainsi que l'adresse IP du serveur Scribe ou Horus.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'utilitaire permet l'intégration au domaine et installe directement le client si ☑ Installation du client est cochée.

La case Redémarrer automatiquement est précochée.

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.

4.1.3.b. PrepaWin pour 2.5.1

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel `PrepaWin` permet de préparer et d'intégrer une station Windows XP ou Seven Professionnel 32 ou 64 bits sur un domaine Scribe.

Pour plus d'informations, vous pouvez consulter le document suivant :

http://eole.ac-dijon.fr/pub/Documentations/divers/IntegrDom_PrepaWin_Scribe.pdf [http://eole.ac-dijon.fr/pub/Documentations/divers/IntegrDom_PrepaWin_Scribe.pdf]

Le logiciel `PrepaWin` est une contribution de Jérôme Labriet de l'académie de Besançon.

4.1.3.c. IntegrDom pour 2.5.1

PrepaWin et IntegrDom sont à utiliser sur un module Scribe 2.5.1.

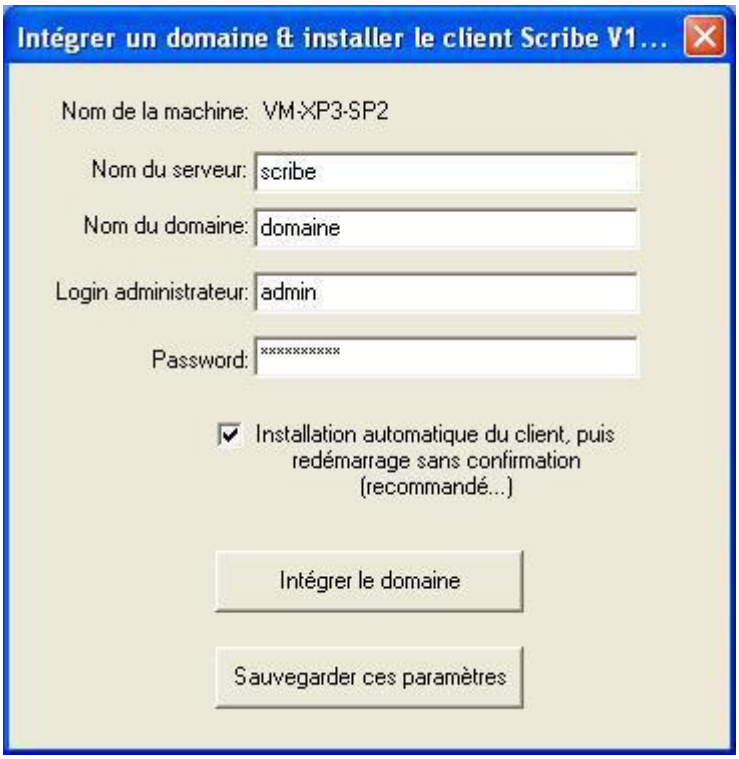
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel `IntegrDom` est fourni dans le répertoire personnel de l'utilisateur `admin`.
Cet outil permet de joindre une station XP au domaine et d'y installer le client Scribe en une seule fois.

Il est possible de pré-paramétrer le logiciel. Pour cela :

- se connecter en admin sur une station déjà intégrer au domaine ;
- lancer le programme `U:\IntegrDom\IntegrDom.exe` ;
- remplir les paramètres de configuration ;
- cliquer sur *Sauvegardez les paramètres* ;
- copier le contenu du répertoire `U:\IntegrDom\` sur une clé USB.



Intégration au domaine et installation automatique du client Scribe

Pour joindre une nouvelle station au domaine, il faut :

- connecter la clé USB sur la station ;
- lancer `IntegrDom.exe` depuis la clé USB ;
- cliquer sur *Intégrer le domaine*.

Les erreurs éventuellement retournées par IntegrDom sont celles retournées par l'utilisation de la fonction NetJoinDomain : http://msdn.microsoft.com/en-us/library/aa370433(v=vs.85).aspx.

> Le logiciel `IntegrDom` est une contribution de Daniel Piquée de l'académie de la Réunion.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.1.3.d. Joinscribe

`joinscribe` est un outil d'intégration au domaine et d'installation du client Scribe qui s'exécute depuis le serveur.

L'outil joinscribe n'est pas pré-installé sur le serveur Scribe.
Il s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
# apt-eole install joinscribe
```

Avant d'exécuter joinscribe, il faut préparer le poste client de la manière suivante :

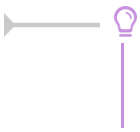
- dans les "options des dossiers", onglet `Affichage`, décocher l'option `☑ Utiliser le partage de fichiers simple` ;
- mettre un mot de passe à l'utilisateur administrateur ;
- désactiver le pare-feu de Windows.

Une fois les postes clients préparés, lancer `joinscribe` depuis la console du serveur Scribe.



Exemple d'utilisation de joinscribe :

```
joinscribe -d 192.168.1.1 -f 192.168.1.254
joinscribe -d 192.168.1.25
```



En cas de problème, consulter sur le serveur Scribe les fichiers `/var/log/joinscribe/` et sur le poste client `c:\windows\eole\tmp\ParamIntegr.log`.

Le logiciel `joinscribe` est une contribution de Christophe Dezé de l'académie de Nantes.

4.1.4. Intégration et installation du client Scribe 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"
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le fichier `Win_Samba3DomainMember.reg` mis à disposition dans `/home/esu/Console/` et accessible 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 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.

Activer manuellement le support de partage de fichiers SMB 1.0/CIFS

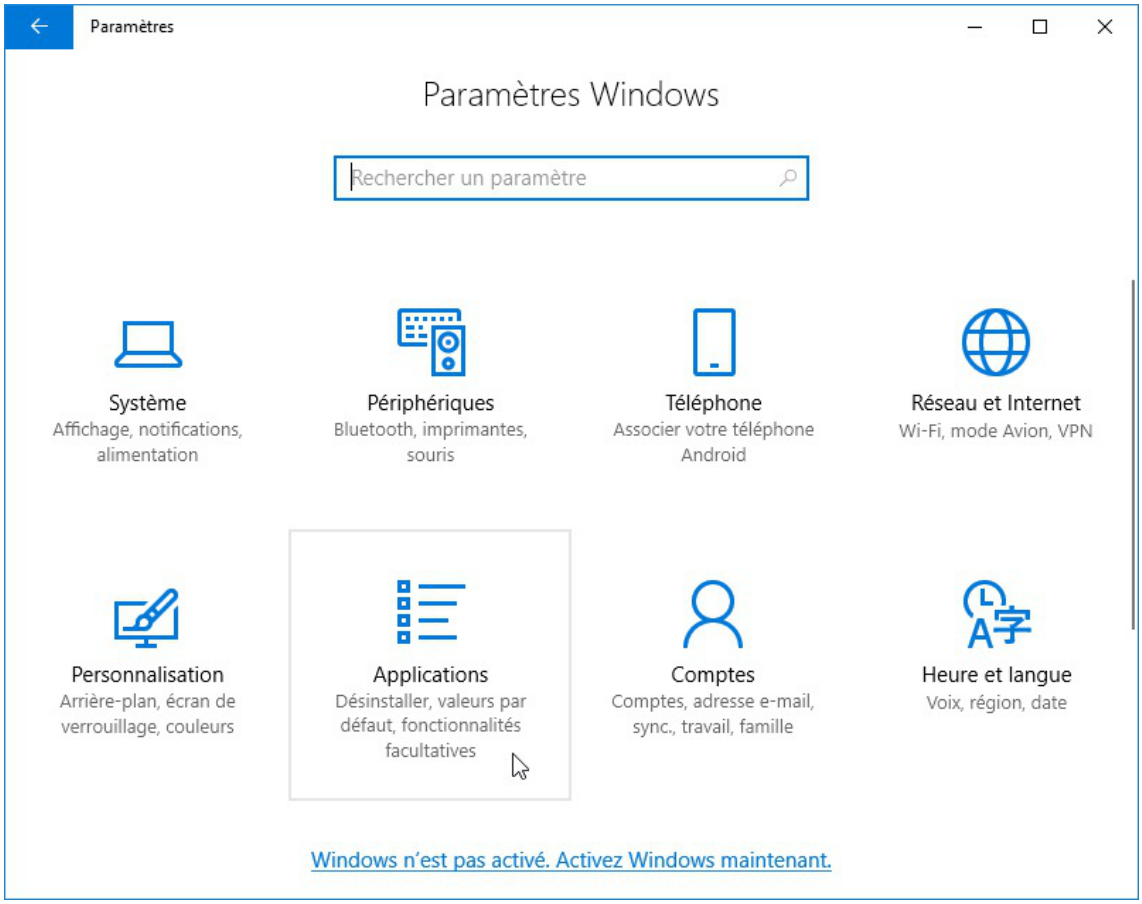


Sur un module EOLE à jour, l'activation du `support de partage de fichiers SMB 1.0/CIFS` est réalisée automatiquement par JoinEOLE et sa commande d'activation a été ajoutée au script `Win10.bat`.

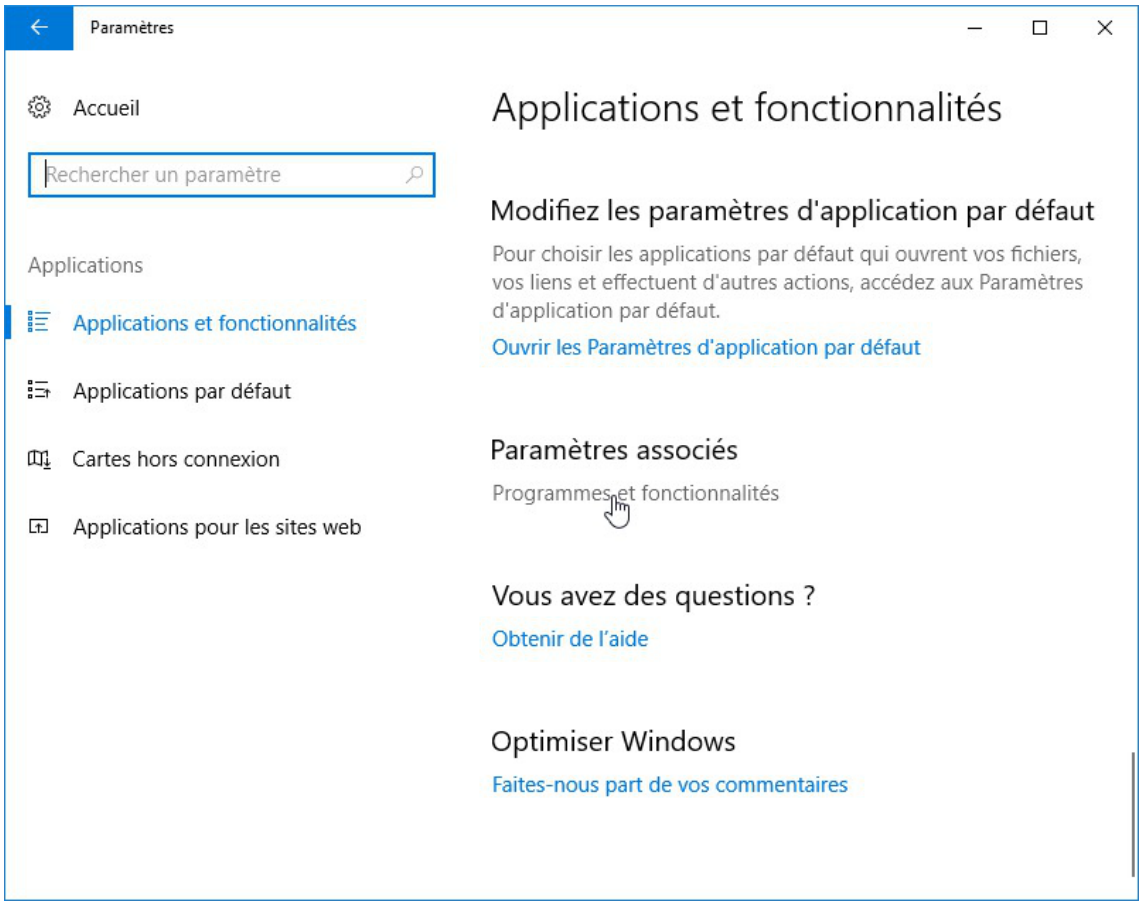
Paramétrer Windows de la façon suivante :

- Menu `Windows` et sélectionner `Paramètres` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

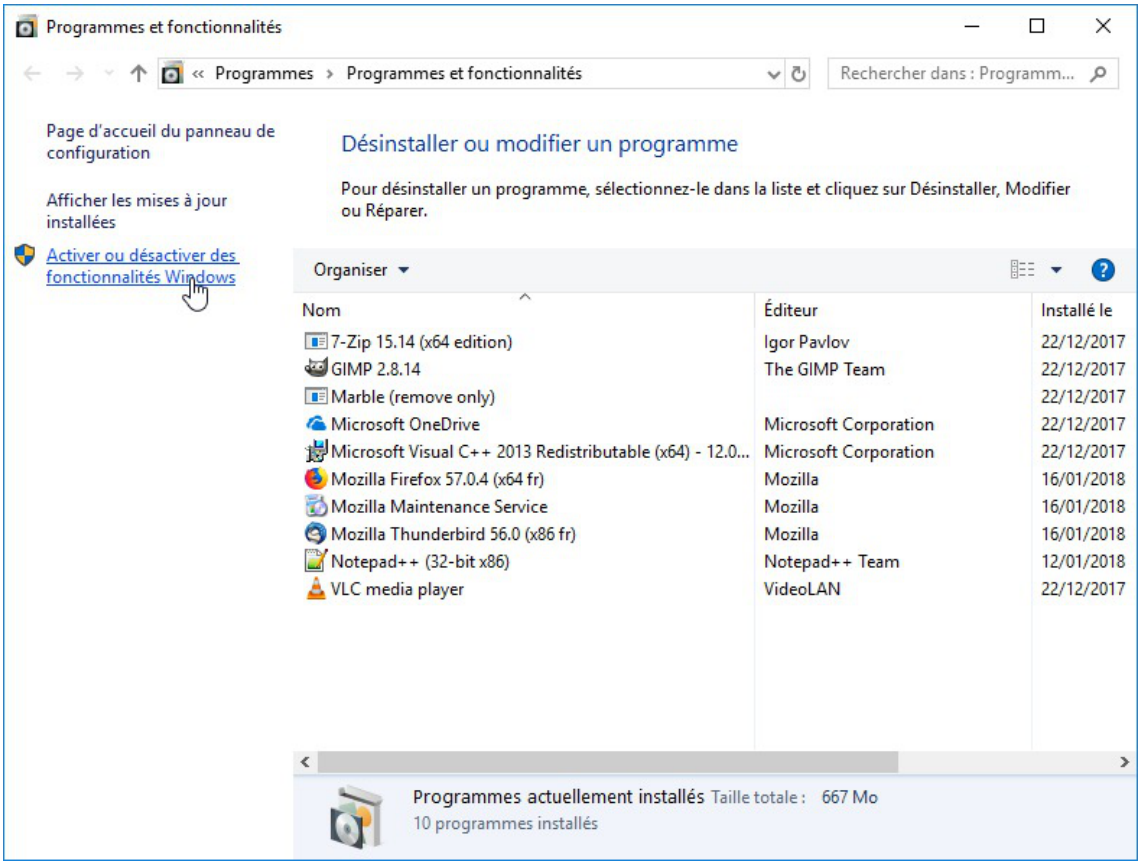


- Cliquer sur `Applications` ;

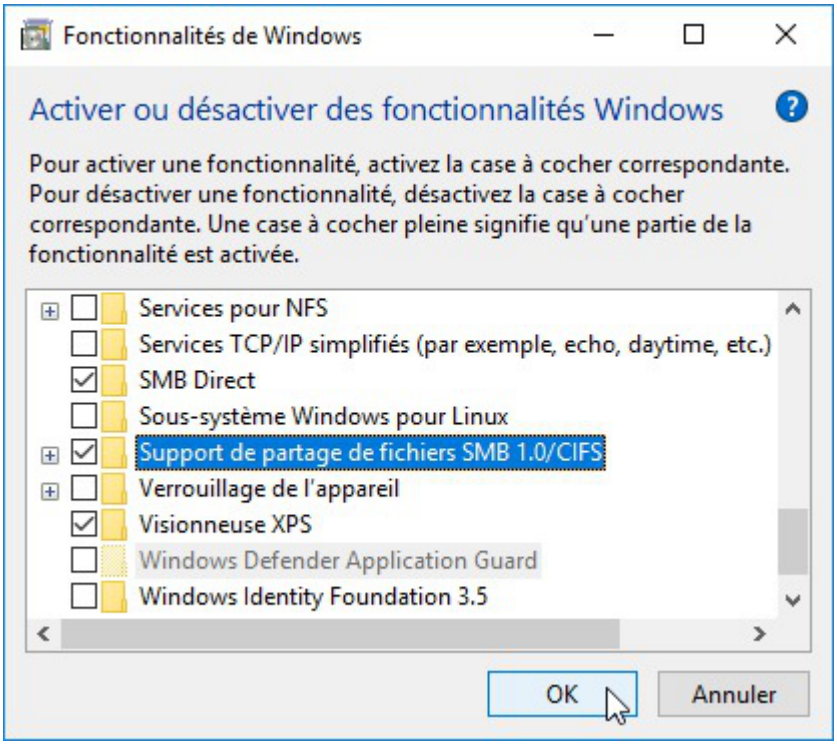


- Descendre et cliquer sur `Programmes et fonctionnalités` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

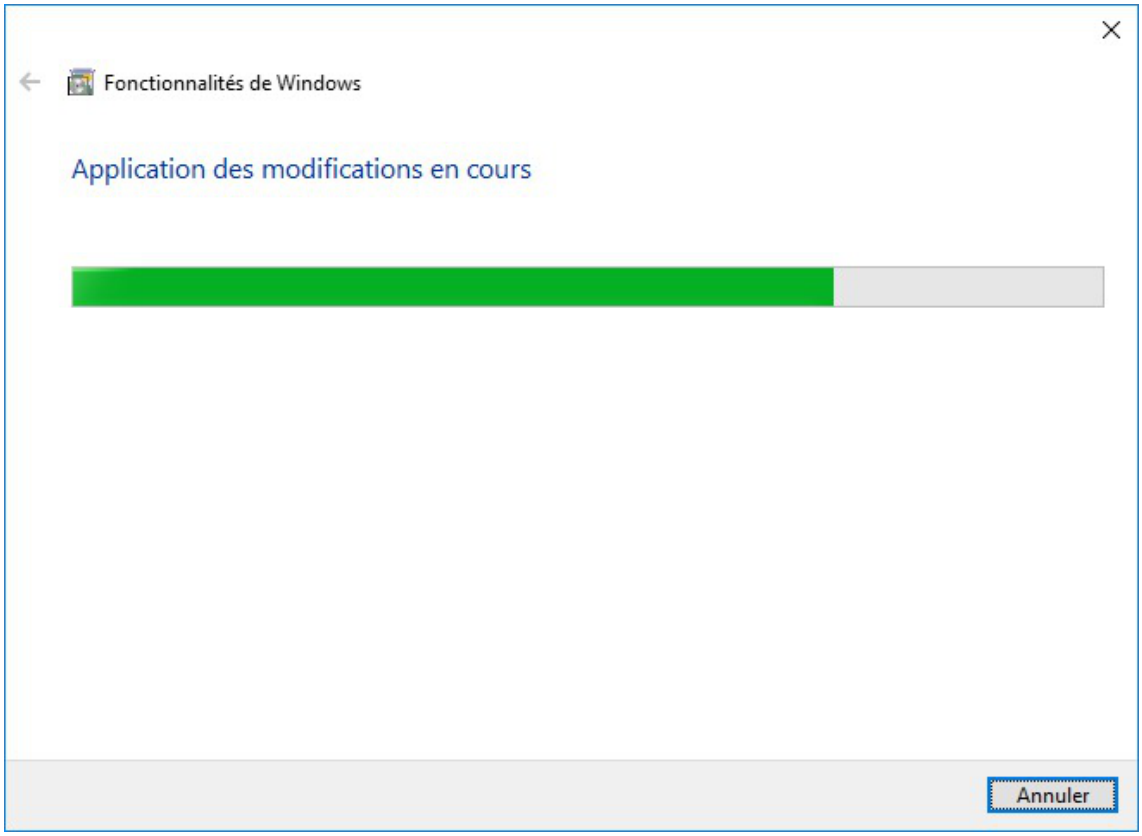


- Cliquer sur `Activer ou désactiver des fonctionnalités Windows` ;



- 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)



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(

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

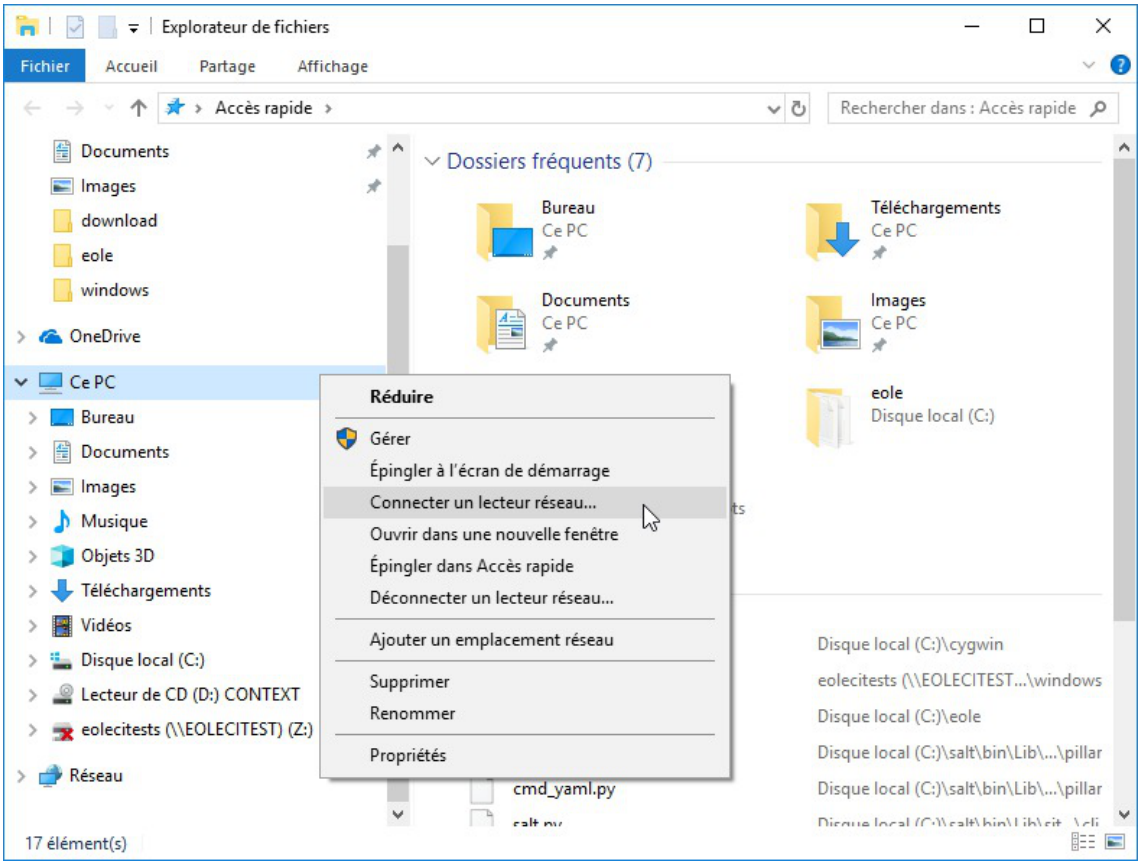
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:00000001
```

Monter un répertoire en spécifiant les identifiants de connexion

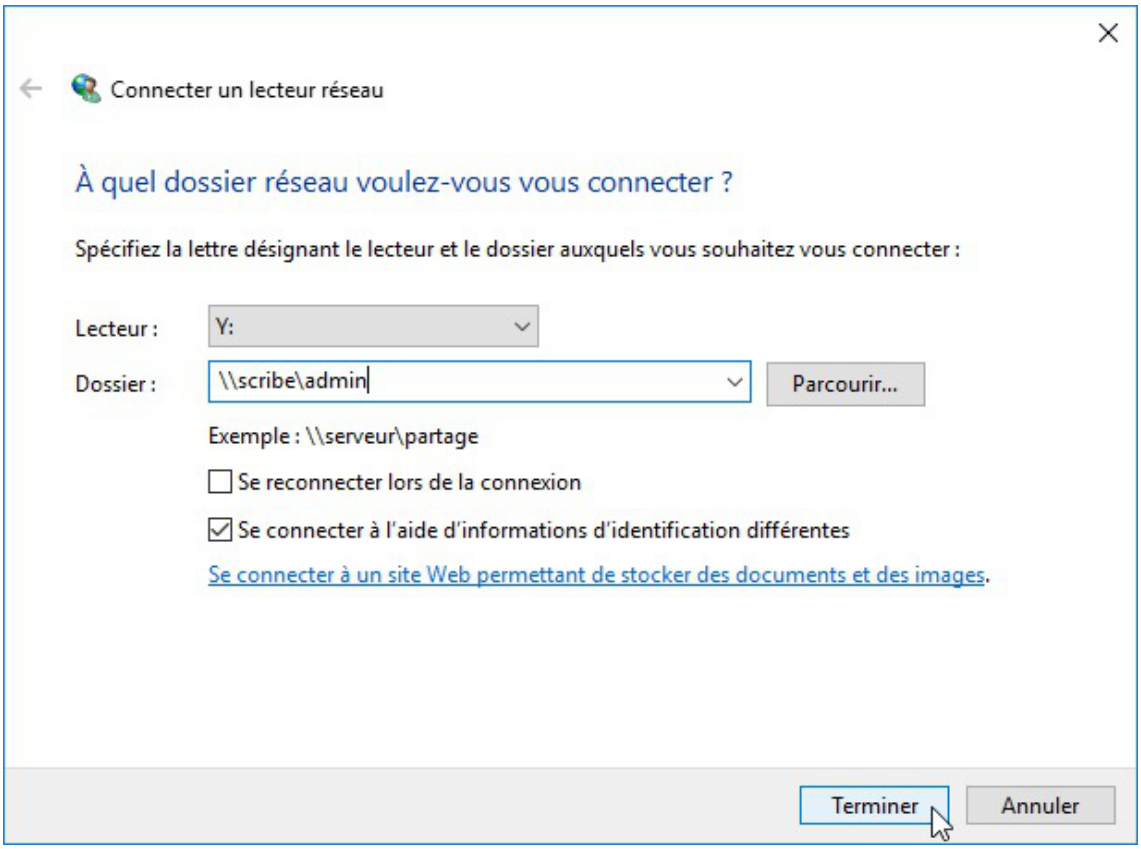
Pour accéder au répertoire personnel de l'administrateur :

- Se connecter sur le poste en tant qu'administrateur ;
- Se rendre dans l'explorateur de fichier ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

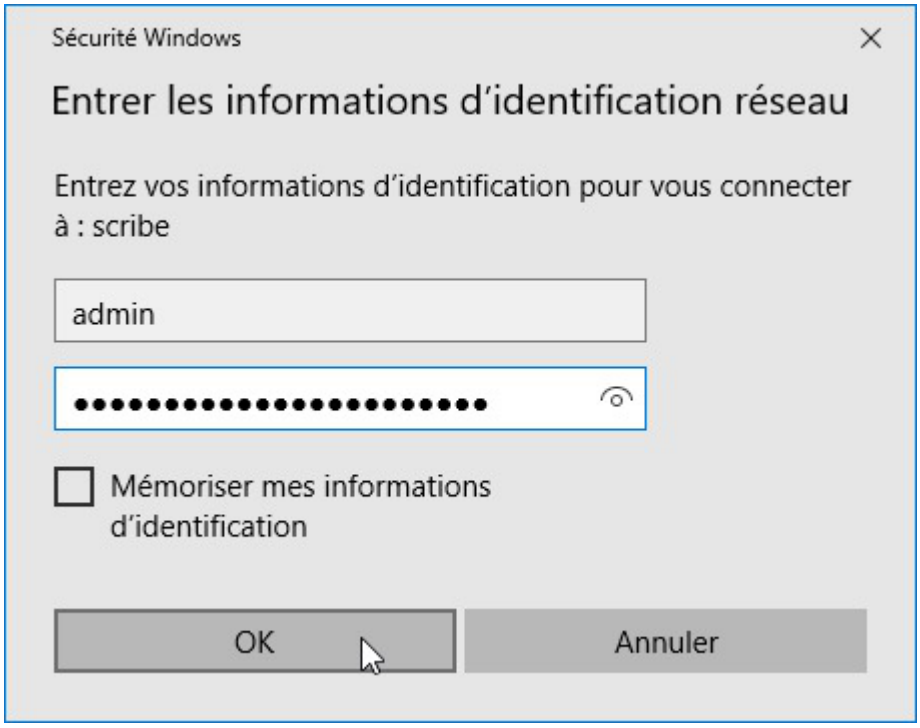


- Faire un clique droit sur `Ce PC` ;

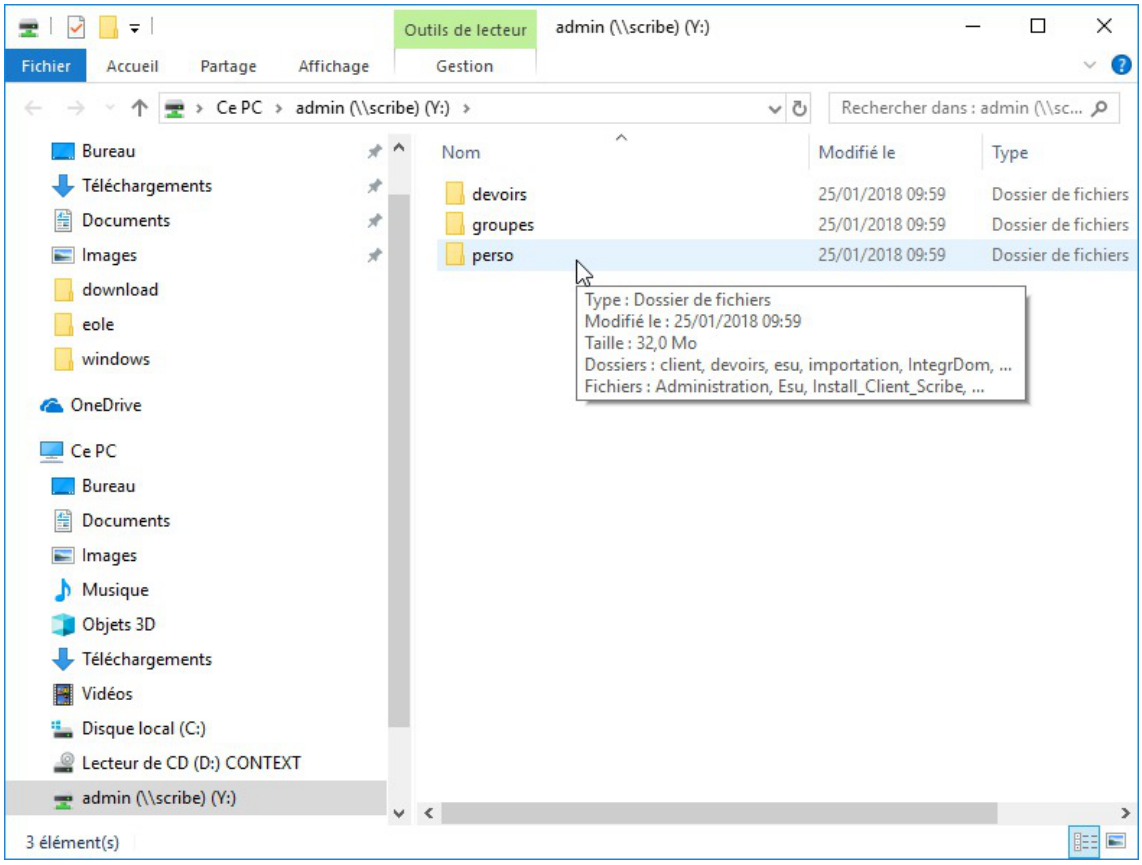


- Saisir `\\scribe\admin` dans le champ `Dossier`, décocher ☑ Se reconnecter lors de la connexion, cocher ☑ Se connecter à l'aide d'informations d'identification différentes et cliquer sur le bouton `Terminer` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Saisir le compte `admin` et la clé secrète associée ("mot de passe") et cliquer sur le bouton OK ;

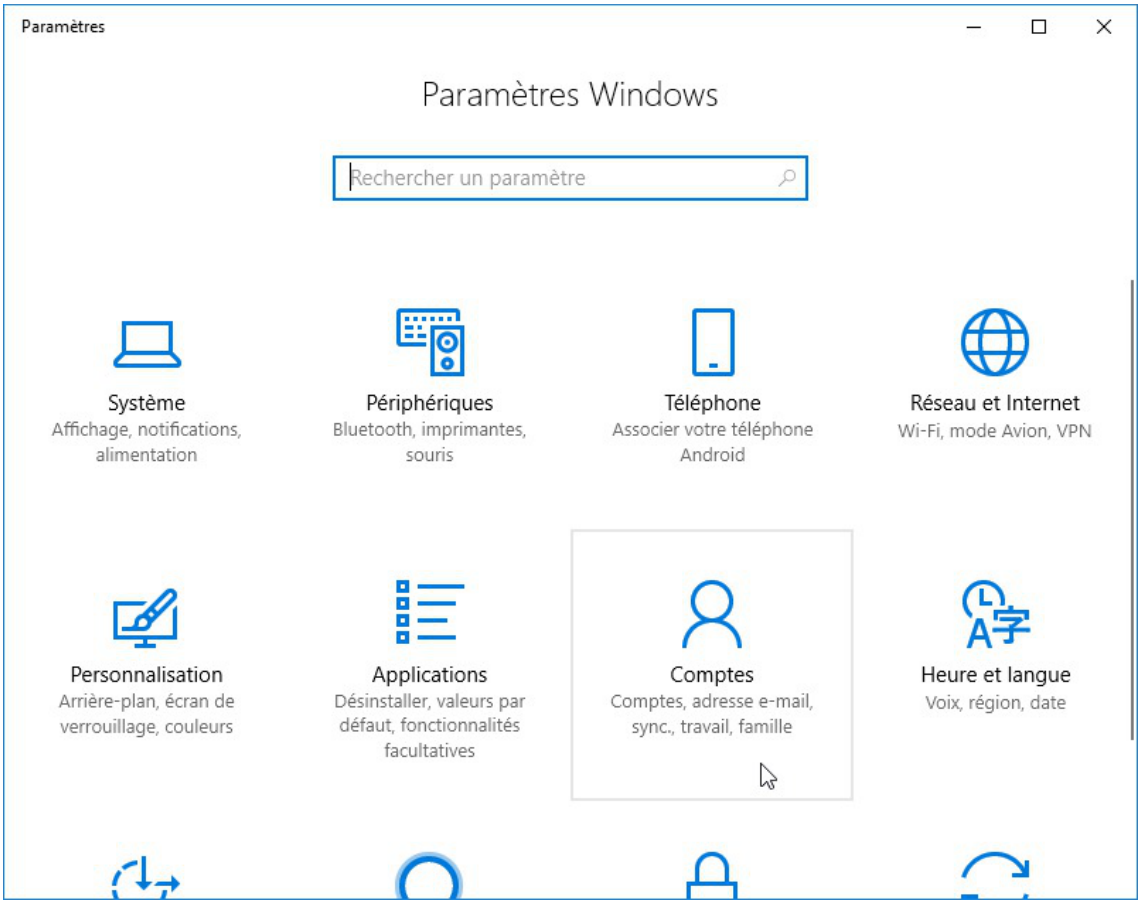


Jonction au domaine

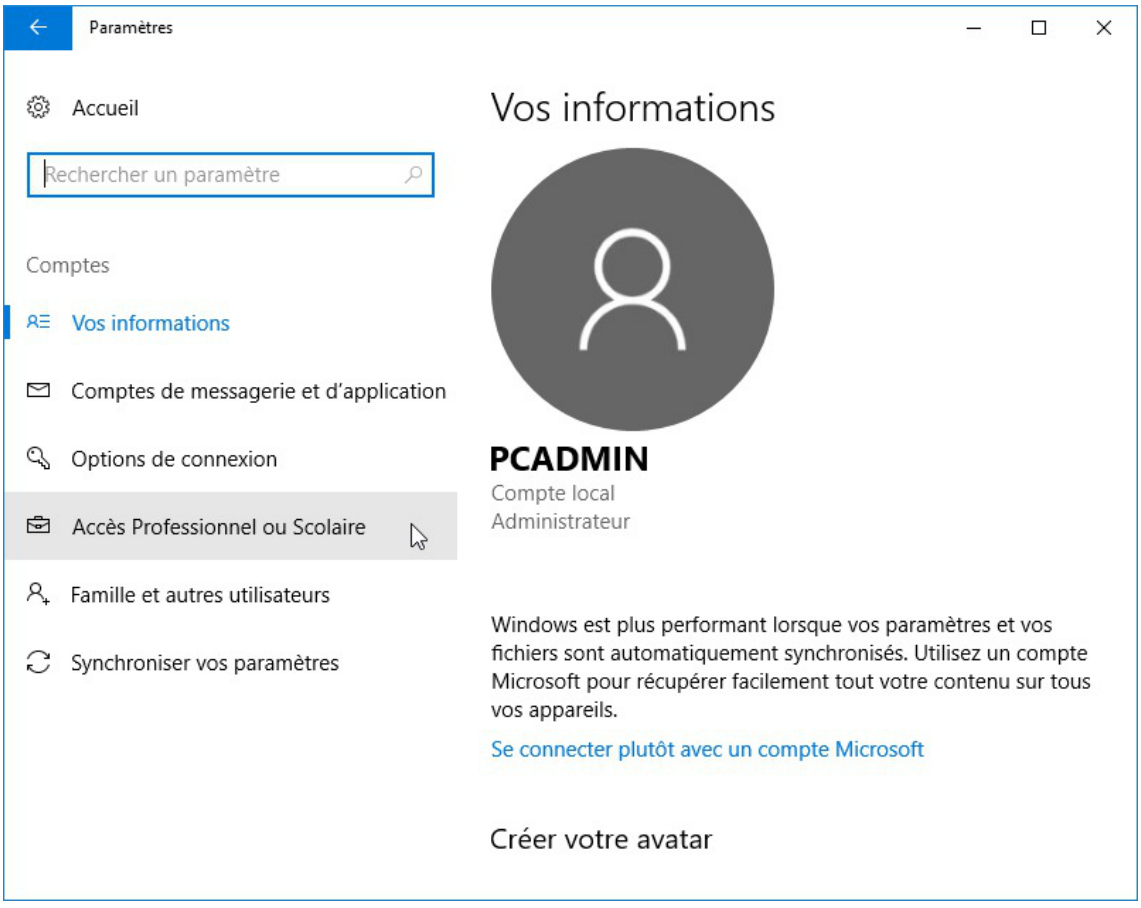
Ajouter la station au domaine de la façon suivante :

- Menu Windows et sélectionner Paramètres ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

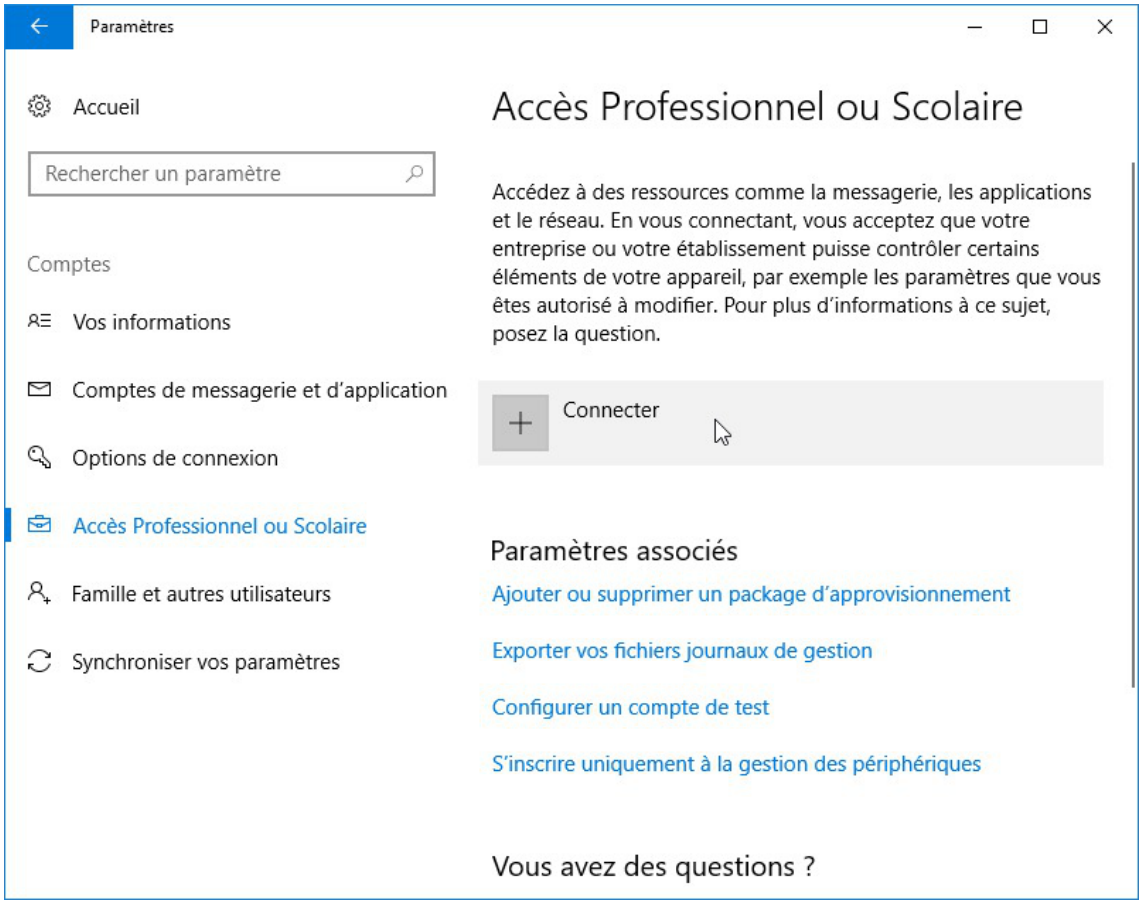


- Cliquer sur `Comptes` ;



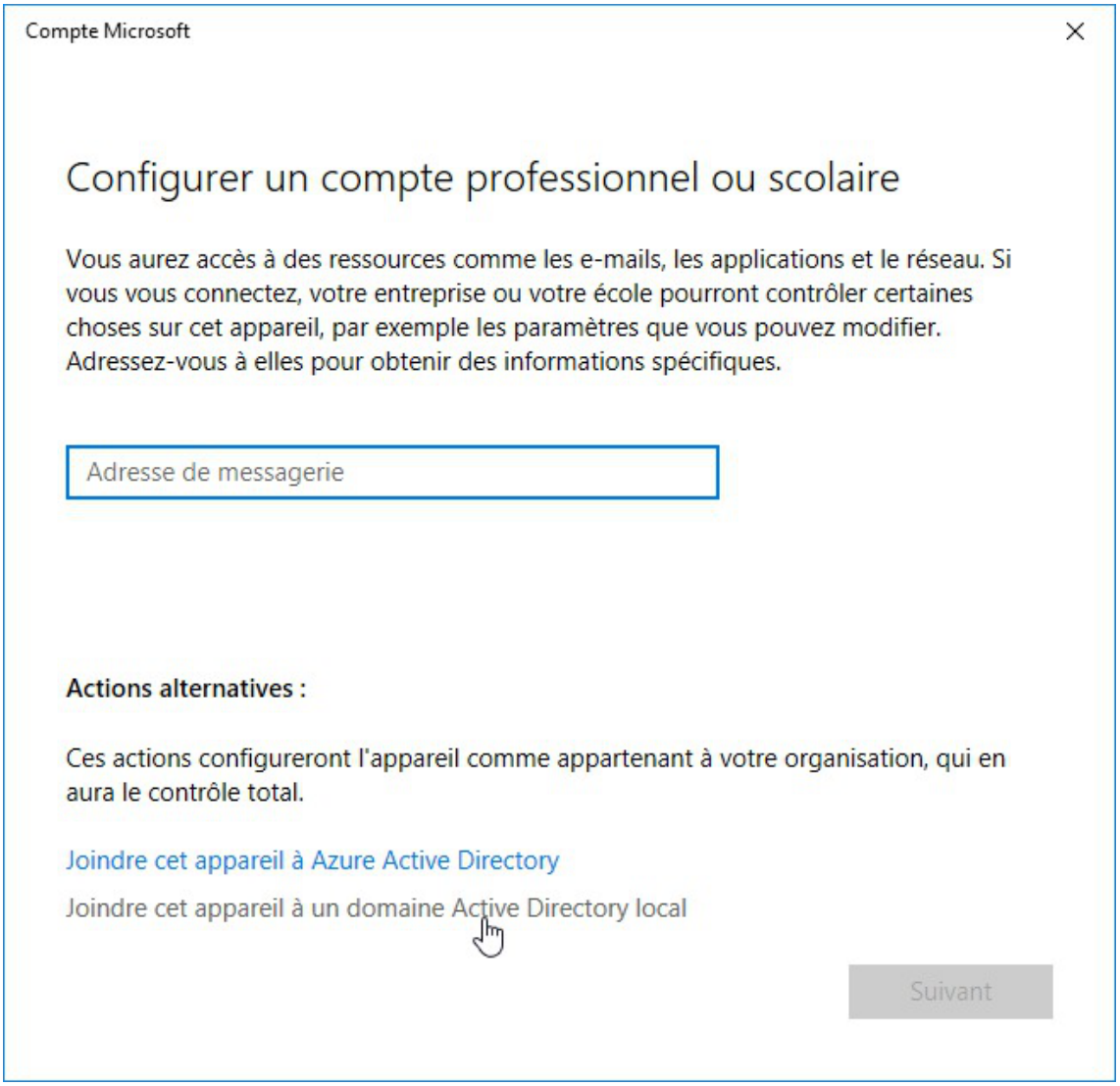
- Cliquer sur `Accès Professionnel ou Scolaire` dans le menu de gauche ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

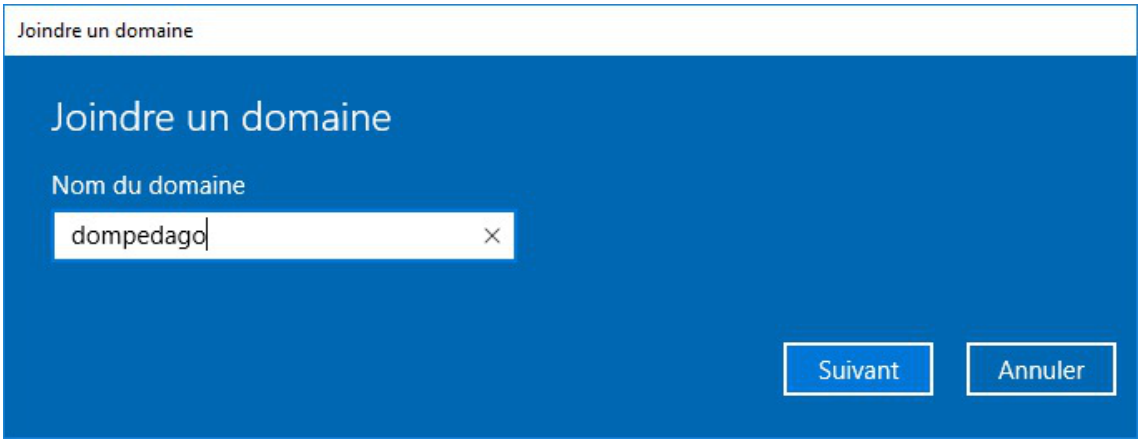


- Cliquer sur Connecter ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

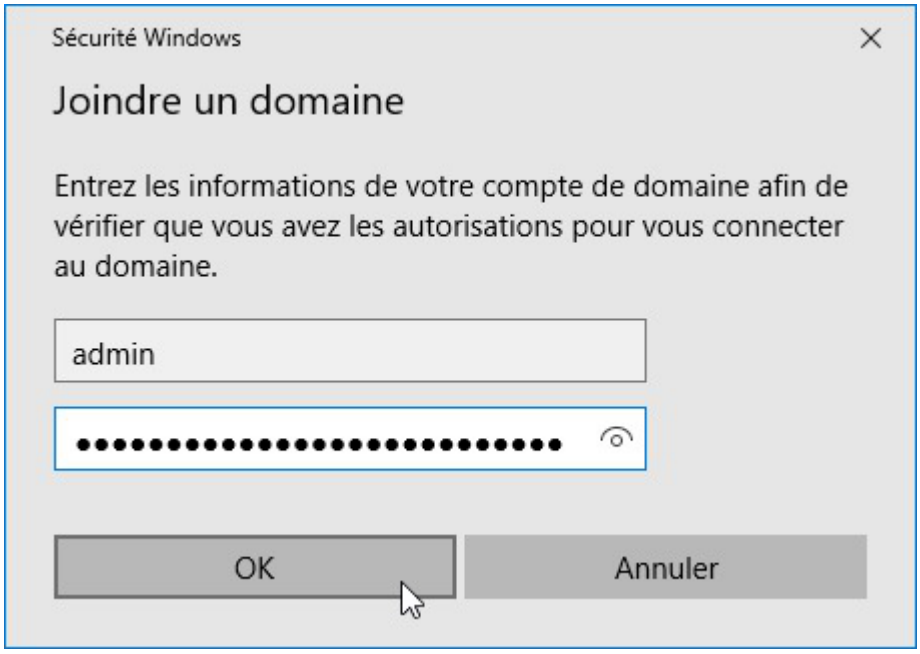


- Cliquer sur `Joindre cet appareil à un domaine Active Directory local` ;

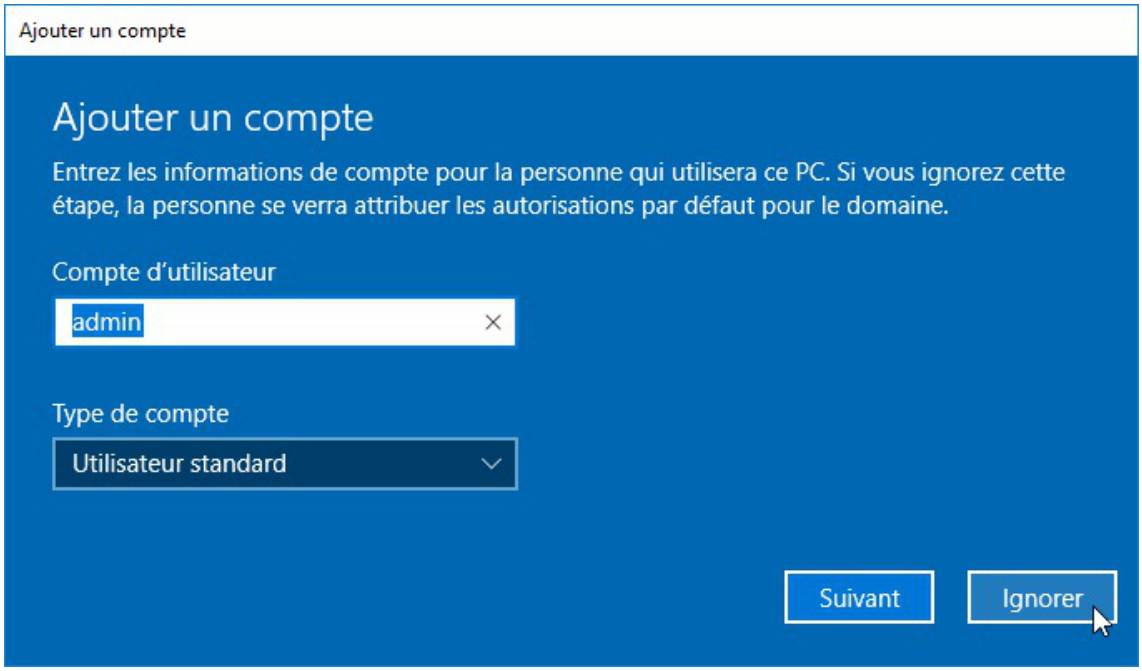


- Saisir le nom du domaine et cliquer sur `Suivant` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

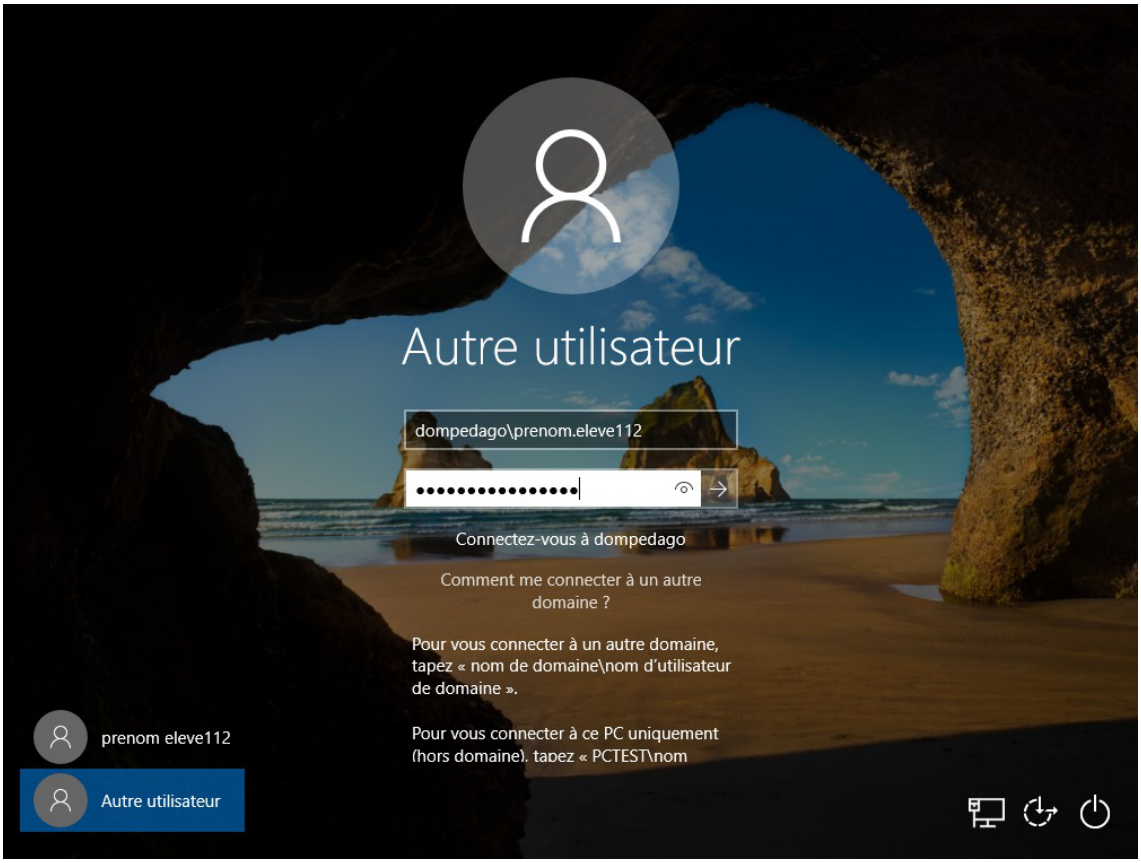


- Saisir le nom du compte administrateur du domaine ainsi que la clé secrète ("mot de passe") associée au compte et cliquer sur le bouton `OK` ;



- 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"
```

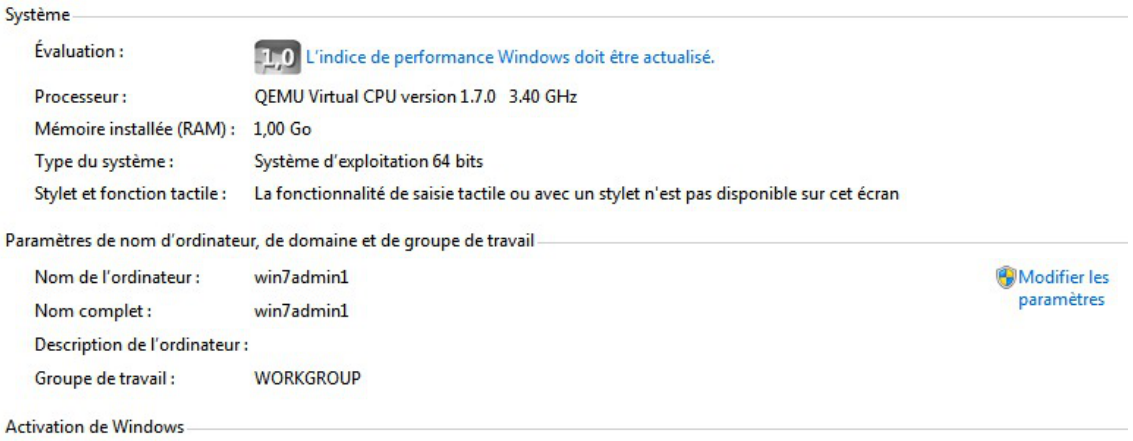
Un fichier `Win7_Samba3DomainMember.reg` est mis à disposition pour modifier la base de registre dans `/home/esu/Console/`.

Jonction au domaine

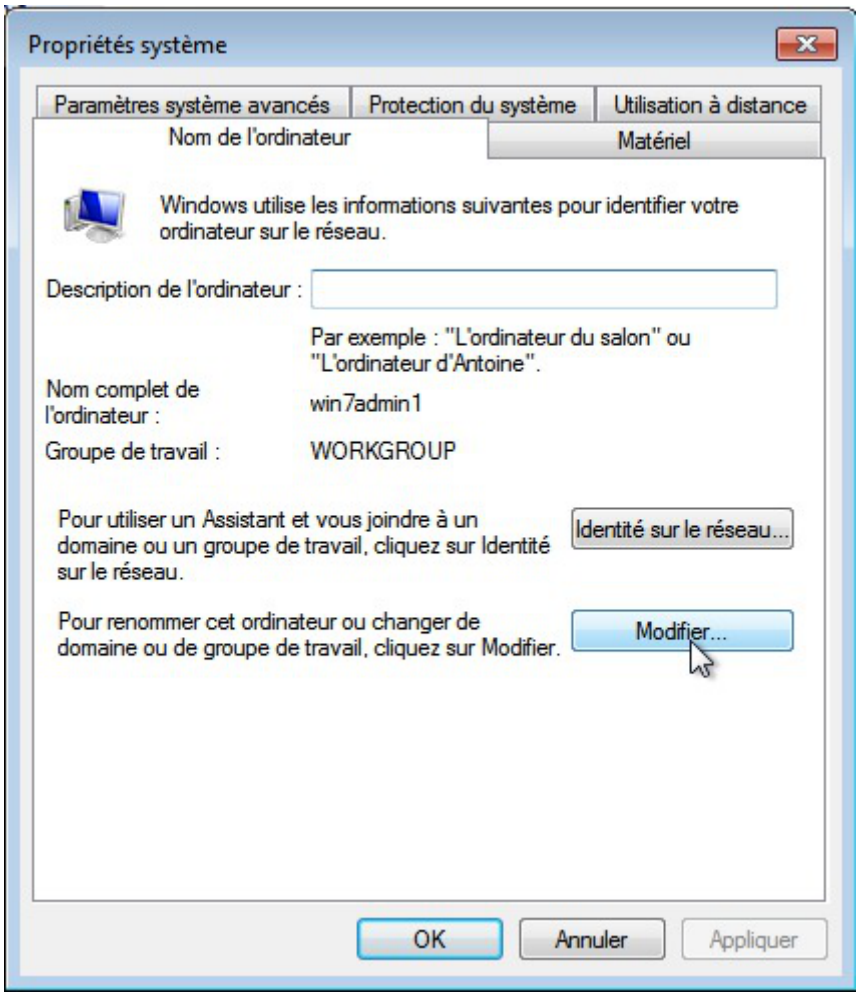
Ajoutez la station au domaine de la façon suivante :

- 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)

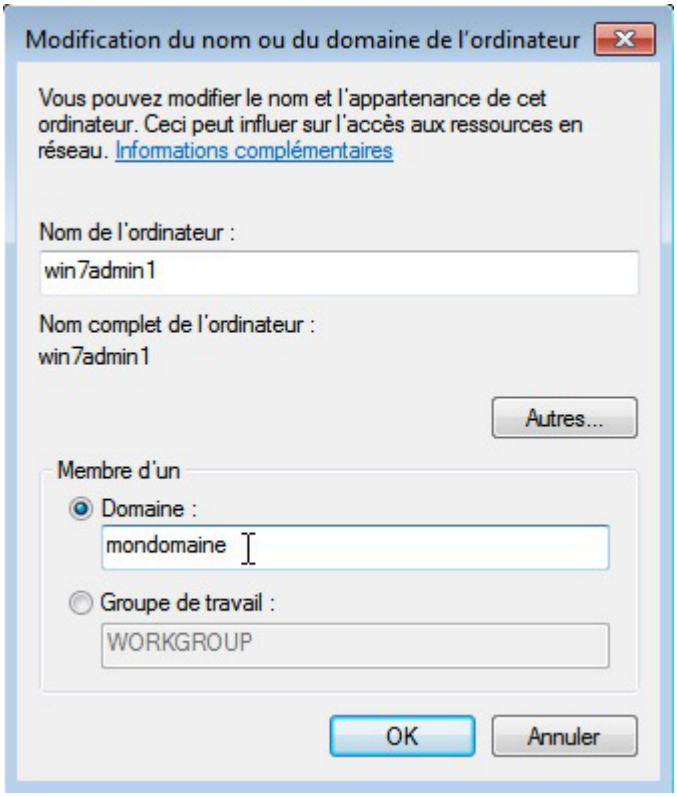


- Cliquer sur Modifier les paramètres ;

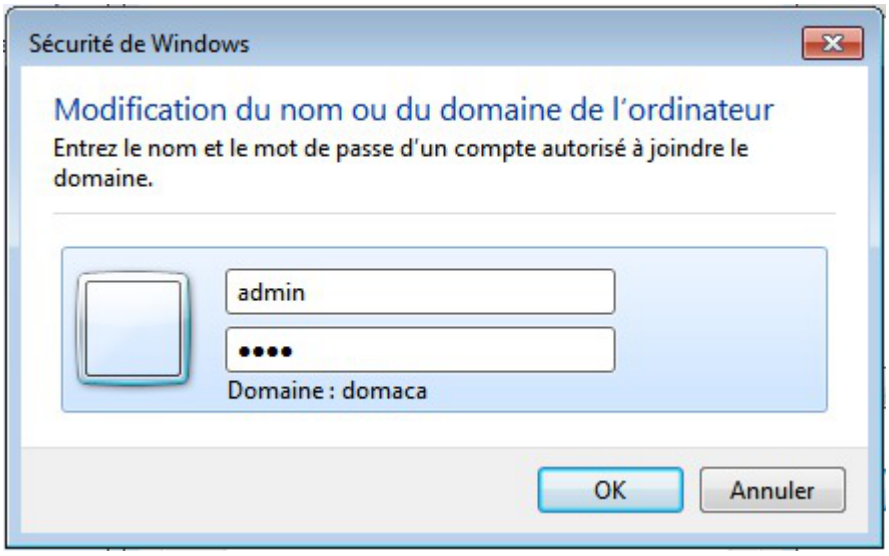


- Cliquer sur le bouton Modifier... ;

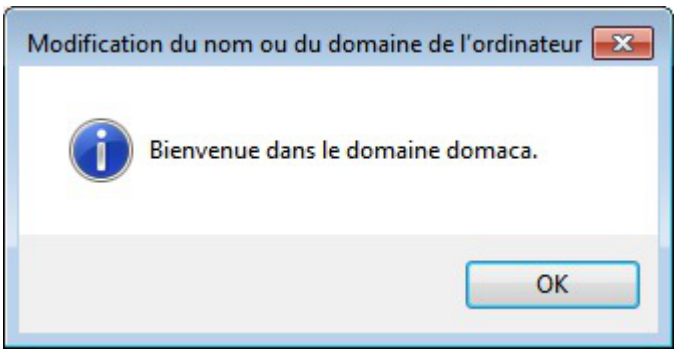
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Renseigner le nom de domaine Samba et cliquer sur `OK` ;

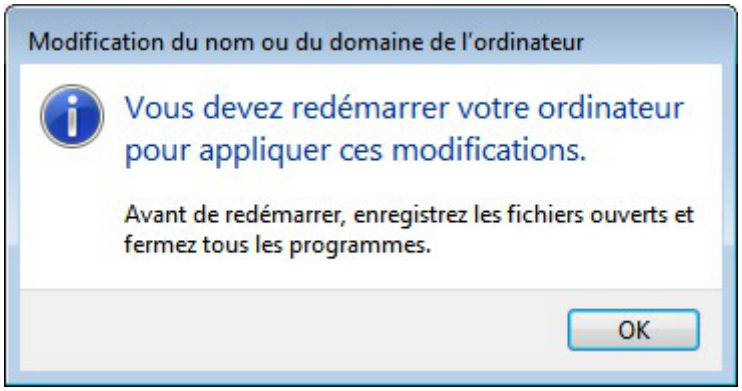


- Utiliser le compte `admin` ou un compte ayant les droits suffisants pour finaliser l'intégration ;

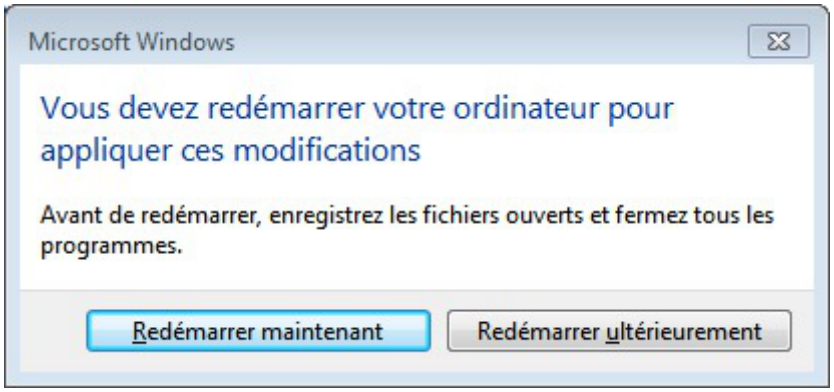


- Confirmer le message de bienvenue ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Confirmer le message d'avertissement ;



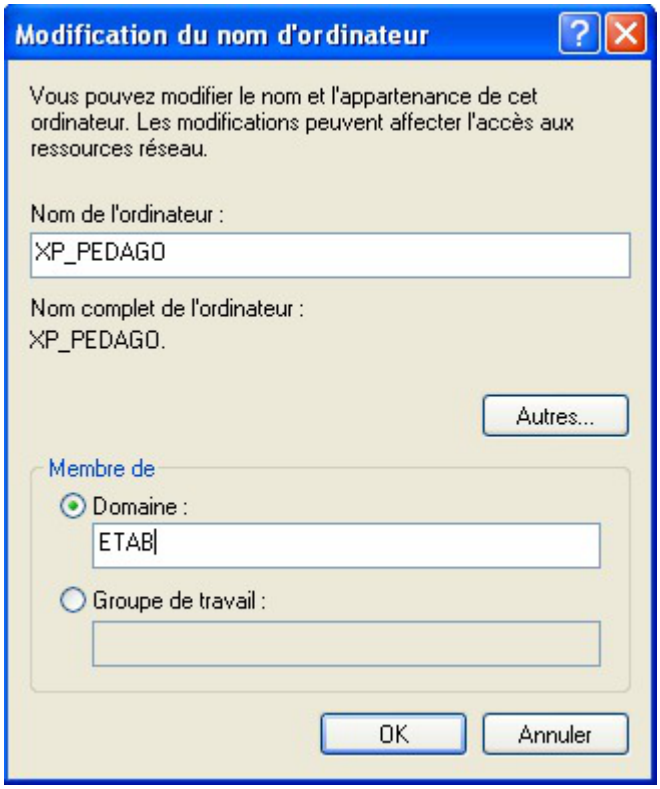
- Redémarrer maintenant.

Intégration au domaine pour Windows XP

Ajoutez la station au domaine de la façon suivante :

- clic droit sur le `Poste de travail` ;
- `Propriétés` ;
- onglet `Nom de l'ordinateur` ;
- cliquer sur `Modier...` ;
- sélectionner `◉ Domaine` :
- dans `Membre de` renseigner le nom du `◉ Domaine` ;
- valider : utiliser *admin* ou un compte ayant les droits suffisants pour finaliser l'intégration ;
- redémarrer.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Intégration manuelle au domaine

Installation du client Scribe

Pré-requis à l'installation du client Scribe

Le service pack 3 pour Windows XP est recommandé pour un fonctionnement correct du client Scribe.

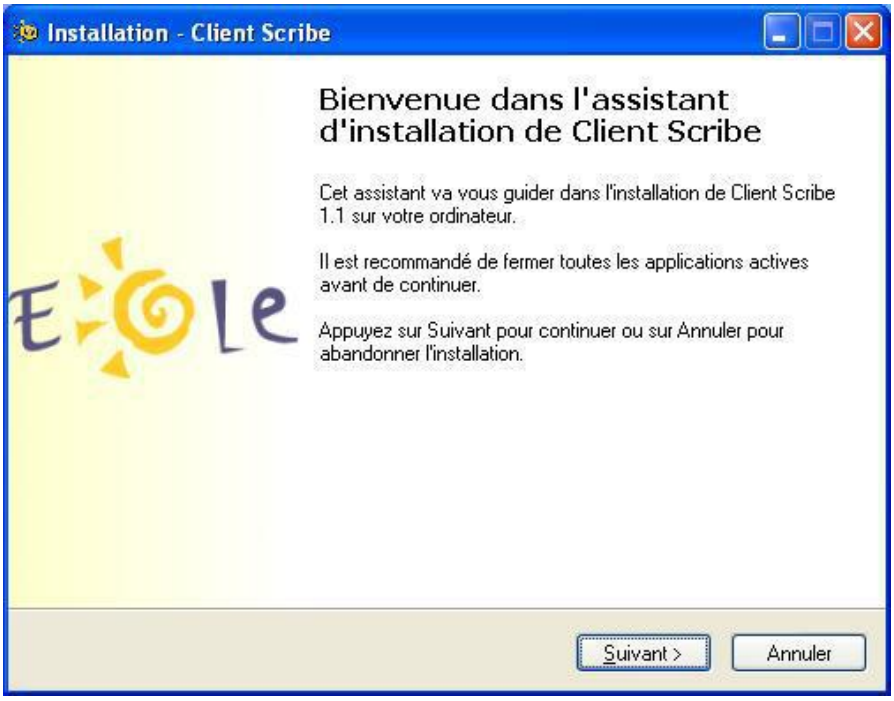
Windows Vista est compatible avec l'ensemble des applications.

Il est indispensable que la station soit mise à l'heure avant son intégration au domaine, pour cela exécutez la commande `net time /SET /YES \\<adresse ip scribe>`.

Installation manuelle du client

L'installeur du client possède un raccourci accessible avec l'utilisateur **admin** dans `U:\Install_Client_Scribe`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Installation du client Scribe

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"

Versions 64 bits

Pour les versions 64 bits de Windows 7, une version spécifique du client Scribe avait été diffusée.

Depuis, les deux installeurs ont été fusionnés et l'exécutable `cliscribe-setup.exe` détecte

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

automatiquement l'architecture du système.

Windows 2000

L'installeur du client Scribe utilise le programme `sc.exe`. Les utilisateurs de windows 2000 trouveront cet exécutable dans le windows 2000 resource kit [http://support.microsoft.com/kb/927229].
`sc.exe` peut aussi être copié depuis windows XP dans `%WINDIR%\System32`.

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.

4.1.5. Mise à jour du client Scribe

Le client Scribe installé sur les stations Windows est automatiquement mis à jour si une nouvelle version est disponible sur le serveur. L'installeur du client Scribe 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 Scribe, le fichier `%WINDIR%\Eole\install.ini` est créé. Ce fichier contient la version du client installé ;
- 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_scribe/install.ini`. (lié pour "*admin*" dans `U:\client\install.ini`).

Les opérations effectuées par le service de mise à jour du client Scribe sont journalisées dans `%WINDIR%\cliscribe_updater.log`.

Le service de mise à jour du client Scribe 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 Scribe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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.

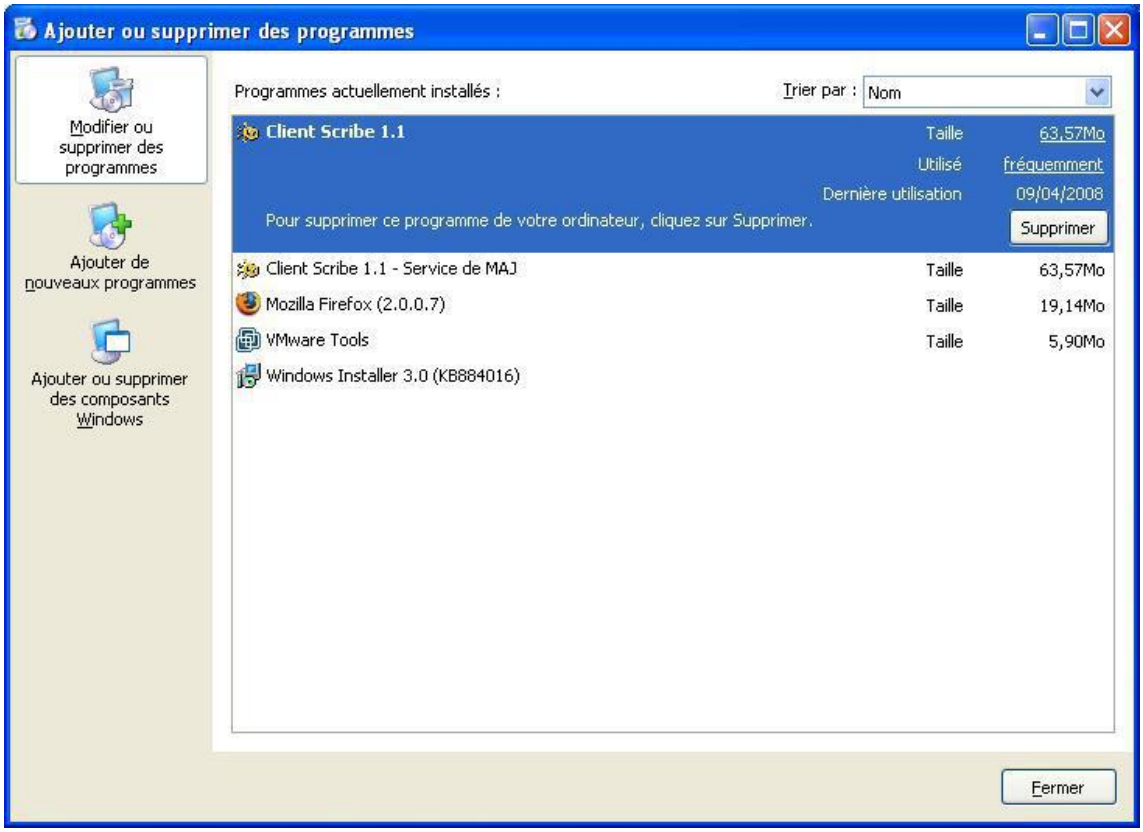
Aucune aide ne pourra être apportée si le client n'est pas à jour.

4.1.6. Désinstallation du client Scribe

La désinstallation du client Scribe s'effectue dans :

- `Panneau de configuration`
- `Ajout/Suppression de programmes`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Désinstallation du client Scribe

Le client Scribe 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.

4.2. Administration des clients Windows

Afin de faciliter l'administration des clients, divers outils ont été développés et installés sur le module Scribe :

- **ESU**, configuration du poste client et de l'environnement de l'utilisateur, composé d'une console et d'un client ;
- **Gestion-postes**, action sur les élèves par les professeurs (observation/diffusion de poste, blocage temporaire, ...) ;
- l'**EAD**, action sur les postes et les utilisateurs.

Fonctionnement général sous Windows

Sur un module Scribe 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- installation du poste client ;
- intégration au domaine Scribe ;
- installation du client Scribe ;
- utilisation.

À cet instant les utilisateurs peuvent utiliser le poste client. Le module Scribe est livré avec une configuration ESU par défaut sous la forme d'un groupe de machine "**grp_eole**" comportant trois groupes d'utilisateurs : **DomainAdmins**, **professeurs** et **eleves**.

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.901] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

4.2.1. L'ouverture de session

Le client Scribe/ESU fonctionne sous forme de service. Ce service est accompagné de deux applications s'exécutant dans l'environnement de l'utilisateur à l'ouverture de session.

En plus d'appliquer la configuration ESU, le client Scribe gère l'observation et la diffusion de l'écran du poste, le blocage Internet et le "mode devoir", l'arrêt, le redémarrage et la fermeture forcée de session depuis l'EAD.

Lorsqu'un utilisateur du domaine Scribe ouvre une session sur un poste Windows, un ensemble d'actions sont effectuées. Certaines sont des mécanismes internes à Windows, d'autres sont spécifiques à Scribe.

Après qu'un utilisateur du domaine ait validé son mot de passe la session s'ouvre :

- le profil de l'utilisateur est installé ;
- exécution de `%WINDIR%\Eole\cliscribe\logon.exe`.

Le programme `logon.exe` effectue les actions suivantes :

- lecture du fichier `\\<scribe>\netlogon\<login>\WinXP.txt` et exécution des instructions ;
- requête sur le serveur pour :
  - l'application des règles ESU ;
  - l'application du blocage ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- l'application du mode d'observation (vnc_viewonly).

Simulation d'ouverture de session

Lors de la mise en place de la configuration d'ESU, il est souvent nécessaire de ré-ouvrir une session pour tester les nouveaux paramétrages.

La ré-application des règles sans avoir à ré-ouvrir une session peut se faire avec :

`Démarrer => Exécuter => "%WINDIR%\Eole\cliscribe\logon.exe"`

Généralités sur les scripts personnalisés

Il est possible d'ajouter des commandes à exécuter à l'ouverture de session.

Ces commandes doivent être renseignées dans un fichier `.txt` se trouvant dans un des sous-répertoire de `\\<scribe>\netlogon\scripts`.

Ces scripts peuvent être ajoutés pour :

- un utilisateur → `/home/netlogon/scripts/users/admin.txt` ;
- un groupe → `/home/netlogon/scripts/groups/eleves.txt` ;
- une machine → `/home/netlogon/scripts/machines/poste01.txt` ;
- un OS (Win95, Win2K, WinXP, Samba, Vista) → `/home/netlogon/scripts/os/WinXP.txt` ;

Windows 7 et Windows 10 sont traités de la même manière que Windows Vista *(OS=Vista)*.

Les noms de machines doivent être écrits en minuscules.

- un OS et un utilisateur → `/home/netlogon/scripts/os/Win2K/admin.profil.txt` ;
- un OS et un groupe → `/home/netlogon/scripts/os/WinXP/professeurs.txt`.

Les scripts personnalisés sont concaténés dans le script principal, par défaut au début de celui-ci. Si des instructions doivent être effectuée après (nécessité d'avoir accès au lecteur `commun` par exemple), placez la balise **%%NetUse%%** et ajoutez les instructions ensuite.

L'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.

Pour éditer les fichiers personnalisés sous Windows, il est recommandé d'utiliser `Notepad++` à la place.

Lors de la personnalisation d'un script d'ouverture de session il peut être tentant d'utiliser un système d'élévation de pouvoir afin d'installer et paramétrer des applications. Le problème de cette élévation de pouvoir est qu'elle utilise un compte Windows local. En cas d'accès à un partage du serveur Scribe, la connexion se fait avec le compte de la machine (`sevenk64-1$`) et non avec le compte de l'élève (`eleve.test`) ou de l'enseignant (`enseignant.test`) qui se connecte.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Scripts personnalisés pour exécuter des commandes

Pour exécuter des commandes il faut utiliser l'instruction `cmd`.

Par défaut le programme d'ouverture de session affiche le programme et attend la fin de son exécution pour continuer. Un programme qui ne se ferme pas (ex. notepad.exe) provoquera des ouvertures de session très longue et incomplètes.

- l'option NOWAIT permet de ne pas attendre la fin de l'exécution du programme ;
- l'option HIDDEN permet de masquer la fenêtre.

Le format est :

cmd,commande,[options]



Exécuter *notepad.exe* pour l'utilisateur *user.assr* lorsqu'il ouvre une session sur un poste Windows XP :

Fichier *<scribe>**netlogon**scripts**os**WinXP**user.assr.txt* :

```
cmd,%WINDIR%\notepad.exe,NOWAIT
```

Scripts personnalisés pour monter des lecteurs

Pour monter des lecteurs il faut utiliser l'instruction `lecteur`.

Si la lettre spécifiée est déjà utilisée par une ressource réseau, celle-ci est déconnectée avant ré-utilisation de la lettre pour la nouvelle ressource. Dans le cas contraire (lecteur local, clé USB, CD-Rom, lecteur carte, etc.), la première lettre disponible est utilisée.

Le format est :

lecteur,lettre:,partage



Monter le partage *monserveur**partage* sur la lettre *V:* pour tous les utilisateurs du domaine :

Fichier *<scribe>**netlogon**scripts**groups**DomainUsers.txt* :

```
lecteur,V:,\\monserveur\partage
```

4.2.2. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 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.

4.2.2.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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 ;
- 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`.

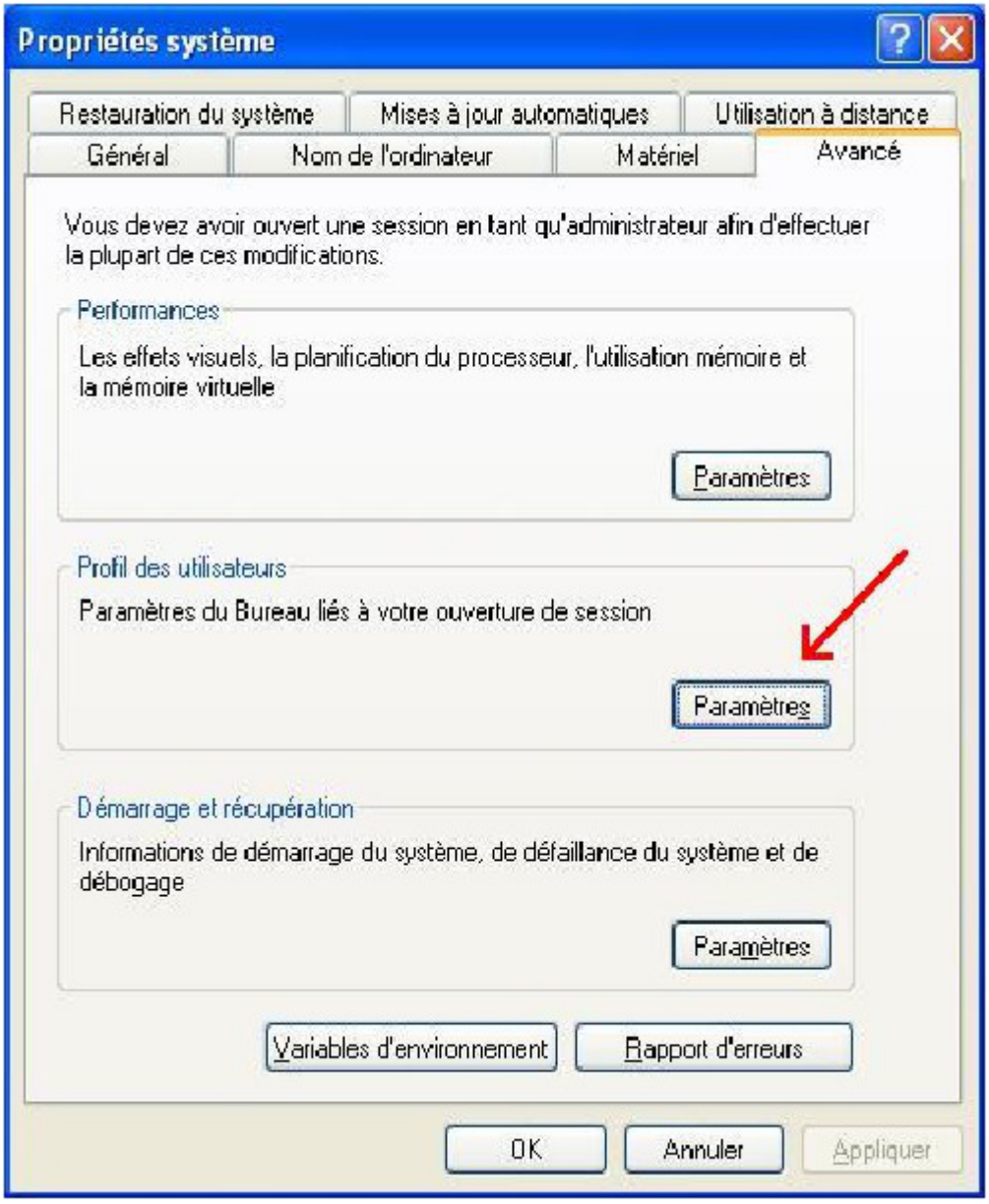
Ces dernières informations sont donc retrouvées lors de la prochaine ouverture de session.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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`.



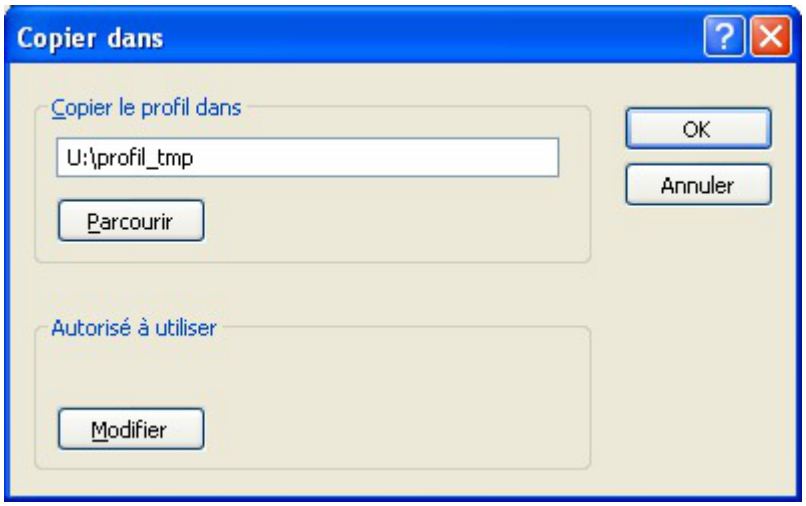
Dans la partie `Autorisé à utiliser` cliquer sur `Modifier`. Entrer `tout le monde` puis cliquer sur `Vérifier les noms`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Et cliquer sur OK.

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

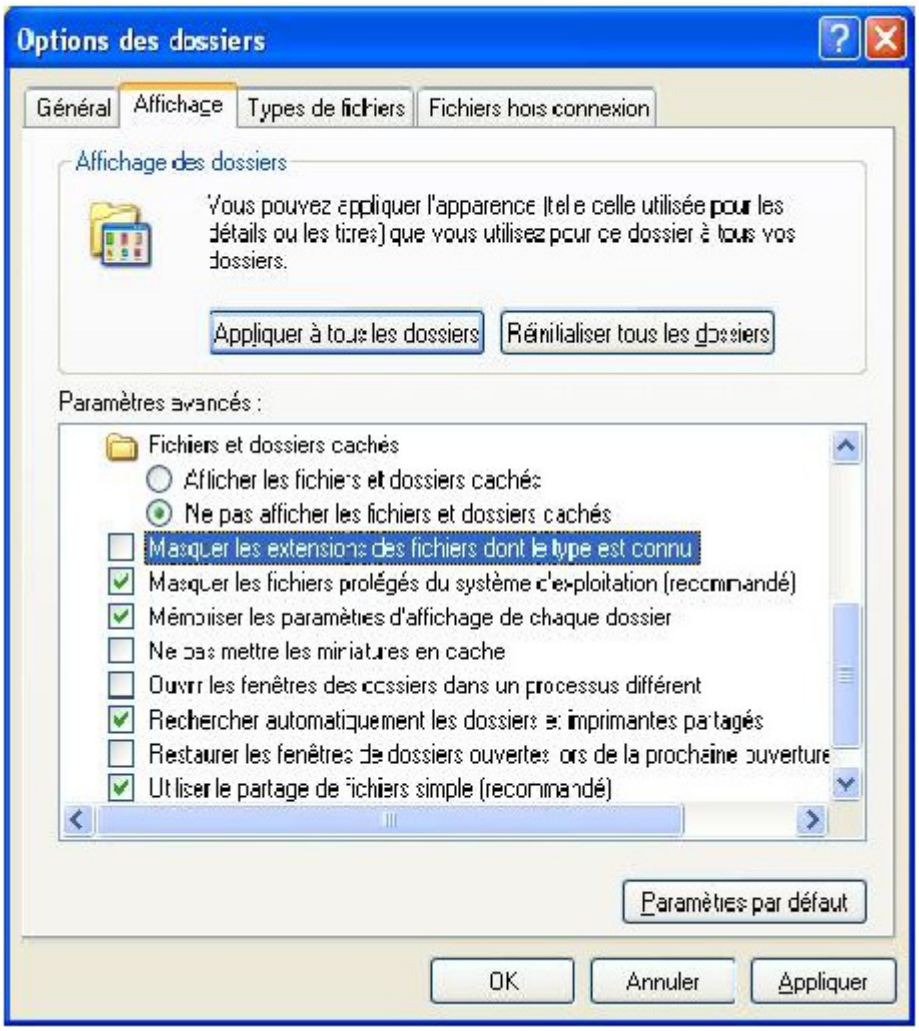
Ceci permet de spécifier un profil différent pour certains utilisateurs (ex. : profil pour les professeurs et profil2 pour les élèves).

> 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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`").



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.

4.2.2.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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une des solutions permettant de contourner le problème est d'utiliser un utilitaire nommé `Windows Enabler`.

- http://www.yamprod.net/index.php?tag/Windows%207%20Seven%20profil%20copy%20copie%20prc
- http://www.angelfire.com/falcon/speedload/Enabler.htm

Sous Windows 7 SP1, pour que `Windows Enabler` fonctionne, il faut impérativement désactiver l'UAC[p.903] 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.

4.2.2.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.903]AC[p.903].

Le programme `logon.exe` affiche alors la question : `Ré-initialiser le Menu démarrer et le Bureau` ? suivit par celle de l'UAC[p.903] (si il est activé) pour la validation de l'action.

L'UAC[p.903] 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.2.3. Gestion des configurations clientes avec ESU

4.2.3.a. Introduction

Présentation

ESU[p.889] 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.

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.

4.2.3.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 ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 :

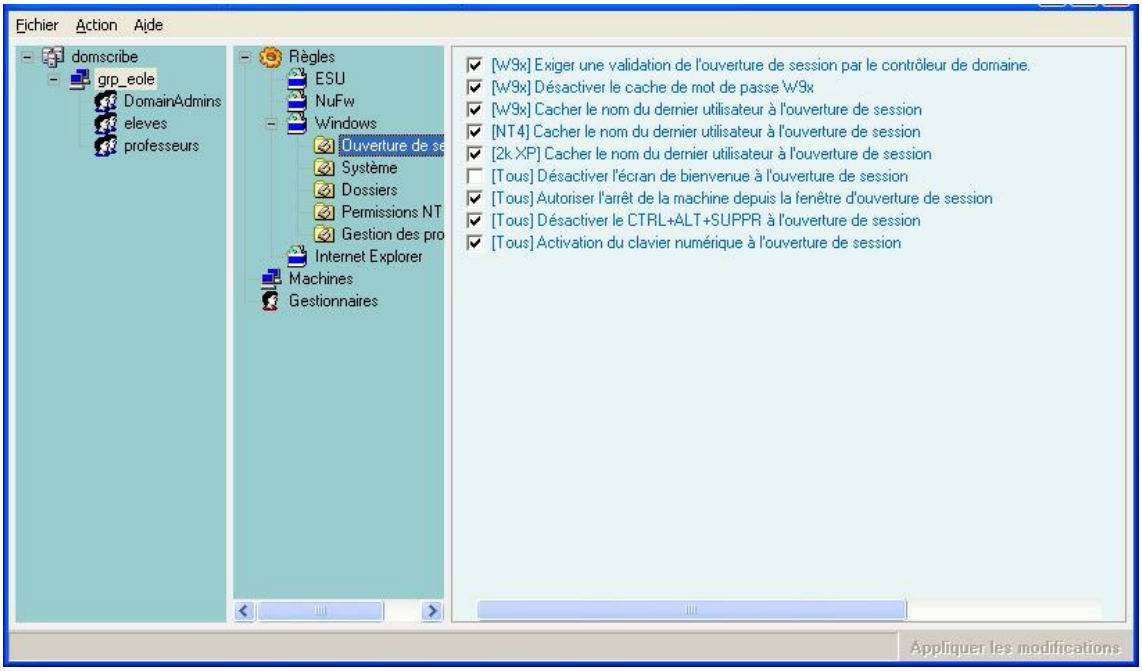
- la première liste les groupes de machines du domaine, et les utilisateurs/groupes gérés dans ce groupe de machines ;
- la seconde contient les différentes catégories de règles. Ces catégories peuvent comporter des sections ;
- la troisième partie affiche les règles et leur paramétrage.

La première colonne montre l'organisation générale d'ESU. La première ligne indique le nom du domaine.

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 "*****").

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.



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

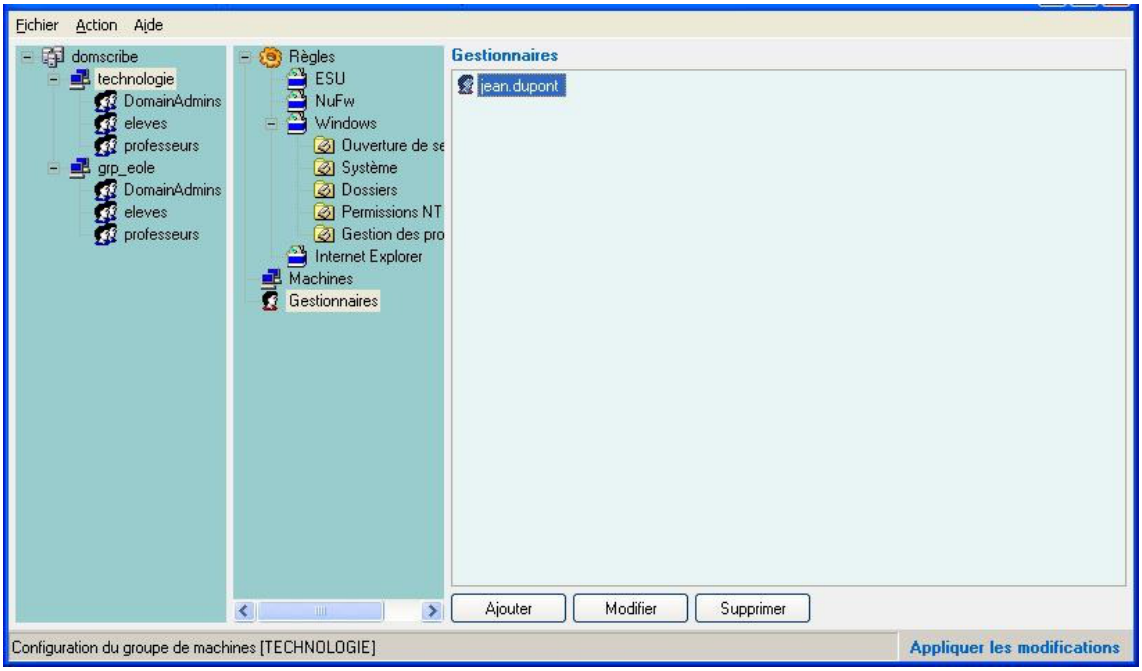
Les Gestionnaires

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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>\`).



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

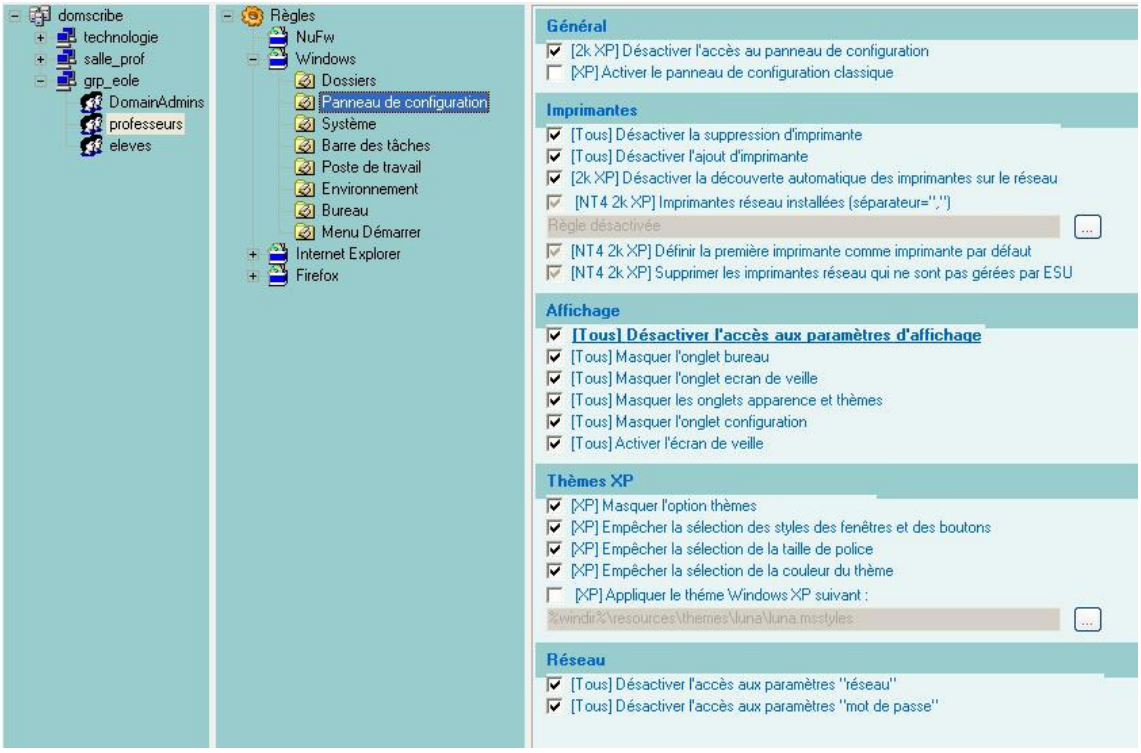
Les membres du groupes DomainAdmins ont un accès complet à la console Esu sans qu'il ne soit nécessaire de les ajouter comme gestionnaires.

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.

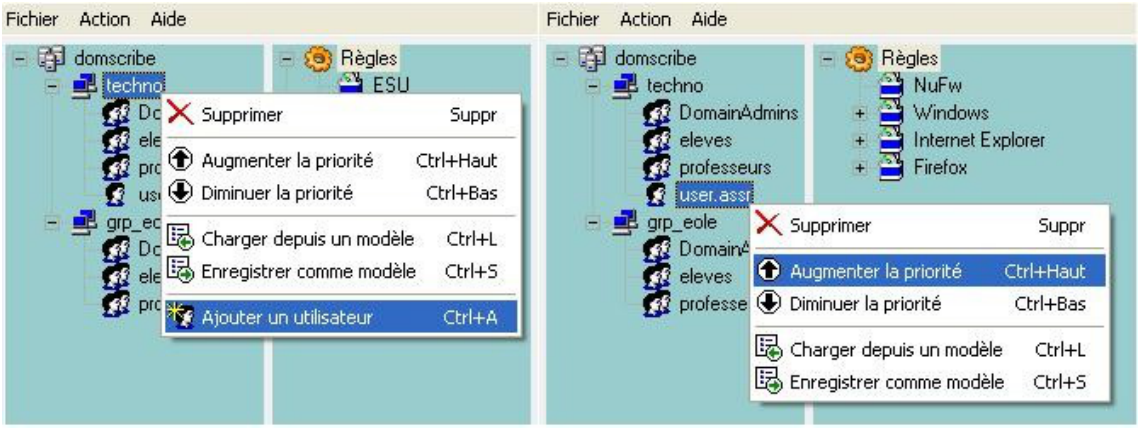
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

Ceci ne concerne pas les postes Windows Me et inférieur et nécessite l'utilisation de ESU.

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.

Voir aussi...

Onglet Esu : Configuration du proxy ESU

> 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)

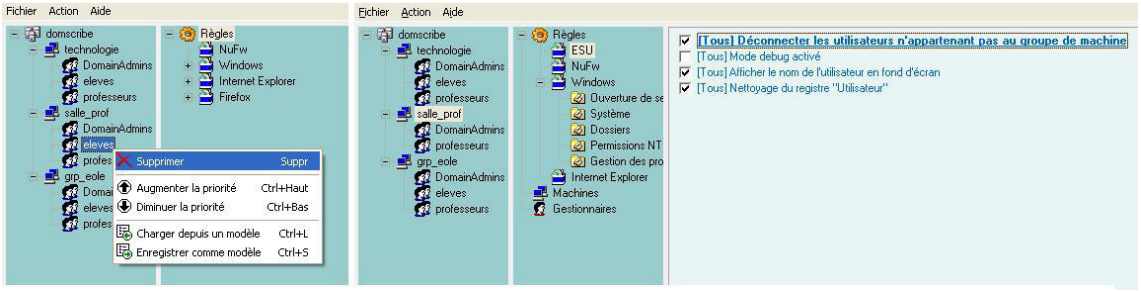


Configuration ESU des options Firefox

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

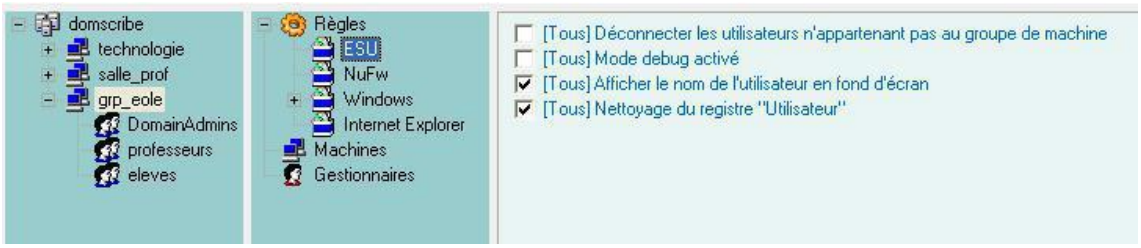
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_DomainAdmins[Scribe].xml
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_eleves[Scribe].xml
- U:\esu\Console\Modeles\GU\GroupeUtilisateur_professeurs[Scribe].xml

Ces modèles peuvent être utilisés lors de l'ajout d'un utilisateur ou d'un groupe dans un groupe de machines (ex. *user.assr*).

4.2.3.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 se fait par utilisateur/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*, créez 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%

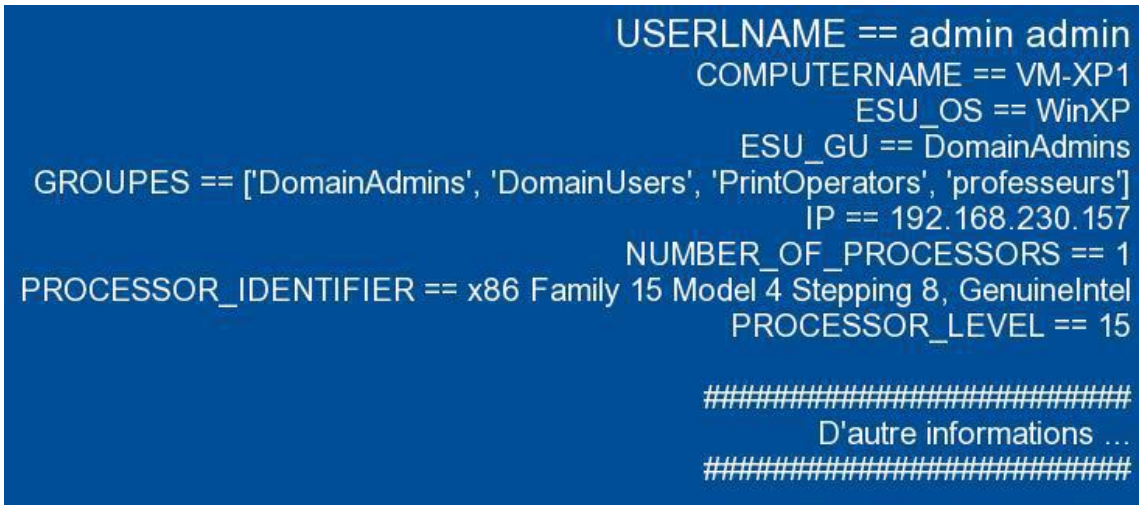
Exemple de configuration personnalisée du texte en fond d'écran

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)

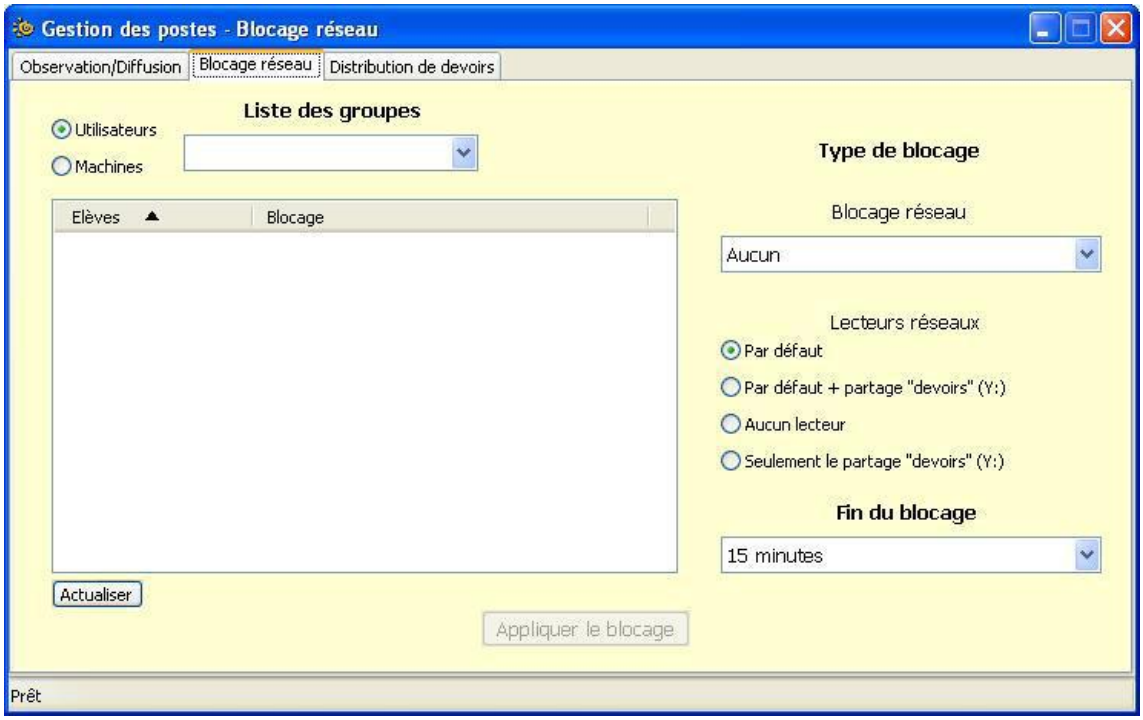
D'autre informations ...
##########################
Résultat :



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.

4.2.4. L'application Gestion-postes

Gestion-postes est une application pour le système d'exploitation Microsoft Windows, accessible uniquement par les enseignants (`P:\Gestion-postes`) qui permet diverses opérations sur une sélection de postes ou d'utilisateurs.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'application propose trois outils accessibles via trois onglets :

- le premier onglet sert à l'observation et la diffusion d'un poste. Il n'est possible d'observer que des élèves, en revanche un professeur peut diffuser son poste sur celui d'un autre professeur. Il est bien entendu indispensable que l'observateur et l'observé soient tous les deux connectés ;
- le second onglet contient le "*mode devoir*" : blocage de l'accès aux partages et/ou à Internet pour des élèves. Il **n**'est **pas** indispensable que les élèves à bloquer soient connectés. Le blocage s'appliquera dès leur ouverture de session ;
- le troisième onglet permet de distribuer des documents. Ces documents peuvent être distribués à tous les groupes (niveau, classe, équipe pédagogique, matière, groupe...) et peuvent être accompagnés de données en lecture seule qui ont l'avantage de ne pas être dupliquées sur le serveur.

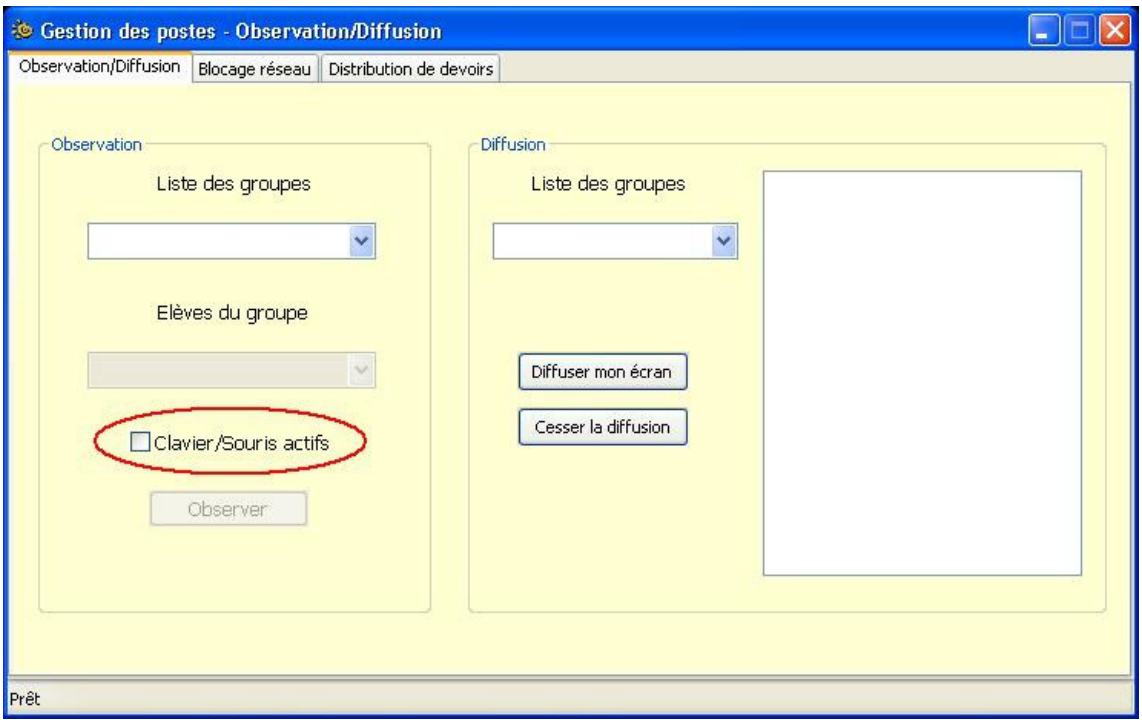


Il n'existe pas d'équivalent pour des clients GNU Linux. Par contre, l'application EOP est accessible au travers d'un navigateur web.

4.2.4.a. Observation / Diffusion du poste

Observation

L'observation consiste à afficher le poste d'un élève dans une fenêtre sur le poste du professeur. La sélection d'un élève à observer se fait par classe ou par groupe, seuls les élèves connectés sont listés.



Observation, activation de la prise en main du poste (clavier et souris de l'observateur actifs)

La liste des élèves connectés affiche l'identifiant de l'élève et le nom de la machine sur laquelle il est connecté.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Une fois l'élève sélectionné, cliquer sur Observer. La requête est transmise au serveur et à la station de l'élève ce qui peut prendre quelques instants.

L'application permet d'observer plusieurs élèves en même temps, cependant le nombre dépend de la qualité et de la vitesse du réseau.

Le niveau d'observation VNC[p.904] est paramétrable dans l'EAD : Outil / VNC.



Trois niveaux d'observation :

- Désactivé ;
- Visualisation simple ;
- Visualisation et contrôle.

En mode *Visualisation et contrôle*, l'utilisateur pourra choisir via la coche *Clavier/Souris actifs* s'il veut pouvoir prendre la main sur la station élève.

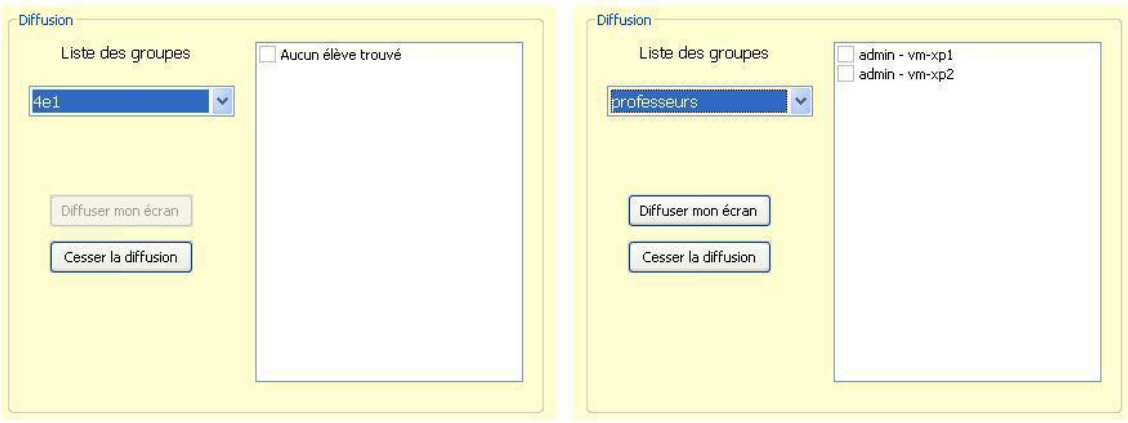
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Une ré-ouverture de session sur le poste client est nécessaire afin de prendre le changement du mode de contrôle de VNC en compte.

Diffusion

La diffusion est l'affichage du poste du professeur sur un ou plusieurs postes élève et/ou professeur. La sélection se fait par classe, par groupe ou par membre du groupe *professeurs*. Comme pour l'observation, seuls les utilisateurs connectés sont listés.



Le bouton `Cesser la diffusion` arrête la diffusion immédiatement sur tous les postes.

Toute nouvelle diffusion (nouveau clic sur le bouton `Diffuser mon écran`) **interrompra** la diffusion précédente.



La qualité du réseau influe directement sur le nombre maximum de diffusions simultanées possibles.

4.2.4.b. Bloquer Internet / Masquer les partages (Mode devoir)

Les professeurs peuvent restreindre l'accès à Internet et/ou aux partages ainsi que monter le partage *devoir* pendant une période donnée.

Ces restrictions sont appliquées immédiatement si l'élève est connecté, sinon elles sont appliquées à l'ouverture de session.

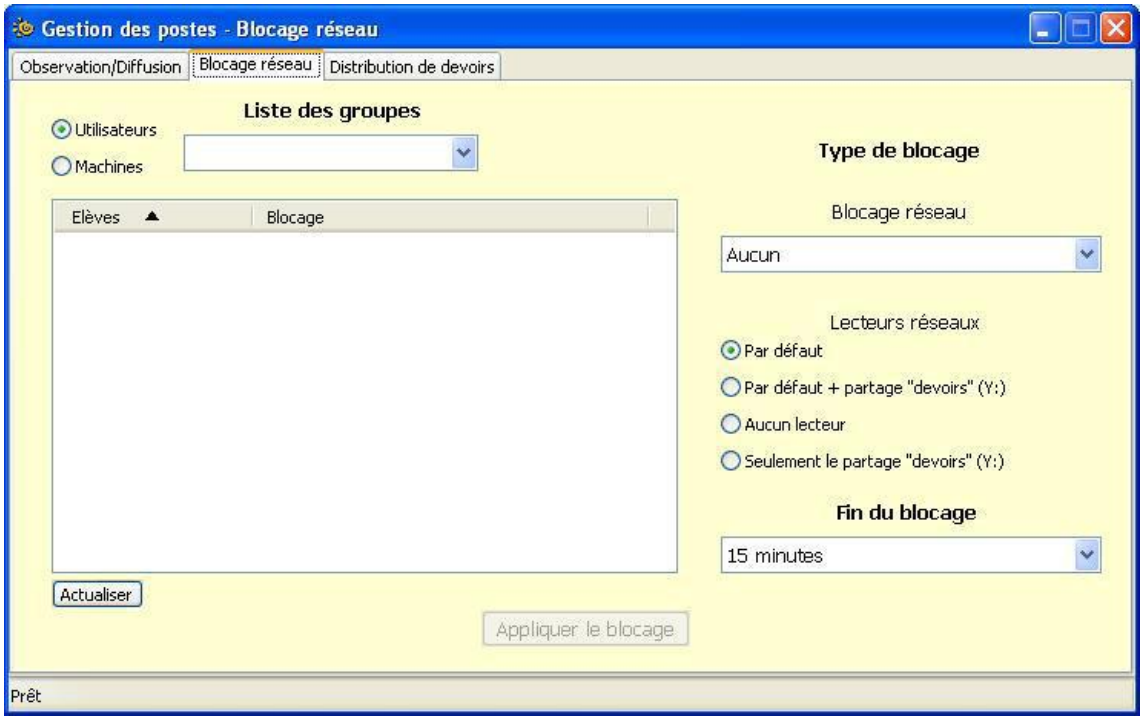
Lorsque la période d'interdiction est écoulée l'environnement de l'élève est automatiquement remis en mode normal s'il est encore connecté.

Blocage Internet

La sélection du blocage Internet se fait via la liste déroulante `Type de blocage`.

Le blocage Internet interdit tous les accès réseau en dehors des services DNS, VNC et du service Samba (ports 137-139 et 445) à destination du module Scribe. Cela afin de permettre l'ouverture d'une session sur le domaine et d'accéder aux partages. Aucun accès à internet, direct ou par proxy, n'est possible.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le blocage réseau peut s'appliquer à un utilisateur ou à une machine.

Il est possible de sélectionner plusieurs utilisateurs en même temps en gardant la touche Maj ou Ctrl enfoncée.

Masquer les lecteurs réseaux

En plus du blocage de l'accès à Internet, l'application permet de masquer les lecteurs réseau spécifiques au module Scribe pour une durée donnée afin que l'élève n'ait plus accès à son dossier personnel ni aux dossiers groupes et dossiers communs (choix `Aucun lecteur réseau`).

Les documents sont distribués dans le dossier "devoirs" situé sur le serveur. Il est accessible en chemin UNC [p.904] par \\<adresse_du_serveur>\<login_utilisateur>\devoirs

L'application propose de monter ce dossier comme nouveau lecteur nommé `Y:`

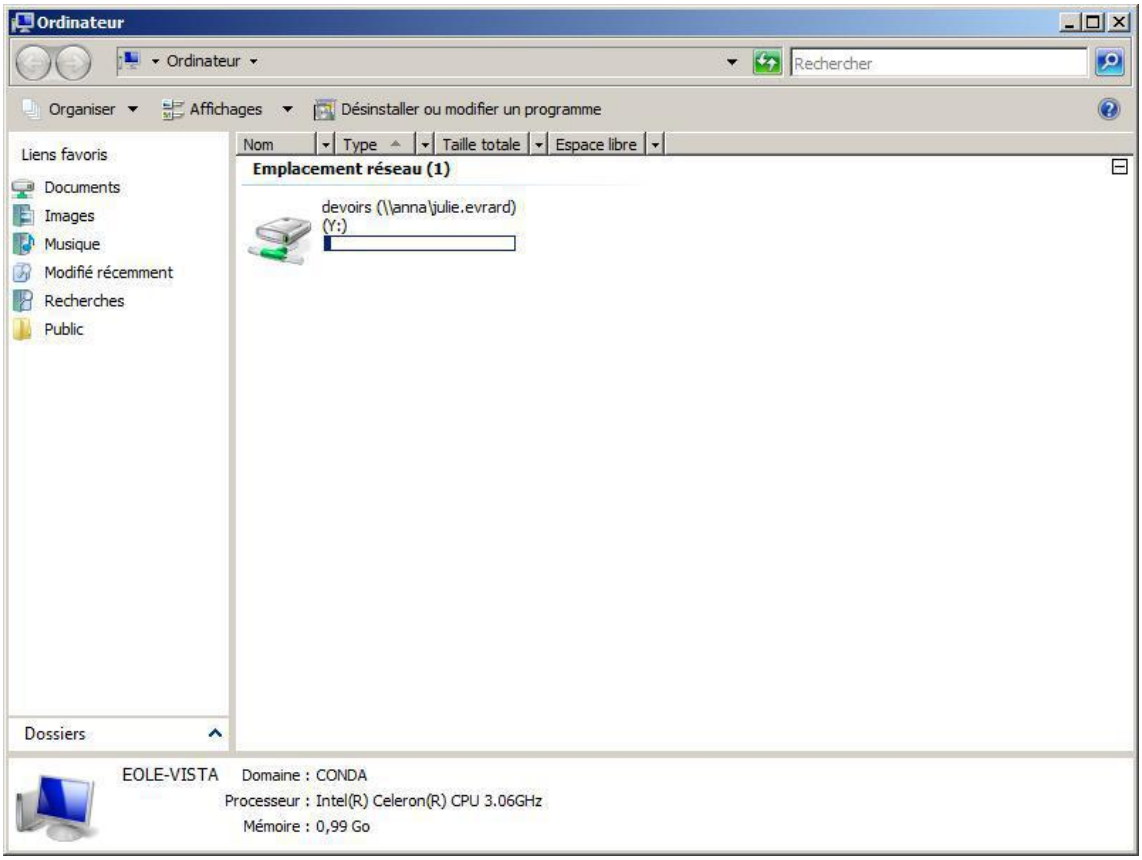
Sélectionner le bouton radio `Seulement le partage "devoirs"` masquera tous les lecteurs puis connectera le dossier "devoirs" de l'utilisateur au lecteur `Y:` dans le poste de travail.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur et l'empêche de diffuser ou de récupérer le ou les documents. Aucun utilisateur ne peut donc prendre connaissance des documents à l'avance.

Pour masquer tous les lecteurs et connecter le dossier "devoirs" de l'utilisateur au lecteur `Y:` il faut sélectionner le bouton radio `Seulement le partage "devoirs"`.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur. Cela l'empêchera de récupérer et de diffuser le devoir vers d'autres utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Comme pour le blocage de l'accès Internet, le masquage des partages a une durée limitée. À la fin de cette période, si l'élève est encore connecté sur un client, il retrouvera son environnement initial automatiquement.

Gestion-postes offre la possibilité de spécifier une liste de lecteurs à afficher même si l'un des choix `Aucun lecteur` ou `Seulement le partage "devoirs"` a été fait. Pour ce faire il faut placer un fichier nommé `lecteurs.txt` dans `P:\gestion-postes\`

Le fichier doit contenir une liste de lettres de lecteur à afficher sans les deux points ":" et séparées par des virgules ",".

Exemple de contenu du fichier `lecteurs.txt` :

```
c,d,s
```

4.2.4.c. Distribution de devoirs

La distribution peut être composée de deux éléments :

- le ou les documents sous forme d'un ou plusieurs fichiers. Ils seront copiés dans chacun des dossiers personnels `devoirs`/ `nom_de_l'enseignant` / `<nom_du_devoir>` des utilisateurs du groupe sélectionné. Les utilisateurs auront un accès en lecture et en écriture à ces fichiers (modification/suppression) ;
- les données jointes au(x) document(s) qui sont des fichiers supplémentaires dont la modification est impossible. Ils sont copiés une seule fois à un endroit spécifique du serveur. Des liens symbolique vers ces fichiers sont créés dans le sous-répertoire `donnees` du répertoire `devoirs`/ `nom_de_l'enseignant` / `nom_devoir` de chacun des utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Si la distribution de document est un travail éducatif, la distribution s'effectue en suivant les 4 étapes suivantes :

- distribuer ;
- ramasser ;
- rendre : distribution des devoirs corrigés ;
- supprimer : effacement des fichiers du devoir.

Distribuer

La distribution de document commence par la sélection d'un ou plusieurs fichiers dans `Devoir à distribuer`. L'ajout de fichiers dans `Donnée` est facultatif, ces fichiers supplémentaires accompagneront le devoir mais leur modification sera impossible.

Il faut nommer le devoir dans le champ `Nom du devoir` , c'est sous ce nom qu'il apparaîtra pour l'utilisateur et pour le gérer (ramassage).

Ensuite il faut sélectionner le groupe auquel le devoir doit être distribué. Tous les groupes sont présents dans la liste, y compris les groupes incluant des utilisateurs *professeurs*.

La case `Uniquement aux élèves du groupe` est cochée par défaut. Décochée, elle permet d'envoyer les documents aux autres membres du groupe, comme par exemple aux enseignants.

Par défaut, l'option `Dans le dossier 'perso\devoirs'` étant sélectionnée, les documents seront distribués dans le répertoire personnel des utilisateurs.

L'option `Dans le partage 'devoirs' (non accessible par défaut)` permet de préparer la distribution différée de documents. Ce travail de préparation peut donc se faire aussi bien à l'extérieur qu'à l'intérieur de l'établissement. La distribution ne sera effective qu'au travers du logiciel `Gestion-postes`.

Cliquer sur `Distribuer`, une boite de dialogue affiche le nombre de devoirs prêts à être distribués et demande confirmation.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Lorsque la distribution est terminée, un message affiche le nombre de documents effectivement distribués et le nom du répertoire de stockage. Ce nom est automatiquement associé au devoir, il correspond à <identifiant_du_distributeur>-<numéro_devoir>. Ce sous-dossier est présent dans le répertoire "devoirs" de l'utilisateur. Il contient l'ensemble des documents et des liens vers les données.



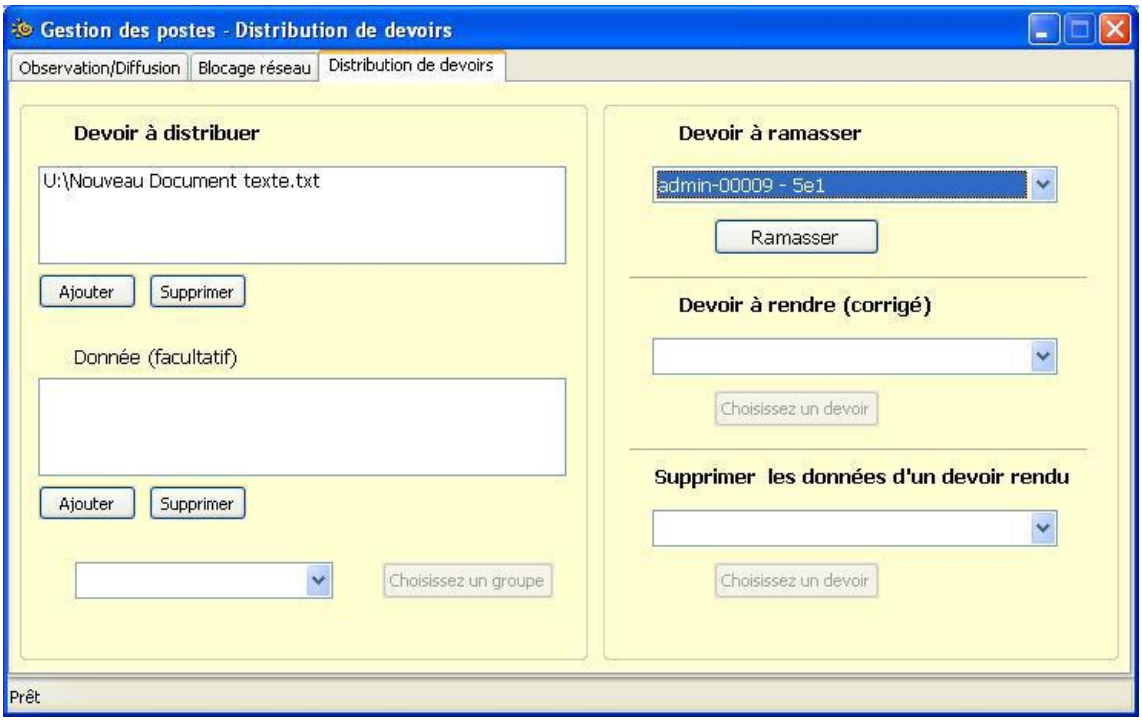
L'opération peut prendre du temps dans le cas de fichiers volumineux et de nombreux membres dans le groupe cible.

Veillez à ne pas fermer l'application pendant la distribution.

N'étant copiées qu'une fois puis liées dans les dossiers "devoirs", les données ont l'avantage d'économiser de l'espace disque sur le serveur.

Ramasser

Sélectionner le devoir à ramasser. Dans la liste déroulante, le nom du groupe auquel a été distribué le devoir est affiché à côté du nom du devoir.

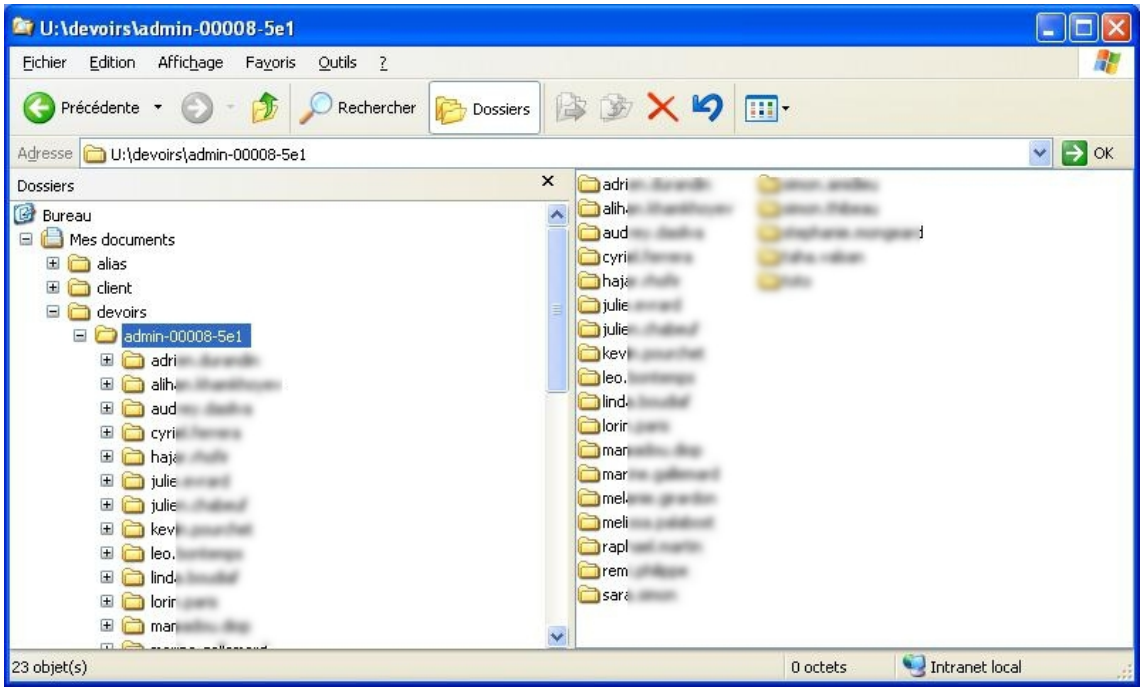


À la fin du ramassage, un message rend compte de l'opération. Si un élève a supprimé le dossier du devoir, celui-ci ne pourra pas être ramassé, un répertoire du nom de l'élève sera quand même créé mais sera vide.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'action ramassage des devoirs effectue une copie des fichiers du devoir (sans les données) dans le répertoire "devoirs" du dossier personnel de celui qui exécute le ramassage et prend la forme `U:\devoirs\<nom_devoir>-<groupe_cible>\<identifiant_de_l'élève>\`



> Lors du ramassage d'un devoir, tous les fichiers et dossiers contenus dans `U:\devoirs\<nom_devoir>\` (sauf le répertoire `donnees`) sont recopiés. Il est donc possible de donner comme devoir la création d'un nouveau fichier.

Rendre les copies corrigées

Tout comme sur une version papier, la correction peut s'effectuer sur la copie en éditant directement le fichier mais elle peut aussi bien se faire sous forme d'ajout de fichier. En effet, c'est tout le dossier qui sera copié dans le répertoire personnel de l'élève lors de la restitution de la correction. La restitution se fait dans le répertoire personnel des utilisateurs à savoir `U:\devoirs\<nom_devoir>\correction\`

Une boîte de dialogue informe du résultat de l'opération.

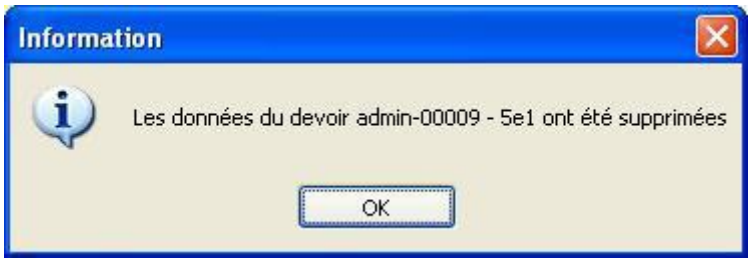


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Suppression des données

Lorsqu'un enseignant distribue des données en plus des documents, elles sont copiées dans `U:\devoirs\.distribues` et des liens vers ces fichiers sont ensuite créés dans le répertoire `nom_du_devoir` \ `donnes` de chacun des destinataires.

Il est possible de supprimer ces fichiers lorsqu'ils sont devenus inutiles.



- La suppression des données entraînera également la suppression du dossier `<nom_du_devoir>` \ `donnees` dans le dossier des destinataires.
- Cette fonctionnalité permet de supprimer les données liées à une distribution de document qui ne seraient plus utiles par la suite. Elle permet donc d'économiser de la place sur le serveur de stockage.

4.2.5. Administration avancée des clients Scribe

4.2.5.a. Contrôle à distance d'un poste

Exécution de commandes à distance sur le poste

Il est possible de dialoguer avec le service Scribe installé sur les postes clients avec l'utilitaire `cliscribe.py` :

La syntaxe de la commande est :

```
#   /usr/share/eole/controlevnc/cliscribe.py   <IP_POSTE_CLIENT>   <OPTION>
<ARGUMENTS>
```

L'option `-h` permet d'avoir de l'aide sur la commande :

```
# /usr/share/eole/controlevnc/cliscribe.py -h
```

La liste des options est :

- -k ou --killproc <NOM_DU_PROGRAMME>
  termine un programme en cours d'exécution, "explorer.exe" par exemple
- -s ou --shutdown <NIVEAU>
  permet d'éteindre le poste : 0 = éteindre (défaut), 1 = reboot, 2 = fermeture de session
- -e ou --execute <NOM_DU_PROGRAMME>

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

exécute un programme dans l'environnement du service (BUILTIN\SYSTEM)

- -eu ou --executeuser <NOM_DU_PROGRAMME>

  exécute un programme dans l'environnement de l'utilisateur connecté s'il y en a un, sinon renvoie une erreur

  (un utilisateur doit avoir une session ouverte)

- -vc ou --vncconnect <IP_VIEWER_LISTEN>

  exécute la commande `winvnc -connect <IP_VIEWER_LISTEN>` (vncviewer doit être en mode "listen" sur le poste <IP_VIEWER_LISTEN>)

- -va <ÉTAT> ou --vncactive <ÉTAT>

  permet de démarrer ou d'arrêter winvnc sur le client :

  0 = arrête winvnc sur IP_CLIENT, 1 = démarre winvnc sur IP_CLIENT

- -vi <ÉTAT> ou --vncinputs <ÉTAT>

  permet d'activer, désactiver le clavier et la souris pour winvnc sur le client :

  0 = désactive le clavier/souris pour winvnc, 1 = active le clavier/souris pour winvnc

- -f <FW_ACTION> ou --firewall <FW_ACTION>

  permet de gérer le pare-feu sur le client : activation, désactivation, initialisation, ajout de règles, suppression de règles, modification de la politique par défaut

  <FW_ACTION> doit ressembler à `INIT|ADD::rule|DEL::Nom|SETMODE::<in>;;<out>|ACTIVATE::True|False` :

  - INIT initialise les règles de bases (fait une simple initialisation, ne lit pas le fichier `liste_fwregles.eol`)
  - ADD::rule

    Exemple : ADD::'Nom;; ip_src=XX;;ip_dst=XX;;action=XX;;proto=XX;;port_dst=XX;;program=XX'

    - ip_src/dst = me|any|<ip>
    - action=allow|block
    - proto=tcp|udp|icmp|any
  - DEL::Nom
  - SETMODE::<in>;;<out>
  - ACTIVATE::True|False

Terminer un programme en cours d'exécution

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --killproc firefox.exe
```

Exécuter un programme dans l'environnement du service

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --execute '\\scribe\wpkg\wpkg_client_install.bat'
```

(noter les simple quotes ou apostrophes autour de la commande à exécuter)

Initialiser les règles de bases du pare-feu

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
INIT
```

Bloquer l'accès au port TCP 123 par la machine 1.2.3.4 vers la machine 172.16.0.45

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'ADD::maregle;;ip_src=1.2.3.4;;ip_dst=me;;action=block;;proto=tcp;;p
```

Bloquer l'accès au réseau/à Internet pour firefox.exe

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'ADD::maregle;;ip_src=me;;ip_dst=any;;action=block;;proto=any;;progr
Files\Mozilla Firefox\firefox.exe"'
```

Ne fonctionne que sur Vista et supérieur.

Supprimer toutes les règles de pare-feu nommées maregle

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --firewall
'DELL::maregle'
```

Affichage à distance d'un poste client

Il existe 2 méthodes pour prendre la main sur un poste :

- VNC ;
- Le *Bureau à distance Windows*.

VNC

Après s'être connecté en SSH (ssh -X ou putty+Xming) les commandes suivantes permettent l'affichage du poste :

Installer xtightvncviewer

```
# apt-get install xtightvncviewer
```

```
# nohup vncviewer -listen 0 &
```

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --vncinputs
<IP_SCRIBE>
```

Cette méthode ne fonctionne que si un utilisateur est connecté sur le poste.

Bureau à distance

Après s'être connecté en SSH (ssh -X ou putty+Xming) :

Installer rdesktop

```
# apt-eole install rdesktop
```

Activer le bureau à distance

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --execute 'REG ADD
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
"HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f'
```

Redémarrer la machine pour prendre en compte l'activation du bureau à distance

```
# /usr/share/eole/controlevnc/cliscribe.py 172.16.0.45 --shutdown 1 #
```

Attendre que la machine redémarre et exécuter rdesktop

```
# rdesktop 172.16.0.45
```

On peut spécifier une résolution

```
# rdesktop 172.16.0.45 -g 1400x900
```



Cette méthode ferme la session distante s'il y en a une d'ouverte.

4.2.5.b. Le Pare-feu du poste client

Paramétrage du pare-feu sur les postes clients

Il est nécessaire d'avoir un accès "root".

Le fichier `/home/client_scribe/liste_fwregles.eol` contient les règles de pare-feu appliquées à chaque démarrage du poste (à chaque démarrage du service Scribe sur le poste pour être précis).

Ajout d'une règle

Une règle possède la structure suivante :

```
OS : :"NOM_REGLE" ; ;proto="PROTOCOLE" ; ;program="PROGRAMME" ; ;ip src=IP_SOURCE ; ;ip dst=IP_DISTANTE ; ;port dst=PORT_DISTANT ; ;action
```

- OS : WinXP, Vista (séparer par "|" pour plusieurs OS)
- NOM_REGLE : seulement des caractères alphanumériques, sans accents et sans espaces
- PROTOCOLE : any, tcp, udp, icmp
- PROGRAMME : chemin local ou réseau d'un programme
- IP_SOURCE : adresse IP source
- IP_DISTANTE : adresse IP distante
- PORT_DISTANT : port distant
- ACTION : allow, block

Par exemple :

On a un serveur AutoCad avec l'IP 172.16.0.21, on veut y autoriser l'accès en cas de blocage réseau par `Gestion-postes` :

```
WinXP|Vista:: "AcadServeur" ;; proto = "any" ;; ip_src = "any" ;; ip_dst = 172.16.0.21 ;; action = "allow"
```



Il est indispensable de générer une nouvelle *somme md5* à chaque modification de `/home/client_scribe/liste_fwregles.eol` pour que le service Scribe puisse en valider l'intégrité lors de son téléchargement.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
md5sum /home/client_scribe/liste_fwregles.eol > /home/client_scribe/liste_fwregles.eol.MD5SUM
```



/home/client_scribe/liste_fwregles.eol est un template Creole, cela signifie qu'il est écrasé à chaque reconfigure/mise à jour.

Pour pérenniser les modifications réalisées dans /home/client_scribe/liste_fwregles.eol :

```
cp /home/client_scribe/liste_fwregles.eol /usr/share/eole/creole/modif
gen_patch
reconfigure
```

4.2.5.c. Wake on Lan

Le standard Wake on Lan[p.904] permet le réveil d'une machine à distance et présente des intérêts variés.

Par exemple, on peut vouloir démarrer les stations la nuit pour exécuter WPKG[p.905] et ainsi appliquer les installations et mises à jour sans perturber les utilisateurs.

La nouvelle version du logiciel ecoStations intègre la fonctionnalité Wake on Lan pour les postes clients gérés par le serveur Scribe.

Installation du paquet wakeonlan

Le paquet wakeonlan fournit l'application permettant de réveiller les stations à distance.

Pour l'installer :

```
# apt-eole install wakeonlan
```

Récupération des adresses MAC

Il est nécessaire de disposer des adresses MAC[p.882] des stations à réveiller.

Les adresses MAC des stations sur lesquelles le client Scribe est installé sont disponibles peuvent être listées en utilisant le script manage_stations.py :

```
# /usr/share/eole/controlevnc/manage_stations.py --list-all
seven64-1;192.168.230.131;08:00:27:85:0C:95;pcwin7,10.1.2.51,02:00:0A:01:02
```

Le caractère ; délimite les stations et le caractère , permet de séparer les informations associées à chacune des stations.

Paramétrage des stations

Il est nécessaire de paramétrer le Wake on Lan dans le BIOS[p.885] des stations à réveiller.

Cela se fait en général dans le menu du BIOS : Alimentation/Power, Wake On Lan/Remote Wake Up=> Enabled.

Démarrage d'une station à distance

Une fois le BIOS paramétré et la station éteinte, exécutez la commande suivante sur le serveur :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# wakeonlan 08:00:27:85:0C:95
```

Démarrage de toutes les stations à distance

Pour demander le démarrage de toutes les stations, il faut exécuter la commande wakeonlan pour chacune des adresses MAC des stations listées :

```
1 /usr/share/eole/controlevnc/manage_stations.py --list-all | sed 's/;/\n/g' |  while
  read i;
2 do
3     mac=$(echo $i|cut -d ',' -f 3);
4     wakeonlan $mac;
5 done
```

Voir aussi...

> ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés [p.514]

4.2.5.d. Gestion des ACLs

Cette partie décrit le fonctionnement entre les ACLs Linux/Samba et les droits sous Windows.

Préambule

Par défaut Linux/Unix connaît trois type de permissions :

- R : Lire (Read)
- W : Écrire (Write)
- X : Exécuter (eXecute)

Le droit d'exécution pour un dossier permet de rentrer dedans.

Le droit de lecture pour un dossier permet de lister son contenu.

Par défaut Linux/Unix considère trois type d'utilisateurs :

- U : utilisateur (user)
- G : groupe (group)
- O : propriétaire (owner)

Les ACLs permettent de compléter ces permissions et de paramétrer des droits particulier pour un utilisateur ou un groupe.

Sur un module EOLE, les ACLs ne sont supportées que sur la partition `/home`.

Attention sur un dossier qui possède des ACLs, les droits Unix sont mal affichés par la commandes `ls -l` ou par l'alias `ll`, il faut utiliser la commande `getfacl` pour les afficher correctement et `setfacl` pour les modifier.

Seules les ACLs par défaut sont hérités, les droits Unix positionnés à `777` sur un dossier n'est pas hérité par les fichiers et dossiers qui seront créés dedans.

Exemple d'un mauvais affichage des droits Unix

```
root@scribe:~# ls -ld /home/workgroups/commun/
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `drwxr-x---+ 5 root root 4096 févr. 12 11:35 /home/workgroups/commun/`
>
> D'après cette commande, les droit Unix sont `750`, le signe `+` indique qu'il y a des ACLs.

Affichage des droits avec la commande getfacl

La commande `getfacl` liste les droits Unix, les ACLs et les ACLs par défaut :

`root@scribe:~# getfacl /home/workgroups/commun/`

`getfacl : suppression du premier / des noms de chemins absolus`

`# file: home/workgroups/commun/`

`# owner: root`

`# group: root`

`user::rwx` ← droit Unix 7

`group::---` ← droit Unix 0 (juste avant la commande `ls -ld` affichait un `5` pour le groupe)

`group:administratifs:r-x` ← ACL

`group:professeurs:r-x` ← ACL

`group:eleves:r-x` ← ACL

`mask::r-x`

`other::---` ← droit Unix 0

`default:user::rwx`

`default:group::---`

`default:group:administratifs:r-x` ← ACL par défaut

`default:group:professeurs:r-x` ← ACL par défaut

`default:group:eleves:r-x` ← ACL par défaut

`default:mask::r-x`

`default:other::---`

On voit que pour le groupe la commande `ls -ld` n'affiche pas les bons droits : `5` au lieu de `0`.

Modifier des droits

Si on veut modifier des droits :

`root@scribe:~# mkdir /home/workgroups/commun/toto`

`root@scribe:~# setfacl -Rm g:eleves:rwx /home/workgroups/commun/toto`

Option de la commande setfacl :

- `-R` pour être récursif
- `-m` pour modifier
- `g:` : indique qu'il s'agit d'un groupe, suivi du nom du groupe ou rien pour le groupe propriétaire
- `:rwx` : lui donne les droits Read Write eXecute

`root@scribe:~# getfacl /home/workgroups/commun/toto/|grep eleves`

`group:eleves:rwx`

`default:group:eleves:r-x`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La même commande mais pour les ACLs par défaut (celles qui seront héritées par le contenu) :

```
root@scribe:~# setfacl -Rdm g:eleves:rwx /home/workgroups/commun/toto
```

- `-d` pour indiquer que l'on modifie les ACLs par défaut

```
root@scribe:~# getfacl /home/workgroups/commun/toto/|grep eleves
group:eleves:rwx
default:group:eleves:rwx
```



Seuls les dossiers possèdent des ACLs par défaut, pour l'héritage. Les fichiers n'en ont donc pas.



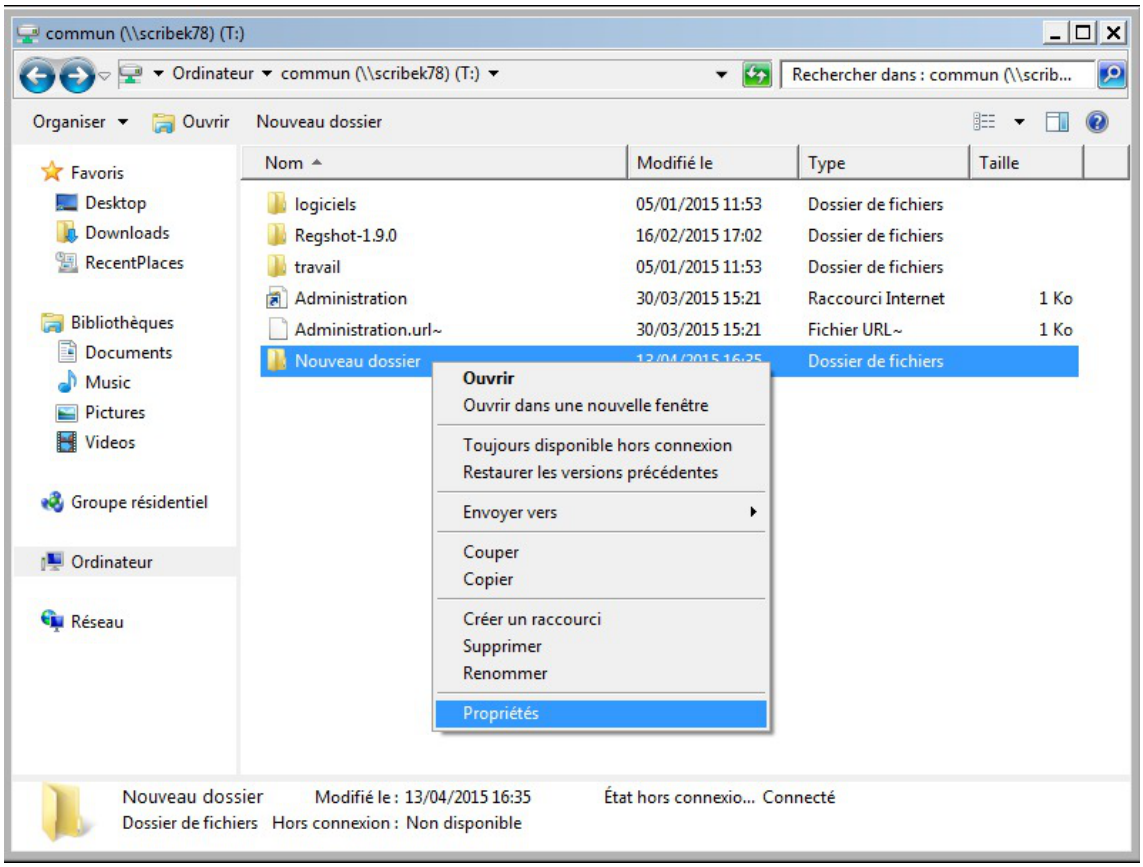
Pour plus d'information il faut se reporter à la page de manuel de la commande :

```
# man getfacl
```

ou

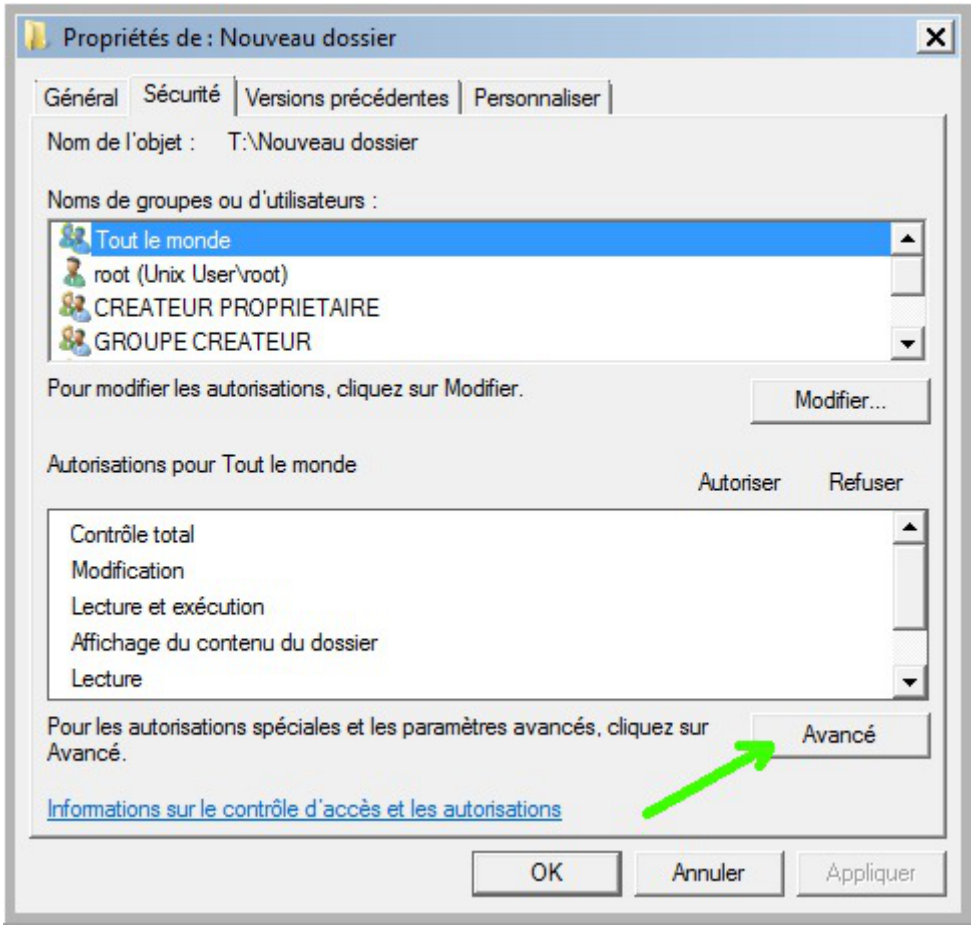
```
# man setfacl
```

Le plus simple est de gérer les ACLs depuis Windows, pour cela faire un clic droit sur un fichier ou sur un dossier et cliquer sur l'action `Propriétés`.

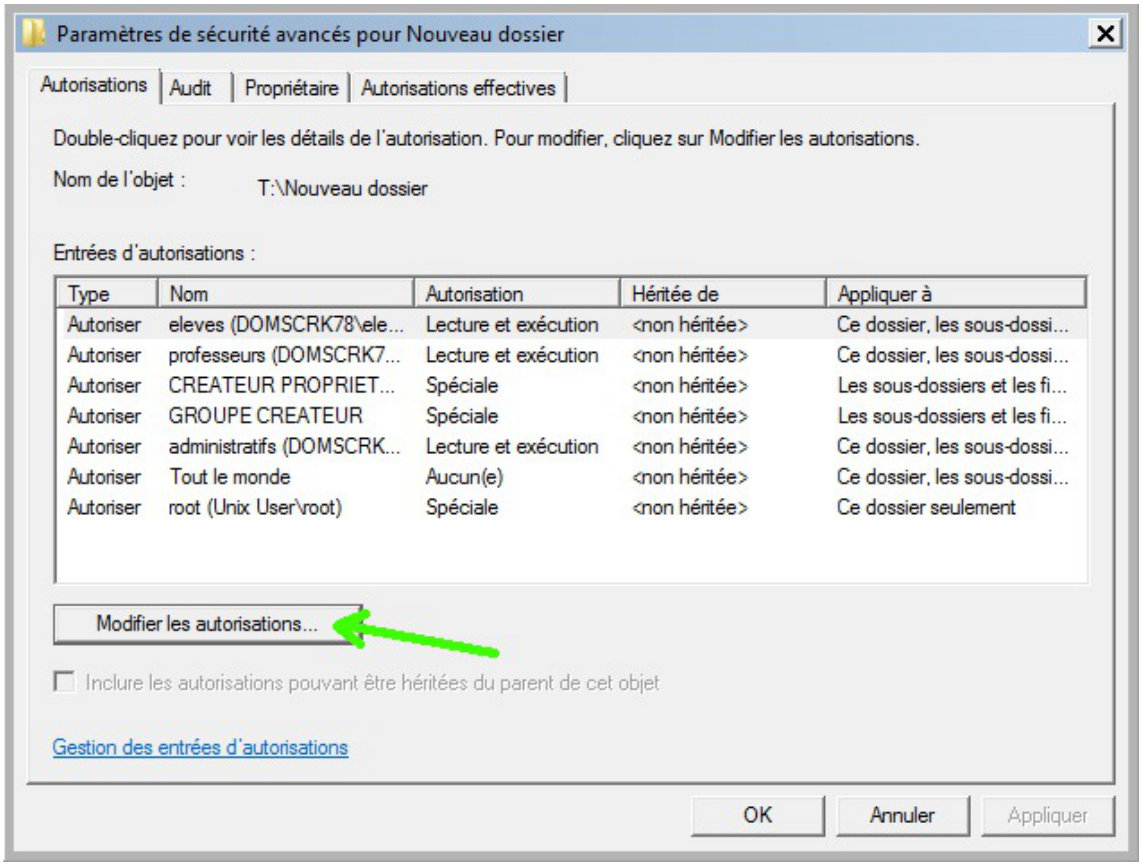


On obtient la fenêtre de propriétés du fichier ou du dossier sélectionné, pour modifier les autorisations il faut se rendre dans l'onglet `Sécurité`, choisir le nom de groupes ou d'utilisateurs, puis cliquer sur le bouton `Avancé`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

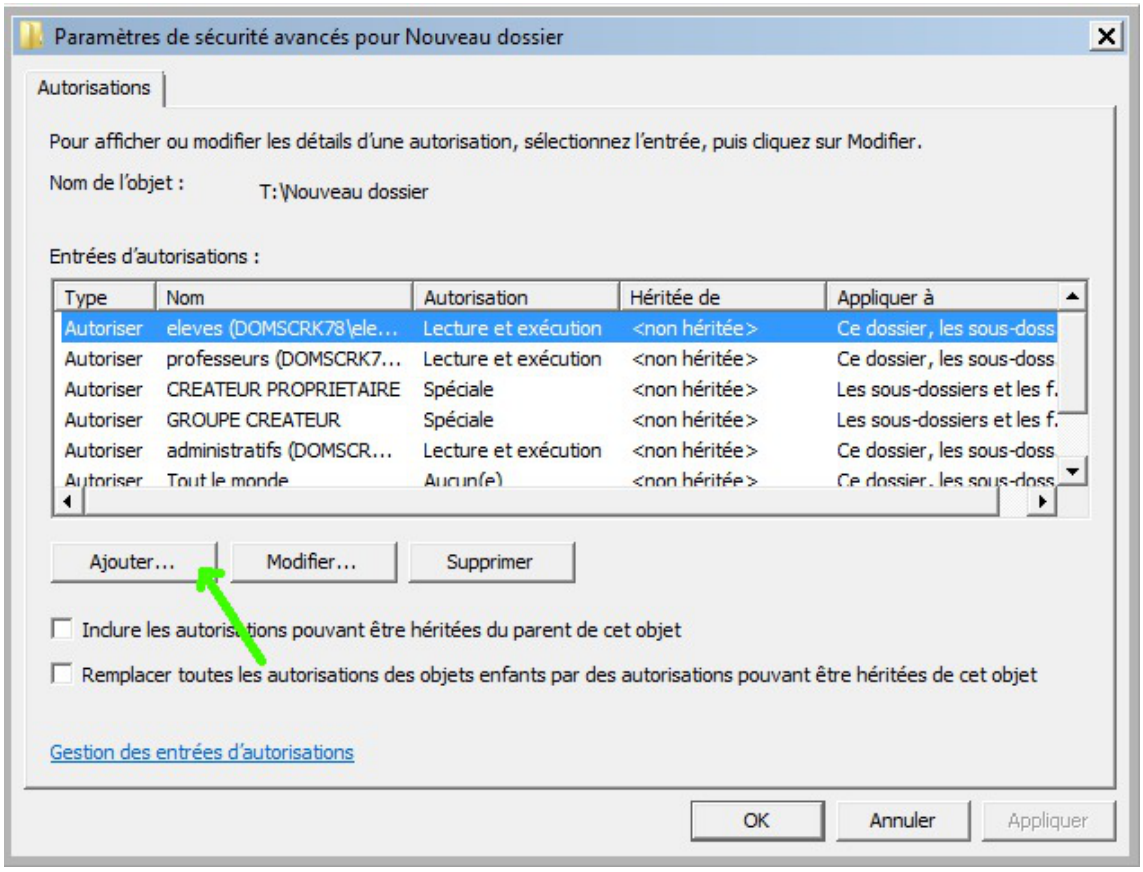


Dans l'onglet Autorisations, cliquer sur l'entrée désirée puis cliquer sur le bouton Modifier les autorisations… .

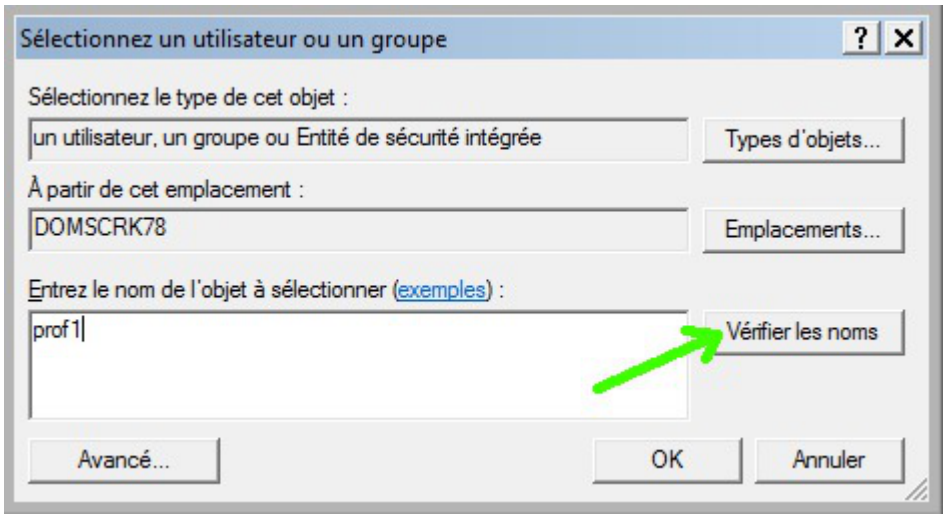


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Parmi les modifications des autorisations il est possible d'ajouter, de modifier ou de supprimer. Cliquer sur le bouton Ajouter….

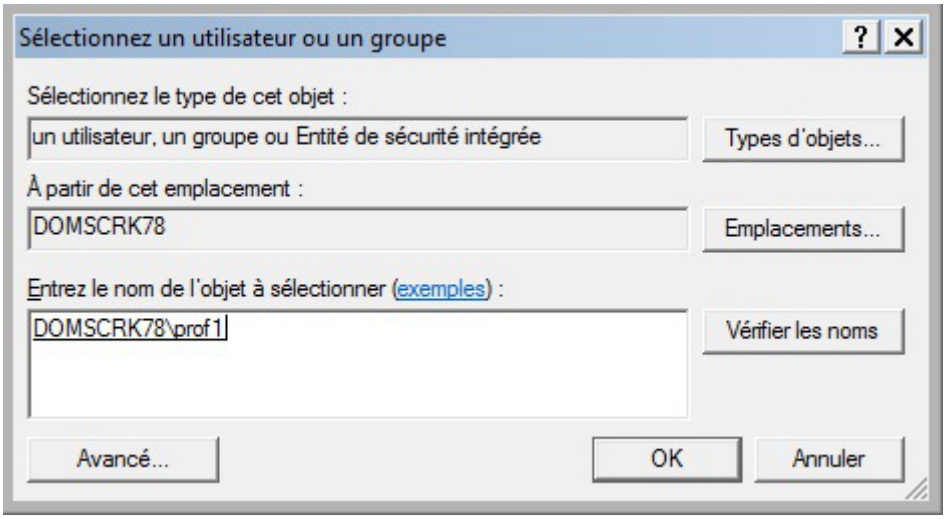


Entrer un nom d'utilisateur ou le nom d'un groupe et cliquer sur le bouton Vérifier les noms.



Valider avec le bouton OK.

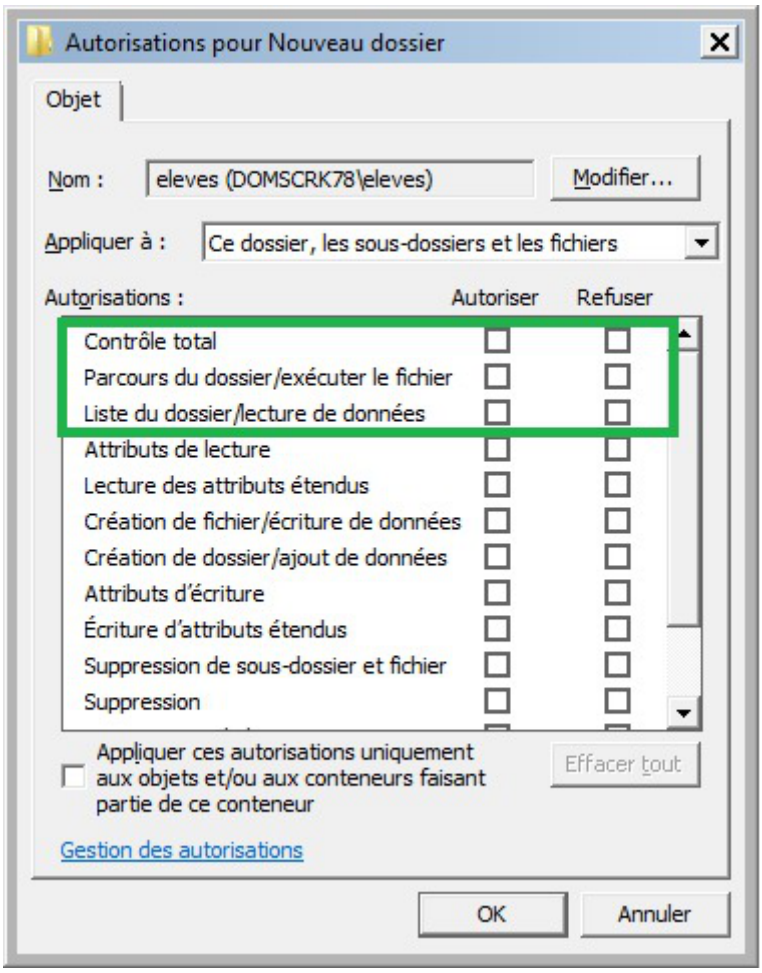
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Cocher les autorisations désirées et valider avec le bouton OK.

Il faut par contre garder à l'esprit que côté serveur on n'a que 3 droits : **R**ead **W**rite et e**X**ecute.

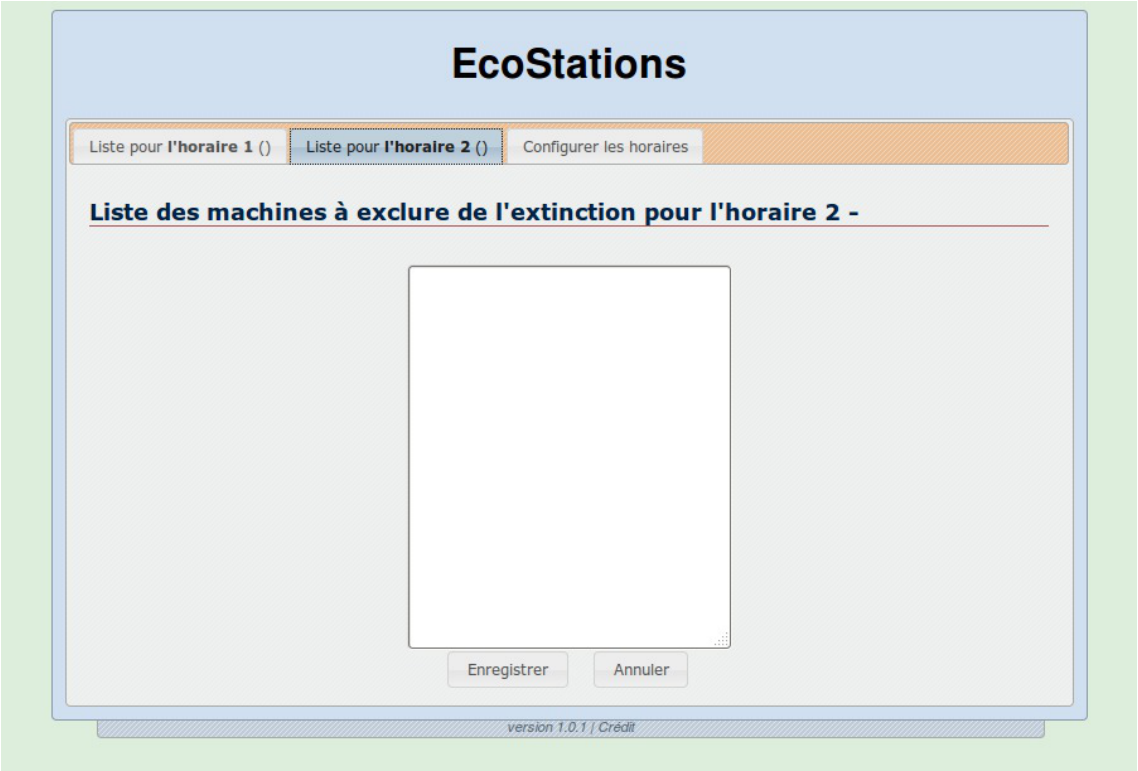
Seules les 3 premières cases à cocher proposées avec cette méthode sont supportées par le serveur Scribe. Les autres ne fonctionnent pas. Les droits sur les autres lignes vont se placer automatiquement.



4.2.6. ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



ecoStations est un outil qui permet d'éteindre le parc informatique d'un établissement suivant une procédure assez souple pour permettre d'intégrer la notion d'internat par exemple ou de station à laisser allumée constamment.

Il faut renseigner via une interface web, deux listes de stations du parc L1 et L2 ainsi que deux horaires distincts H1 et H2.

À l'heure H1, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L1 ; puis à l'heure H2, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L2.

Ainsi, les stations listées dans L1 et L2 ne seront pas éteintes.

ecoStations a été développé en étroite collaboration entre Olivier Hacquard, Pascal Ratte, Laurent Etignard, Frédéric Lamy, Valéry Georges et Jérôme Labriet.

La documentation d'utilisation (disponible dans l'espace contribution) a été rédigée par Pierre Mariot.

http://dev-eole.ac-dijon.fr/projects/ecostations/

Montée de version de l'application ecoStations

L'application ecoStations qui permet de gérer l'extinction et l'allumage des postes à des horaires donnés passe en version 2.4.8.

L'ajout d'un script permet notamment d'annuler le re-démarrage d'une station.

Installation d'ecoStations

ecoStations s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-ecostations
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'application n'est pas disponible immédiatement après l'installation.
L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



L'application fonctionne uniquement sur le module Scribe.



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
```

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/ecostations`
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

Utilisation

Les postes clients doivent avoir été pré-configurés avec `power_config.cmd` afin de supprimer la mise en veille automatique qui bloque l'ordre d'extinction.

Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante :
http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

4.2.7. Gestion 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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.2.7.a. Visualisation des quotas disque dans l'EAD

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.



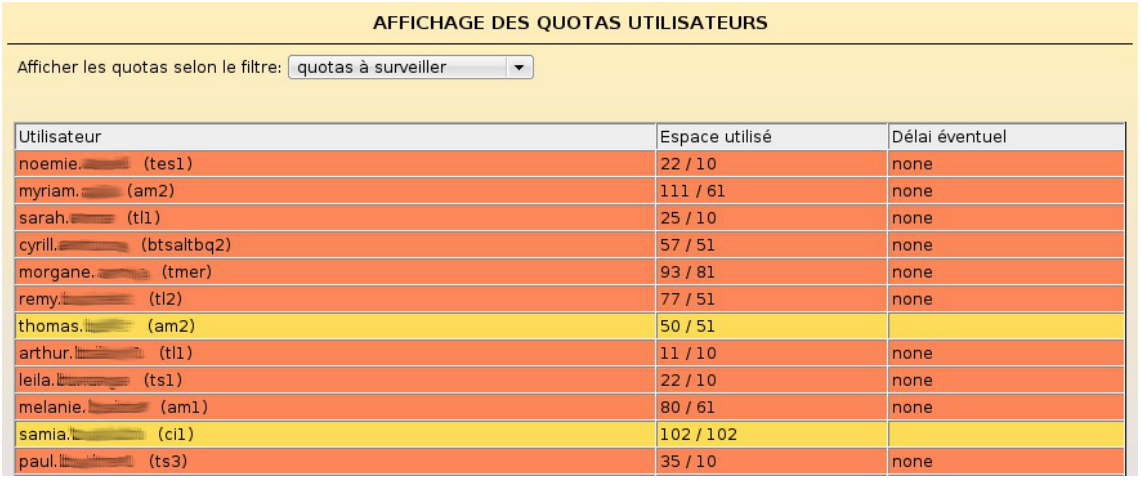
Cette procédure est également à appliquer dans le cas où la commande `repquota -a` ne rend plus la main.

Les quotas sur le module Scribe

Pour consulter les quotas, le menu `Outils/Quotas disque` de l'EAD permet d'afficher les quotas utilisateurs selon 3 filtres :

- Quotas dépassés
- Quotas à surveiller (quotas presque atteint)
- Tous les quotas

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



AFFICHAGE DES QUOTAS UTILISATEURS

Afficher les quotas selon le filtre: quotas à surveiller

Utilisateur	Espace utilisé	Délai éventuel
noemie. (tes1)	22 / 10	none
myriam. (am2)	111 / 61	none
sarah. (tl1)	25 / 10	none
cyrill. (btsaltbq2)	57 / 51	none
morgane. (tmer)	93 / 81	none
remy. (tl2)	77 / 51	none
thomas. (am2)	50 / 51	
arthur. (tl1)	11 / 10	none
leila. (ts1)	22 / 10	none
melanie. (am1)	80 / 61	none
samia. (ci1)	102 / 102	
paul. (ts3)	35 / 10	none

Affichage des quotas utilisateur dans l'EAD

Les quotas sont appliqués sur la partition `/home`. Les quotas concernent, ainsi, l'ensemble des fichiers créés par l'utilisateur sur le serveur (dossiers personnels, partages équipe pédagogique, classe, groupes, etc.).

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.

4.2.7.b. Infosquota : gestion des quotas utilisateurs

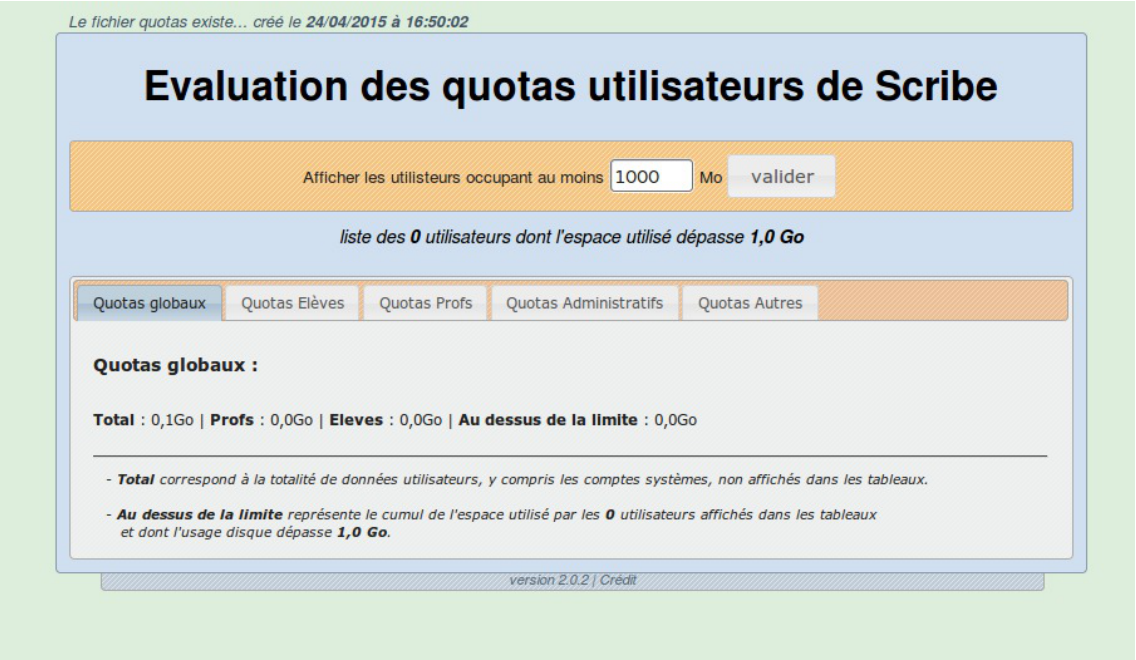
Présentation

Infosquota est un outil qui permet de mettre en place les quotas de manière très souple et très pédagogique. Chaque utilisateur apprend à gérer son quota en suivant une information claire sur son évolution.

Grâce à son outil de visualisation, Infosquota permet de retrouver les fichiers que les utilisateurs ont ventilé hors de leur lecteur partagé personnel. En effet les fichiers dispersés dans d'autres volumes sont

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

comptabilisés dans le quota de l'utilisateur.



Infosquota a été développé par Olivier Hacquard et Jérôme Labriet (Académie de Besançon) en étroite collaboration avec Bruno Debeve (Académie de Bordeaux), Frédéric Poyet (Académie de Dijon) et Pierre Mariot (Académie de Besançon) dans le cadre du projet EOLE.

http://dev-eole.ac-dijon.fr/projects/infquot

Les derniers développements mis à disposition par Bruno Debeve ont également été intégrés.

http://www.debeve.net/infosquota_dev/

Installation d'Infosquota

Infosquota s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
# apt-eole install eole-infosquota
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

L'application fonctionne uniquement sur le module Scribe.

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/`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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`

L'initialisation de l'application (recherche des fichiers) s'effectue lors de l'instance ou du reconfigure suivant l'installation du paquet.

La mise à jour des fichiers s'effectue de façon hebdomadaire.

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/quotas/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

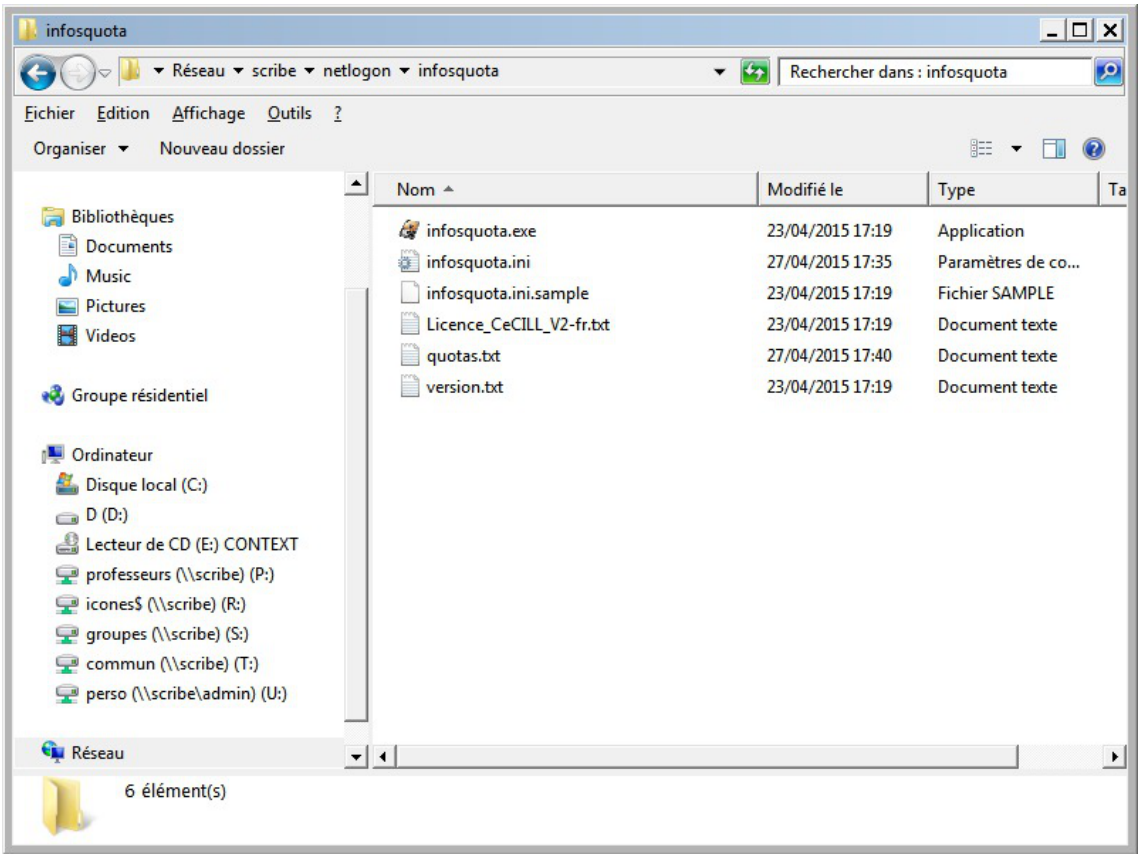
Rôles des utilisateurs

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

Utilisation

L'exécutable `infosquotas.exe` est lancé au démarrage de la session et affiche les messages qui conviennent selon la configuration des quotas établie dans l'EAD et celle des alertes saisies dans le fichier `\\scribe\netlogon\infosquota.ini`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante : http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

Remarques

L'utilisation du disque par utilisateur est enregistrée dans le fichier : `/home/netlogon/infosquota/quotas.txt`.

Le journal généré par le script de recherche des fichiers est disponible dans : `/var/log/infosquota/recherche-fich-users.log`.

La liste des fichiers ventilés d'un utilisateur est stockées dans le fichier : `/var/www/html/outils/quotas/log/<login>.log`.

4.2.7.c. Envoi de courrier électronique en cas de dépassement des quotas

Dans l'onglet `Samba` de l'interface de configuration du module en mode expert, il est possible d'activer l'envoi d'un courrier électronique à un utilisateur dans le cas où celui-ci dépasse le quota disque.

Il faut bien sûr que l'utilisateur ait une adresse de courrier électronique valide définie dans l'annuaire.

> 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Voir aussi...

> Onglet Samba : Configuration du contrôleur de domaine

4.3. Résolution des problèmes du client

4.3.1. Problèmes à l'inscription au domaine

Lorsqu'un problème survient pendant l'inscription au domaine ou à l'ouverture de session, plusieurs pistes sont à explorer.

Sur le serveur

Vérifier l'état du serveur avec la commande `diagnose`.

Vérifier la communication avec le client à l'aide de la commande `tcpcheck` :

```
# tcpcheck 2 <IP station>:139
```

> Sur le serveur les commandes doivent être exécutées avec l'utilisateur `root`, soit sur la console soit en SSH.

Sur un client Windows

Vérifier la configuration réseau de la station avec la commande `ipconfig /all`

Vérifier la communication du client avec le serveur avec les commandes :

```
ping <adresse module>
nbtstat -A <adresse module>
```

4.3.2. Problèmes avec le Client Scribe

Le client Scribe enregistre ses actions dans les fichiers :

- %WINDIR%\cliscribe.log
- %WINDIR%\cliscribe_logon.log
- %WINDIR%\cliscribe_updater.log
- %TMP%\cliscribe_utilisateur-<login>.log

Ces fichiers peuvent être utilisés pour vérifier l'exécution du client Scribe et détecter d'éventuelles erreurs. Le niveau de verbosité est renseigné dans la base de registre sous : `HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : "log_level".

Le niveau de verbosité peut être paramétré dans la console ESU `Domaine => Groupe de machine => "Client Scribe" => "Activer le mode debug du client"`.

Ce sont les valeurs du module *logging* de *Python* qui sont utilisées :

- CRITICAL
- ERROR
- WARNING

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- INFO
- DEBUG

Lorsque le niveau de journalisation (`HKEY_LOCAL_MACHINE\Software\Eole\Scribe` : "`log_level`") est placé sur "**debug**" la fenêtre de mise à jour reste ouverte 40 secondes en cas d'avertissement ("warning") ou d'erreur ("error").

Les "traceback"

Le client Scribe ainsi que l'application *Gestion-postes* peuvent générer des erreurs en cas de problème.

Ces erreurs peuvent contenir le mot "**traceback**". Il s'agit de la pile d'appel (dernières instructions du programme) ayant conduit à cette erreur. Cela permet de retrouver plus rapidement la cause du problème.

Si vous rencontrez une telle erreur et que vous ne savez pas l'interpréter, pensez à joindre le contenu du traceback à votre demande (copie d'écran d'un popup ou fichier de log).

Le fichier de logon

Lors de l'ouverture de session, le client Scribe lit le fichier de logon de l'utilisateur.

Ce fichier se trouve sur le serveur dans le partage `\\scribe\netlogon`.

Le nom du fichier se compose du login et du système d'exploitation avec lequel l'utilisateur se connecte, par exemple : `adminWinXP.txt`.

En cas de problème de génération du fichier de logon il peut être utile de tester sa création manuellement, pour ce faire il faut exécuter la commande suivante :

```
/usr/share/eole/fichier/dyn-logon.py -u <login> -o <type_os> -m <nom machine win> -i <ip machine win>
```

où :

- <login> est login dont le fichier logon pose problème
- <type_os> : Win2K, WinXP, Vista, Win2K3
- <nom_machine_win> : le nom de la machine Windows
- <ip_machine_win> : l'IP de la machine Windows

Les erreurs sur le client

Lorsque le client affiche une erreur elle ne s'est pas forcément produite sur le client.

En effet, lorsque le client se connecte au serveur, le résultat de l'ensemble des actions exécutées sur le serveur est renvoyé au client, y compris les erreurs.

Un "traceback" peut donc contenir une pile d'appel d'un programme se trouvant sur le serveur.

Les fichiers de journalisation (log) du serveur contiendront alors une copie de l'erreur.

Pour tester la communication du serveur avec le client, faire sur le serveur :

```
tcpcheck 2 <ip_station>:8788
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

4.3.3. Problèmes Controle-vnc

C'est le service sur le serveur Scribe qui communique avec le *service client Scribe* installé sur les clients Windows. Il applique la configuration ESU et gère entre autre le blocage et la distribution de devoirs.

Son fichier de journalisation (log) est `/var/log/controle-vnc/main.log`. Pensez à l'examiner lorsque vous rencontrez des problèmes sur le client (traceback par exemple).

4.3.4. Problèmes de droits sur les répertoires partagés

Si des dysfonctionnements persistent et qu'ils semblent causés par des répertoires manquants dans les partages ou des problèmes de droits d'accès, il est possible de réinitialiser les droits à l'aide des utilitaires `droits_user.py` et `droits_partage.sh`.

droits_user.py

La commande `/usr/share/eole/backend/droits_user.py` vérifie la présence des répertoires personnels des utilisateurs (y compris le sous-dossier `prive` des élèves) et leur ré-applique les droits par défaut.

> Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un utilisateur donné en précisant son login en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py toto`

droits_partage.sh

La commande `/usr/share/eole/backend/droits_partage.sh` vérifie la présence des répertoires partagés (y compris les sous-dossiers `donnees` et `travail` pour les classes et les groupes) et leur ré-applique les droits par défaut.

> Dans sa dernière version (Scribe>=2.5.1), il est possible d'exécuter ce script pour un groupe donné en précisant son nom en tant que paramètre du script : `/usr/share/eole/backend/droits_user.py 3eme1`

4.4. 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- **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.

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`.

4.4.1. 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.

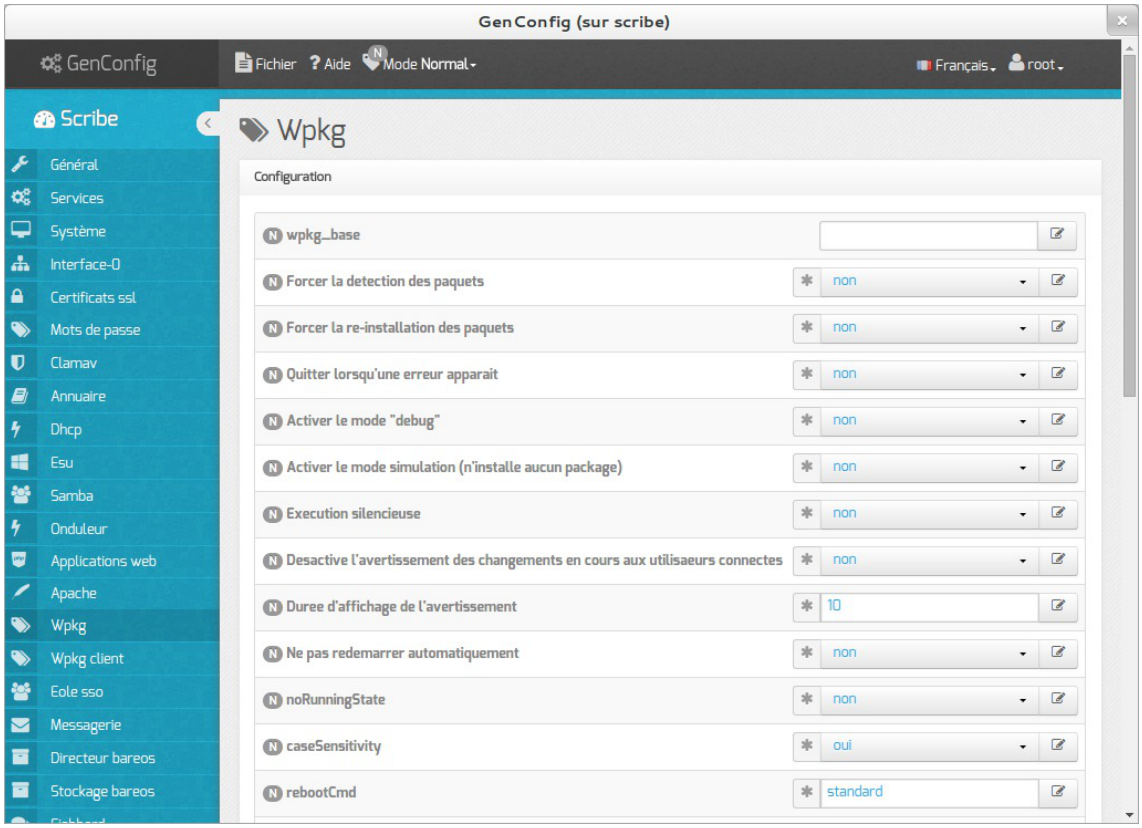
Configuration

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'outil de gestion de la configuration est l'interface de configuration du module.

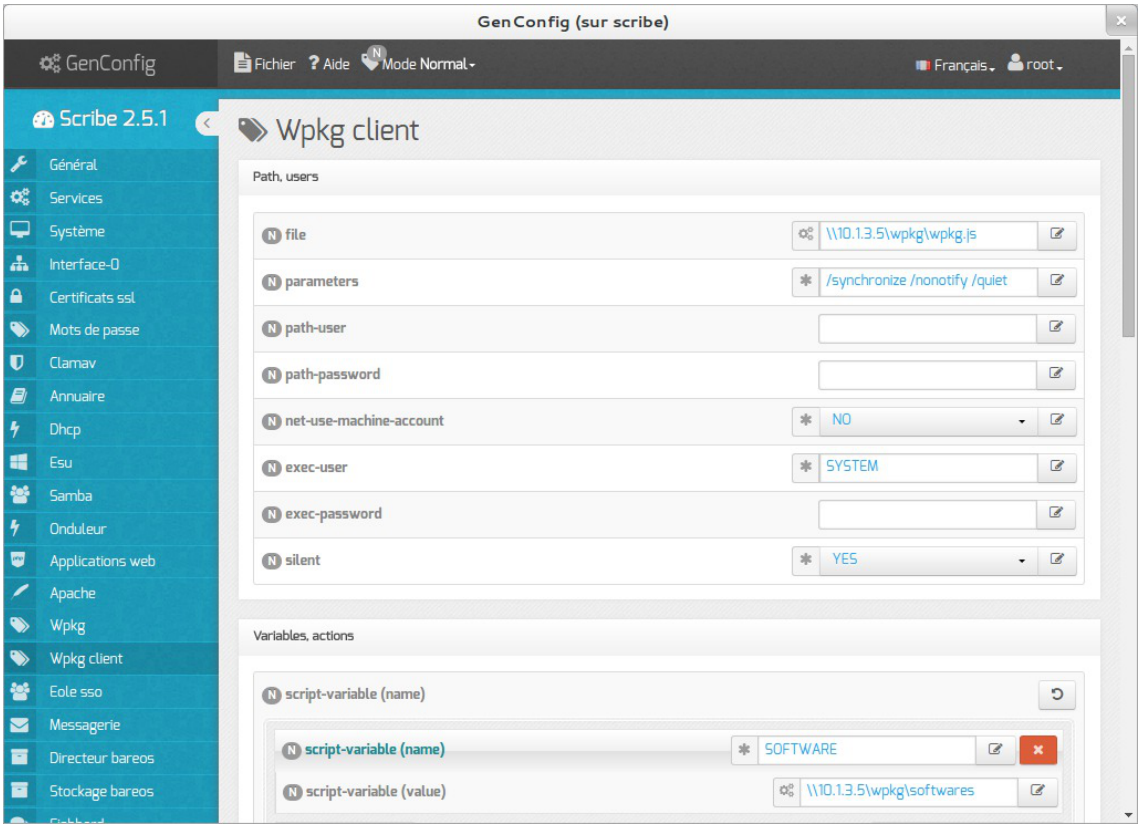
Dans l'interface de configuration du module, dans l'onglet `Services`, le service `Gérer la configuration WPKG` est à `oui` par défaut et 2 onglets concernant WPKG sont visibles :

- Wpkg : les options paramétrables du fichier `config.xml` (options de wpkg.js)



- Wpkg client : les options paramétrables des fichiers `settings.xml` (WPKG Client) et `wpkg-gp.ini` (Wpkg-GP)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



#fixme compléter l'essentiel de la configuration

Il faut ensuite reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# 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`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `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 :

- 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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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
```

4.4.2. 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" />
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
<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 url="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversion%/7z%version%.msi/download" destname="7zip/7z%version%.msi" />
<download url="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversion%/7z%version%-x64.msi/download" 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"' />
</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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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>`.

```
<eoledl dl="http://launchpad.net/ocsinventory-windows-agent/2.0/2.0.3/+download/OCS-NG-Windows-Agent-Setup.exe" 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 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

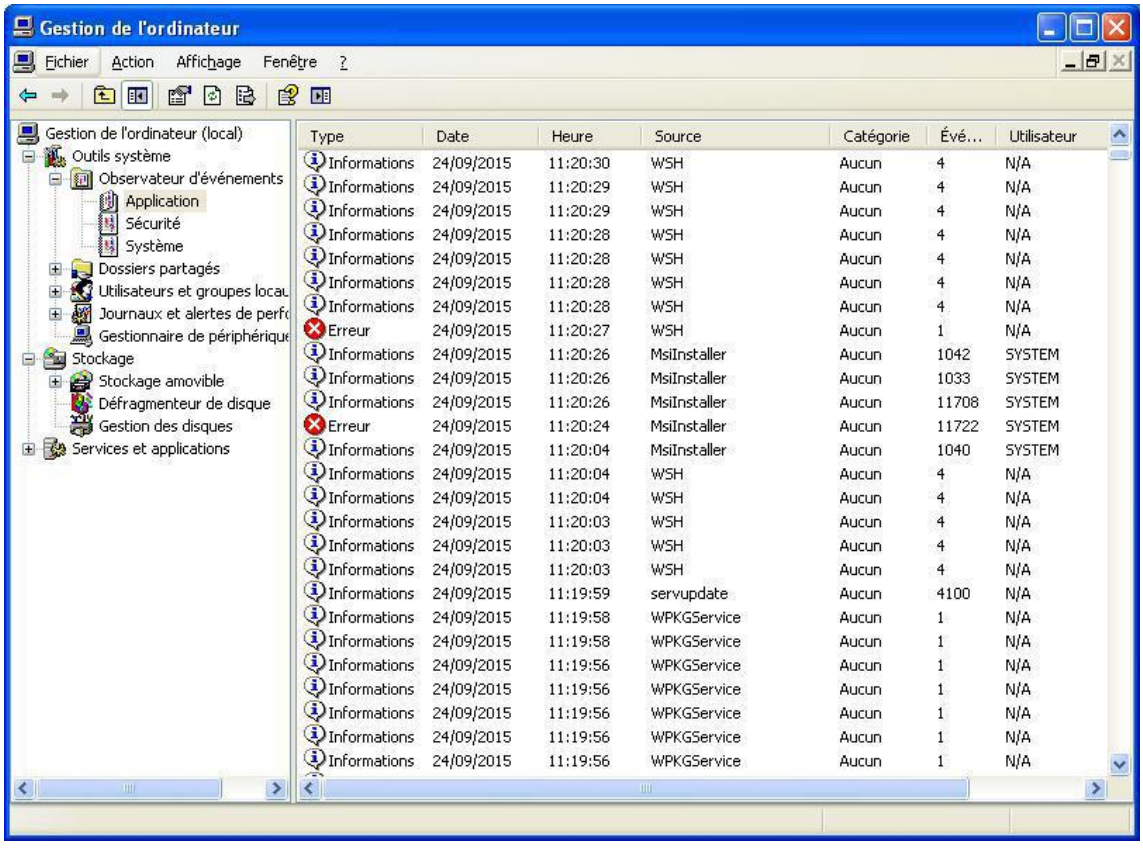
Il est toujours possible de faire une faute de frappe dans un fichier XML, un validateur XML en ligne permet de vérifier la syntaxe XML du fichier : http://xmlvalidation.com/.

Voir aussi...

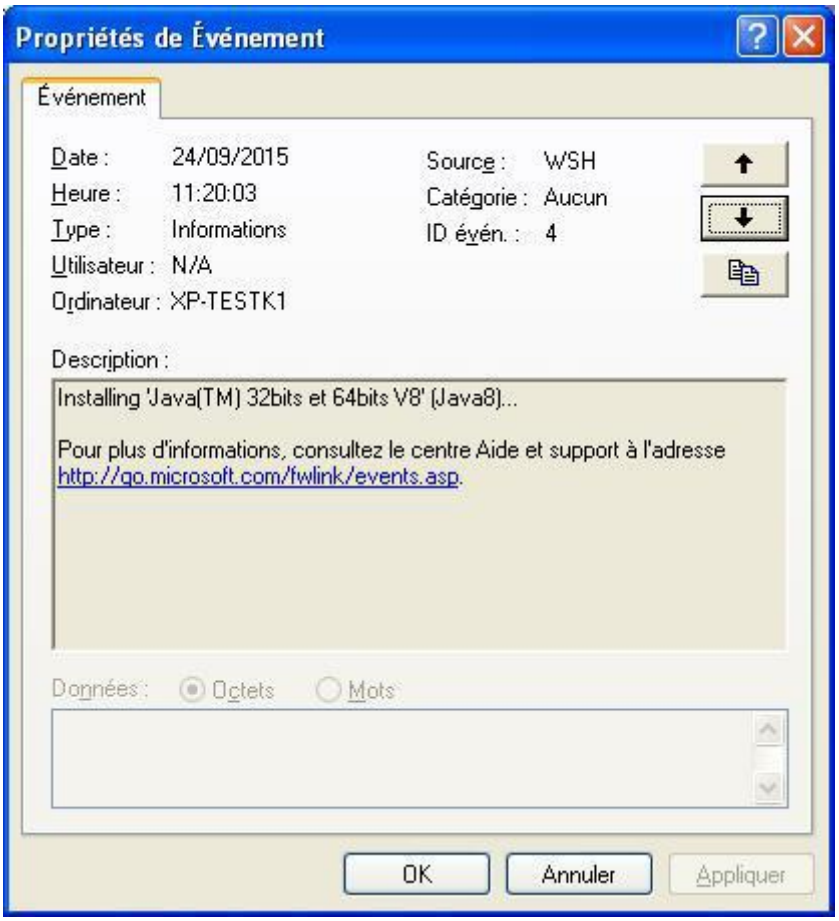
WPKG logiciels avec traitement particulier [p.540]

4.4.3. 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)

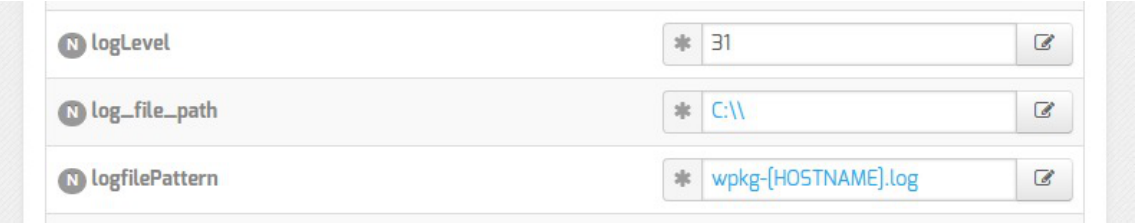
`/log_file_path:c: /logLevel:31`

- 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

4.4.4. 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.

Les chemins utilisateur sont dans HKEY_CURRENT_USER et les chemins machine dans

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

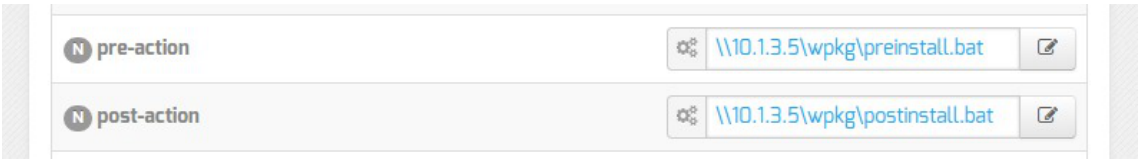
- appeler `preinstall.bat` et `postinstall.bat` depuis `<nom_du_package>.xml` dans les balises `<install>` et `<update>`

  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.

4.4.5. 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.

4.4.6. 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)

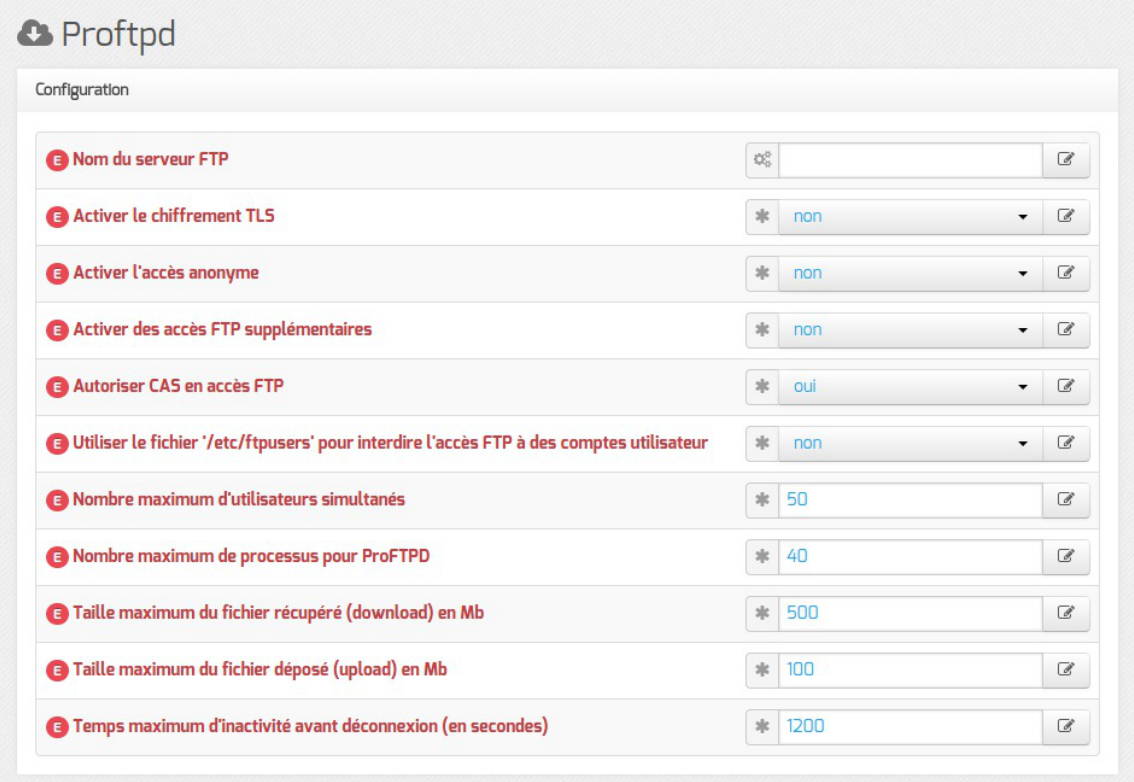
Mise à jour des clients Wpkg-GP (Seven et Windows 8) en version 0.17
http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:6.maj_wpkg_gp

5. 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

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.

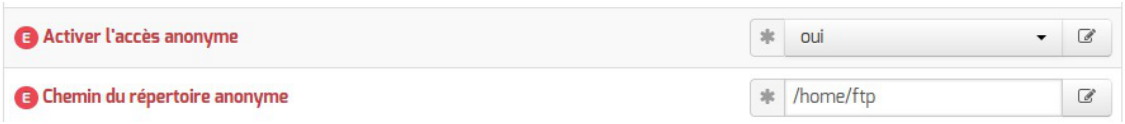
Activer le chiffrement TLS

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Activer l'accès anonyme

L'accès anonyme permet d'ouvrir l'accès en anonyme sur le répertoire de votre choix.



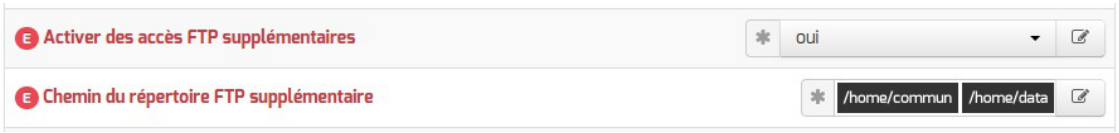
Si la variable est passée à `oui` une nouvelle variable `Chemin du répertoire anonyme` s'affiche, sa valeur est un chemin absolu. Ce répertoire doit être créé manuellement s'il n'existe pas. L'utilisateur `anonymous` peut télécharger depuis le répertoire spécifié, il n'a pas par défaut les droits d'écriture.

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.

Utiliser le fichier /etc/ftpusers pour interdire l'accès FTP à des comptes utilisateur

Cette option ajoute la directive `file=/etc/ftpusers` au fichier de configuration `/etc/pam.d/proftpd`.

Le fichier `/etc/ftpusers` contient une liste des utilisateurs qui ne doivent pas se connecter via 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 à ce 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 dans les accès FTP le mot de passe transite en clair sur le réseau.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

`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.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

6. Les clients Jabber

Jabber, également connu sous le nom de XMPP, est un ensemble de protocoles standards ouverts de l'IETF de messagerie instantanée et de présence, et plus généralement une architecture décentralisée d'échange de données.

Jabber est également un système de collaboration en quasi-temps-réel et d'échange multimédia via Jingle, dont la VoIP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

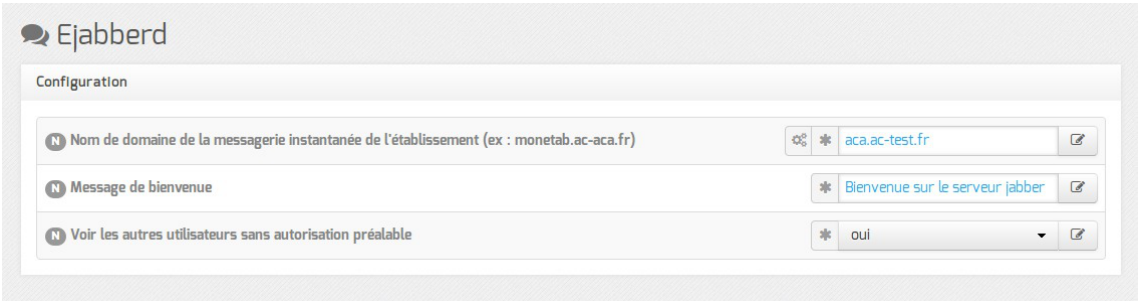
6.1. Mise en place du serveur jabber

Le service jabber (ejabberd) n'est pas pré-installé sur le module Scribe mais il est pré-packagé en tant que paquet additionnel.

Il faut donc installer le paquet manuellement avec la commande :

```
# apt-eole install eole-ejabberd
```

La configuration du serveur ejabberd peut être personnalisée dans l'onglet `Ejabberd` de l'interface de configuration du module.



- `Nom de domaine de la messagerie instantanée de l'établissement (ex : monetab.ac-aca.fr)` permet de personnaliser le nom de domaine des adresses de contact XMPP ;
- `Message de bienvenue` permet de personnaliser le message affiché lors de la connexion d'un utilisateur ;
- `Voir les autres utilisateurs sans autorisation préalable` active le module `shared_roster_ldap` qui permet de mettre en contact des utilisateurs sans entente préalable.

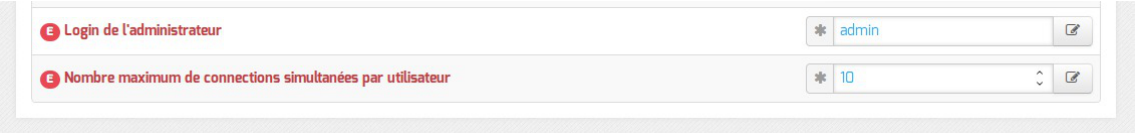
Le service n'est pas disponible immédiatement après l'installation.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Le service est activé par défaut, il peut être désactivé en répondant `non` à la question `Activer le serveur de messagerie instantanée ejabberd` dans l'onglet `Services` de l'interface de configuration du module.

La configuration du serveur ejabberd peut être affinée dans l'onglet `Ejabberd` de l'interface de configuration du module en mode expert.



- `Login de l'administrateur` permet de définir l'utilisateur qui sera administrateur du serveur ejabberd ;
- `Nombre maximum de connections simultanées par utilisateur` permet de limiter le nombre de connexions simultanées par utilisateur.

Vous pouvez vérifier que vous êtes effectivement connecté en lançant la commande suivante sur le serveur :

```
# ejabberdctl connected-users
```

D'autres commandes `ejabberdctl` sont disponibles et documentées avec l'option `help` :

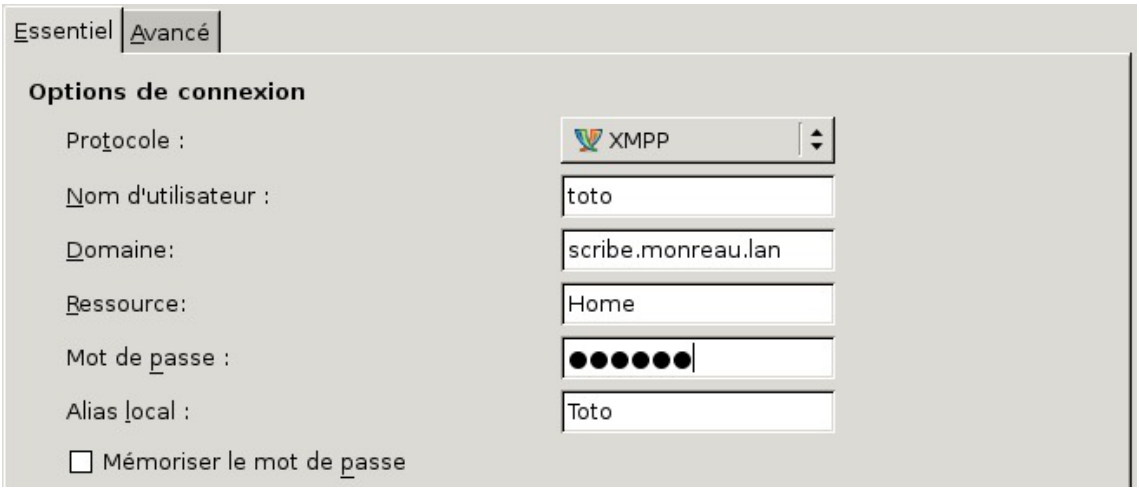
```
root@ejabber:~# ejabberdctl help
```

6.2. Configuration d'un client

Une fois le service mis en place, il est possible de s'y connecter en utilisant un compte présent dans l'annuaire.

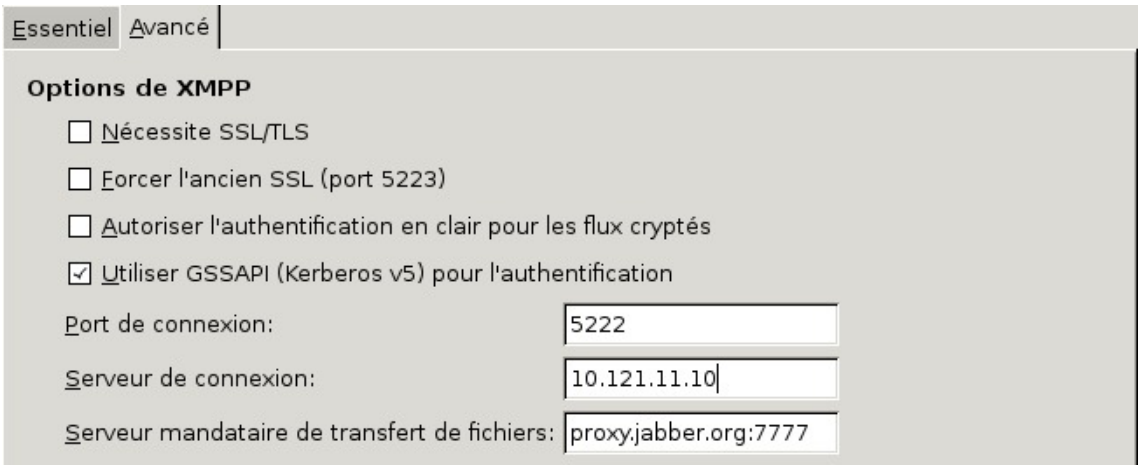
De nombreux logiciels sont compatibles jabberd, les plus connus sont : Pidgin, Gajim, Coccinella et Kopete.

Configuration de Pidgin



Configuration de Pidgin : onglet Essentiel

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

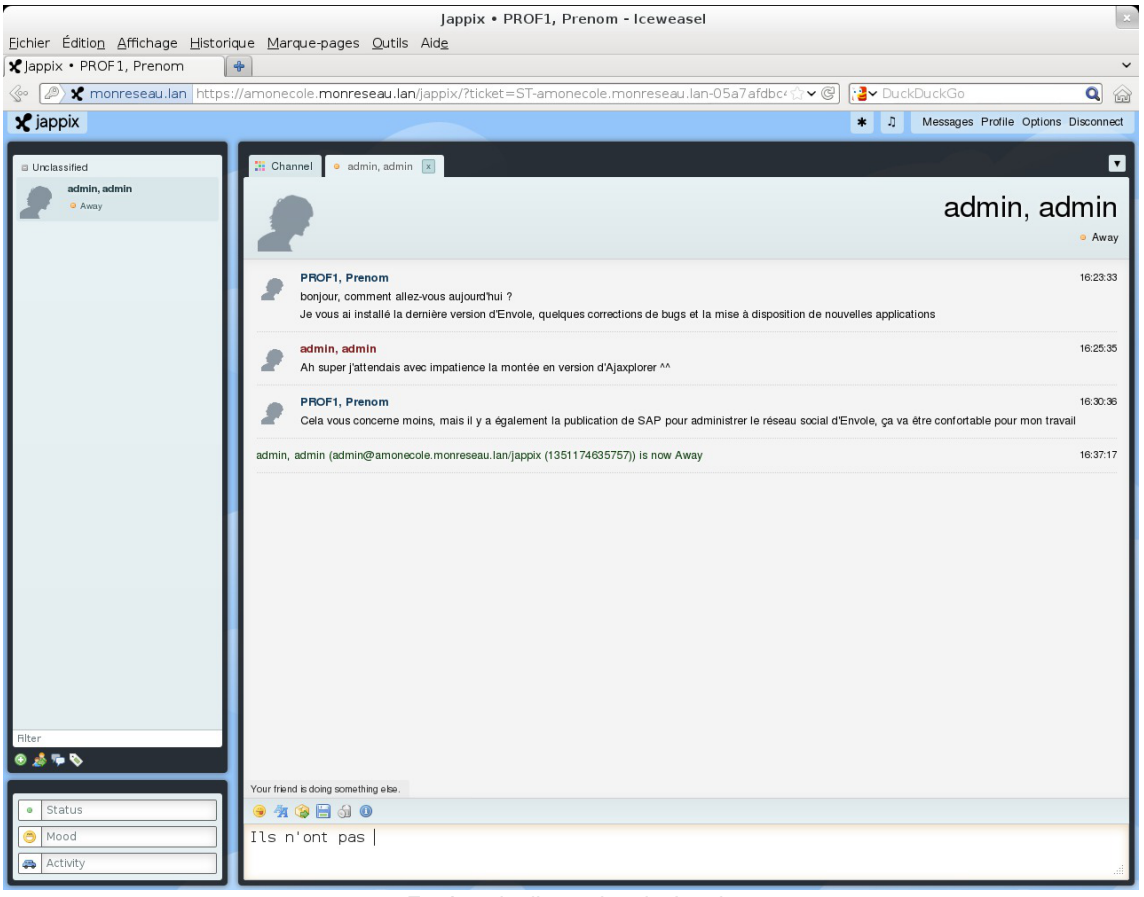


Configuration de Pidgin : onglet Avancé

Il est également possible d'utiliser le client web Jappix sur les modules Scribe et AmonEcole.

6.3. Jappix : client web Jabber

Présentation



Fenêtre de discussion de Jappix

Jappix est un client web de communication instantanée. Il est libre et basé sur le protocole XMPP[p.906].
Il permet une communication en temps réel entre les personnes possédant un compte XMPP.
Cette communication se fait simplement en utilisant un navigateur web moderne.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Un canal est à disposition pour laisser des messages de statut.

http://jappix.com

Installation

Jappix s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-jappix
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Si le serveur Jabber n'est pas installé un conteneur supplémentaire doit être créé, il faut donc exécuter la commande `gen_conteneurs` comme le propose la commande reconfigure.

Cette commande doit être suivie de la ré-instanciation du module avec la commande instance :

```
# instance /etc/eole/config.eol
```



L'application nécessite que le service `ejabberd` soit activé.

Dans l'interface de configuration du module, onglet `Services`, mettre `Activer le serveur de messagerie instantanée ejabberd` à `oui`.

L'application est très sensible à la configuration réseau mise en œuvre et son fonctionnement requiert notamment des noms DNS.

La configuration recommandée est donc la suivante :

domain_jabber_etab = eolesso_adresse = web_url = ssl_subjectaltname_ns = "nom_de_domaine"

Si cette configuration n'est pas respectée, l'erreur suivante s'affichera :

```
Erreur » Service indisponible
```

Attention la modification de certains de ces paramètres nécessite de régénérer les certificats.



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 : `http://<adresse serveur>/jappix/`

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Remarques

Par défaut il n'est pas possible de téléverser des fichiers dans le canal car il n'y a pas de gestion des quotas et la partition du conteneur pourrait se remplir très vite :

En attendant, il est tout de même possible d'activer cette fonctionnalité en créant un répertoire accessible en écriture à Apache :

`# ssh reseau`

`# mkdir /usr/share/jappix/store/share`

`# chown www-data:root /usr/share/jappix/store/share`

ctrl + d pour sortir de la connexion SSH.

7. Administration des listes de diffusion

7.1. Présentation

Sur le module Scribe, le logiciel de gestion de listes de diffusion Sympa[p.902] est pré-installé et configuré de manière à s'intégrer totalement au module.

De la même manière que le système de messagerie de ces modules, le gestionnaire de listes de diffusion gère deux domaines :

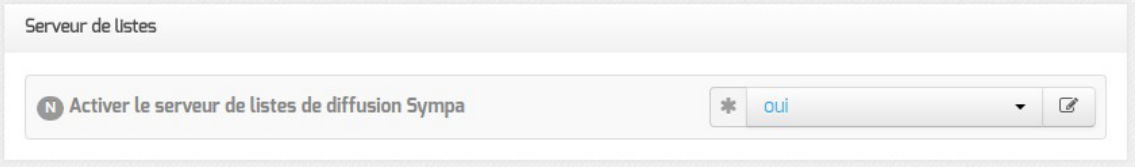
- un domaine Internet, du type **etablissement.ac-acad.fr** ;
- un domaine restreint du type **i-etablissement.ac-acad.fr**.

Sur le module Scribe des listes sont créées automatiquement pour les groupes existants. Mais il est également possible d'en créer manuellement.

Par défaut, l'utilisateur `admin` est l'administrateur de l'application web Sympa et le propriétaire de toutes les listes. Il a un accès complet à la gestion des listes. Il peut déléguer ce rôle en donnant les droits administrateur à un utilisateur.

Il est possible de désactiver les listes de publipostage dans l'onglet Messagerie de l'interface de configuration du module.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



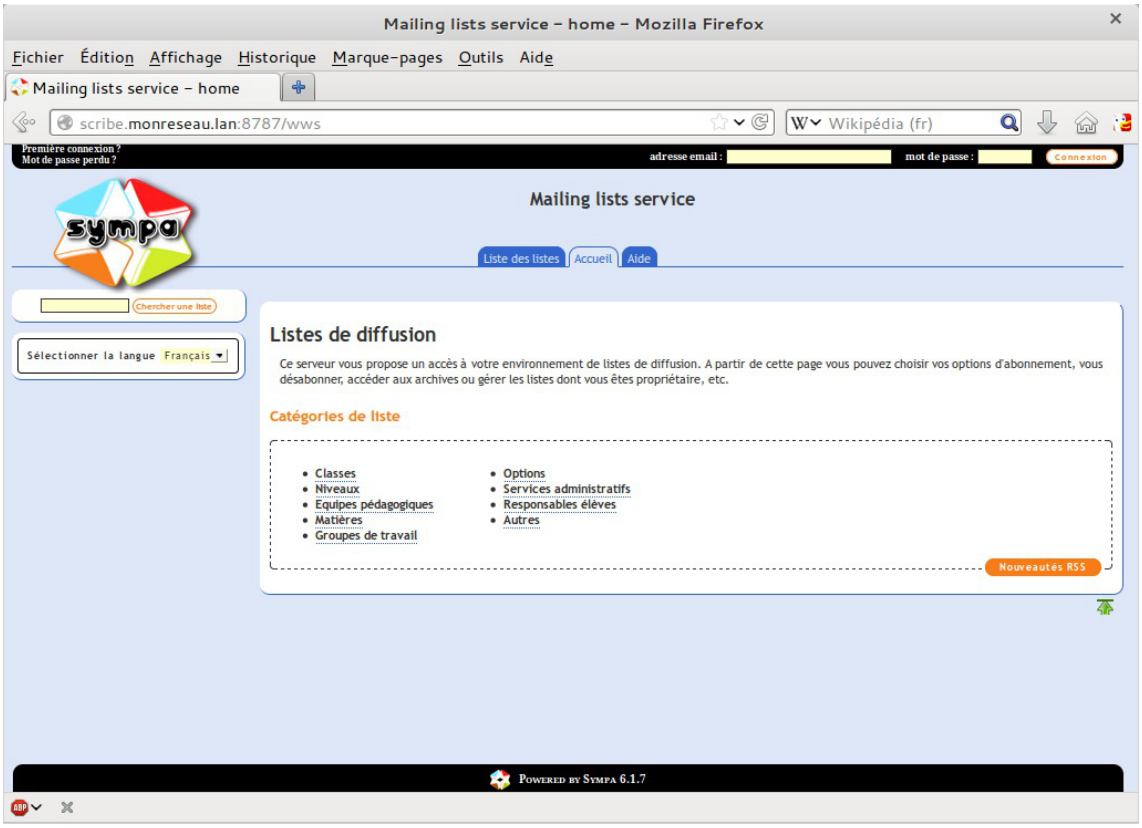
7.2. L'interface web

L'interface web (nommée WWSympa) est constituée d'une interface principale, pour le domaine Internet et d'une interface secondaire (robot), pour le domaine restreint. Elles sont accessibles sur les adresses suivantes :

- `http://adresse_interne:8787/wws` pour le domaine etablissement.ac-acad.fr
- `http://adresse_interne:8888/wws2` pour le domaine i-etablissement.ac-acad.fr

Chacune dispose de sa propre interface d'administration.

Pour se connecter à l'interface web en tant qu'utilisateur `admin`, il n'est pas obligatoire de renseigner l'adresse email comme demandé par l'interface, le compte `admin` suffit.



Les interfaces Sympa sont accessibles uniquement via l'adresse privée du module Scribe.

Sur le module AmonEcole, l'adresse à utiliser est celle de l'interface 1 du serveur.

Il est également possible de créer des listes de diffusion afin d'y inscrire des personnes extérieures.

Ainsi, il est envisageable de créer des listes de toutes sortes (projets locaux, passionnés de kayak, etc.).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

7.3. Les listes créées automatiquement

La plupart des groupes créés par le mécanisme d'importation et via l'EAD se voient associer une liste de diffusion du même nom sur le domaine interne.

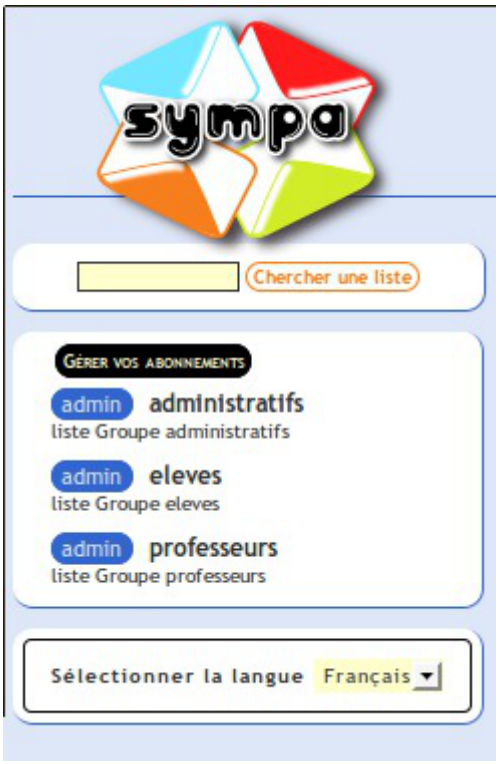
Ces listes sont créées automatiquement et les abonnés de la liste de diffusion sont synchronisés avec ceux du groupe LDAP toutes les deux heures.

Un individu n'est donc pas inscrit à la liste immédiatement après son affectation au groupe.

La synchronisation LDAP implique que la liste des abonnés à la liste ne soit pas modifiable via l'interface Sympa.

Les listes suivantes sont automatiquement créées dans le domaine interne :

- liste `administratifs` ;
- liste `professeurs` ;
- liste `eleves` ;
- liste `resp-<classe>` (responsables).



Pour qu'un personnel enseignant ou administratif apparaisse dans les listes, il est impératif qu'il possède une boite aux lettres locale ou que son adresse de messagerie personnalisée soit renseignée.

Liste pour les responsables

Des listes sont créées automatiquement pour chaque classe avec comme nom `resp-<classe>` et servent à inscrire les responsables de chacun des élèves qui composent cette classe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ces listes ne sont pas peuplées automatiquement, de plus elles ne sont pas visibles dans Roundcube sauf lorsque l'on crée un groupe du même nom. Il n'est pas possible de créer des groupes de responsables sans partage.

Peupler des listes de diffusion

Un document sur la *Création de listes de diffusion (globale et par classe) pour les responsables* écrit (octobre 2014) pour la version 2.3 d'EOLE par Sylvain Godmé et sous licence Creative Commons by-nc-sa reste valable et est consultable à l'adresse suivante :

http://eole.ac-dijon.fr/documentations/2.3/contributions/Creation-liste-responsables.pdf

Créer une liste de tous les responsables

Voici une méthode pour créer la liste de tous les responsables (avec une domaine "-i") sur un module Scribe.

```
# domaine_messagerie_etab=$(CreoleGet domaine_messagerie_etab)
# mkdir /var/lib/sympa/expl/i-$domaine_messagerie_etab/responsables
# touch /var/lib/sympa/expl/i-$domaine_messagerie_etab/responsables/info
# cp /var/lib/sympa/expl/i-$domaine_messagerie_etab/professeurs/config
/var/lib/sympa/expl/i-$domaine_messagerie_etab/responsables/config
# chown -R sympa:sympa /var/lib/sympa/expl/i-$domaine_messagerie_etab/responsables
# python -c "from scribe.eolegroup import
_add_maillist_aliases;_add_maillist_aliases({'groupe':'responsables',
'ldomaine':'i-$domaine_messagerie_etab'})"
```

Éditer le fichier `/var/lib/sympa/expl/i-$domaine_messagerie_etab/responsables/config` et appliquer les modifications suivantes :

- modifier le sujet de la liste à la première ligne (ex : `subject liste de tous les responsables`) ;
- modifier la catégorie de la liste (ex : `topics Responsables`) ;
- remplacer `include_ldap_2level_query` par `include_ldap_query` ;
- à la ligne débutant par `suffix1`

  remplacer le début `suffix1 cn=professeurs,ou=local,ou=groupes`, par `suffix ou=local,ou=responsables,ou=utilisateurs,` ;
- supprimer toutes les lignes suivantes jusqu'à la fin du fichier et les remplacer par celles qui suivent :

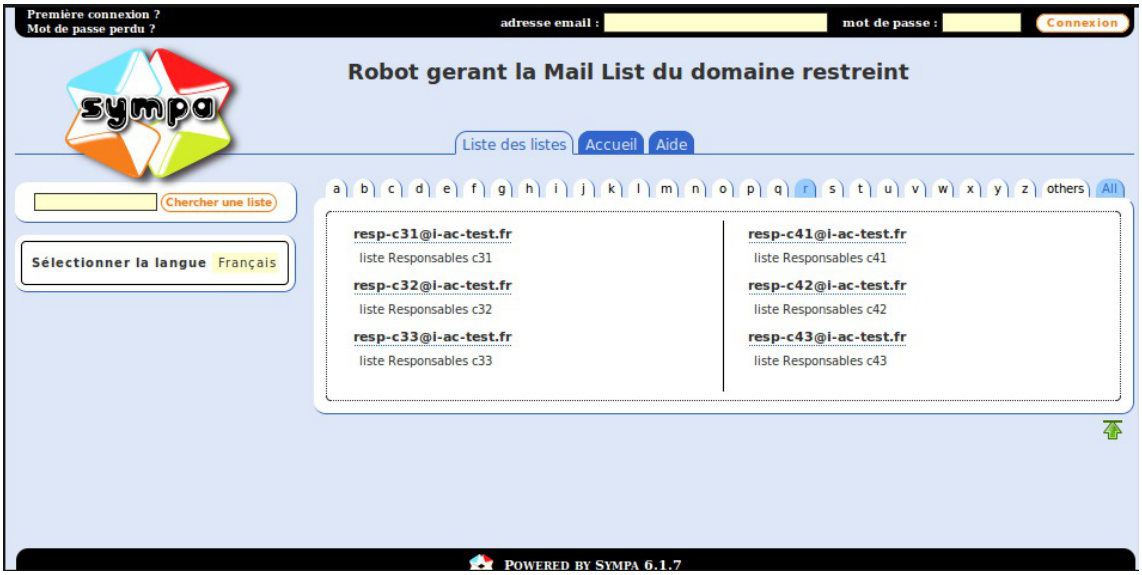
  `filter (objectClass=responsable)`

  `attrs mail`

  `select all`

  `scope sub`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Il faut laisser le temps au daemon sympa de réaliser la synchronisation LDAP pour que les membres de la liste soient les bons.

En effet la copie du fichier config a été faite à partir de la liste professeurs et tant que le sync_include() ne s'est pas fait ce sont les professeurs qui sont membres.

Voir aussi...

Roundcube : interface pour le courrier électronique [p.705]

7.4. Création manuelle de listes

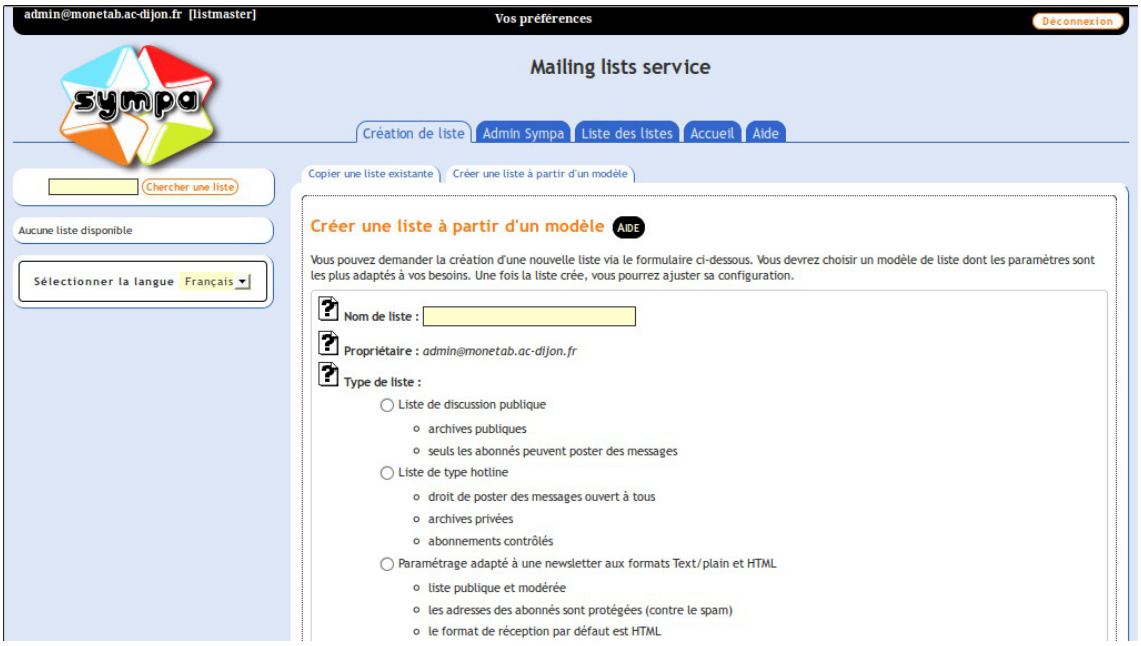
L'application permet de créer manuellement des listes totalement indépendantes de l'annuaire LDAP[p.892] .

Les membres de ces listes sont stockés dans la base MySQL[p.893] de Sympa.

Cette possibilité est utile dans le cas où l'on souhaite gérer une liste de diffusion impliquant des personnes extérieures à l'établissement par exemple.

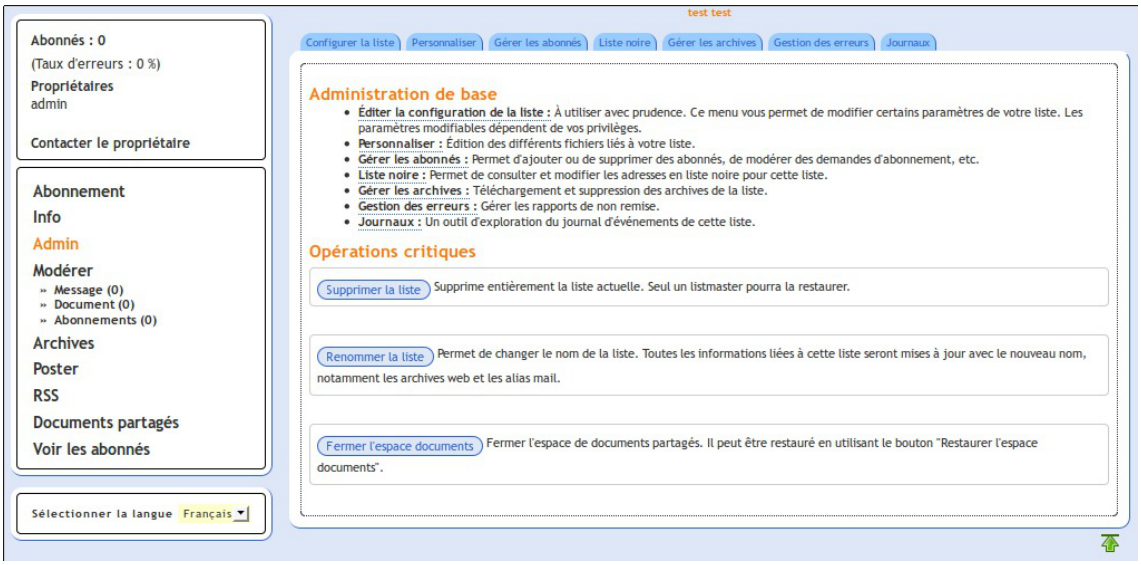
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Création de liste manuelle



Création d'une liste manuelle par l'interface web de Sympa

1. se connecter à l'interface du domaine souhaité avec le compte `admin` ;
2. cliquer sur l'onglet `Création de liste` ;
3. choisir un nom pour cette nouvelle liste (sans espace ni caractère spécial) ;
4. bien réfléchir au `Type de liste` désiré ;
5. saisir l'objet de la liste (descriptif court) ;
6. choisir sa catégorie (le plus souvent `Groupes de travail` ou `Autre`) ;
7. et la description de la liste (descriptif long) ;
8. cliquer sur `Envoyer votre demande de création` ;
9. le bouton `Admin` du menu de gauche permet ensuite d'accéder à la gestion de la liste et des abonnés.



Vue de la page d'administration

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

7.5. Architecture du gestionnaire de liste de diffusion

Les fichiers de configuration définissant chaque liste de diffusion sont stockés dans un répertoire du nom de la liste dans :

- `/var/lib/sympa/expl/` pour les listes du domaine Internet ;
- `/var/lib/sympa/expl/i-monetab.ac-acad.fr` pour les listes du domaine interne

C'est l'une des raisons pour lesquelles il n'est pas possible de modifier la variable `domaine_messagerie_etab` une fois l'instanciation du serveur effectuée.

Les archives des listes sont stockées dans le répertoire `/var/lib/sympa/wwsarchive`.

Pour redémarrer Sympa il faut utiliser la commande `service sympa restart` . Avant cela il faut impérativement que MySQL soit démarré, sinon des erreurs se produiront.

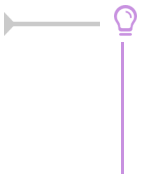
L'interface web Sympa est gérée par le fichier `/usr/lib/cgi-bin/sympa/wwsympa.fcgi`. Il s'agit d'un script CGI[p.885] en perl qui utilise le mode *fcgid* d'apache2 pour fonctionner. La présence d'un sticky bit sur ce fichier est nécessaire pour assurer le bon fonctionnement de l'application.

Les alias des listes de diffusions (utilisés par le MTA[p.893] Exim4[p.889]) sont stockés dans le fichier `/etc/mail/sympa.aliases`

Pour plus d'information, veuillez vous référer à la documentation officielle du logiciel :

http://www.sympa.org/doc/index

Sur le module AmonEcole, tous les fichiers indiqués ci-dessus se trouvent dans le conteneur `bdd`.



Pour modifier les *Catégories de liste* proposées, il est obligatoire de patcher le template EOLE :

`/usr/share/eole/creole/distrib/topics.conf`.

7.6. Architecture messagerie académique

Pour fonctionner pleinement, le système de messagerie proposé sur les modules EOLE a besoin d'adaptations au niveau des serveurs académiques.

Il faut :

- un DNS[p.887] configuré avec les noms de domaines des établissements ;
- un relai SMTP[p.899].

Le relai académique doit être capable de distribuer les adresses Internet (`etab.ac-acad.fr`) et les adresses restreintes (`i-etab.ac-acad.fr`).

Si vous n'avez pas de relai académique, votre domaine restreint sera limité à l'établissement et non à l'Académie.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le DNS

Au niveau du DNS académique, il faut écrire les MX de chacun des domaines Internet des établissements, en les faisant pointer vers le relai académique.

Le relai SMTP

Au niveau des modules Scribe, le relai de messagerie étant le relai académique, tous les courriers électroniques du domaine Internet ou restreint d'autres établissements arriveront sur le relai.

La distribution des courriers électroniques se fait ensuite grâce au routage SMTP (table de routage Postfix ou Exim).

En fonction de vos architectures, vous pouvez remonter sur le module Scribe, soit via votre réseau de concentration, soit via un réseau VPN (Amon-Sphynx), soit via Internet en mettant en place du SNAT sur le pare-feu établissement.

Nous recommandons de positionner le module Scribe sur une DMZ de l'établissement.

Il est recommandé d'utiliser une passerelle dédiée pour faire du routage SMTP avec anti-virus et anti-spam.

Comme toujours en architecture réseau il n'y pas de solution unique !



Le module Seshat permet de mettre en place simplement un relai académique.

7.7. Résoudre des dysfonctionnements liés aux listes de diffusion

Indications utiles au débogage du gestionnaire de listes Sympa :

- les messages d'erreur se trouvent dans le fichier journal : `/var/log/rsyslog/local/exim/exim.info.log` ;
- le gestionnaire de listes Sympa journalise également des informations dans `/var/log/syslog` ;
- les droits sur `/var/lib/sympa` doivent être `sympa:sympa` ;
- vérifier la présence du sticky bit (-rwsr-sr-x 1 sympa sympa) sur le fichier `/usr/lib/cgi-bin/sympa/wwsympa.fcgi` :

```
# ll /usr/lib/cgi-bin/sympa/wwsympa.fcgi
-rwsr-sr-x 1 sympa sympa 611477 avril 10 2014 /usr/lib/cgi-bin/sympa/wwsympa.fcgi*
```

- vérifier que la liste est bien référencée dans `/etc/mail/sympa.aliases` ;
- vérifier que toutes les composantes de l'application sont en service :

```
root@serv-pedago:~# ps -edf | grep sympa
root 21675 21649 0 13:56 pts/0 00:00:00 grep --color sympa
sympa 27000 1 0 07:00 ? 00:00:04 /usr/bin/perl /usr/lib/sympa/bin/sympa.pl
sympa 11183 1 0 07:00 ? 00:01:00 /usr/bin/perl /usr/lib/sympa/bin/bulk.pl
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
sympa    27003    1    0    07:00    ?    00:00:00    /usr/bin/perl
/usr/lib/sympa/bin/archived.pl
sympa    27006    1    0    07:00    ?    00:02:31    /usr/bin/perl
/usr/lib/sympa/bin/task_manager.pl
sympa    27011    1    0    07:00    ?    00:00:00    /usr/bin/perl
/usr/lib/sympa/bin/bounced.pl
```

Sur le module AmonEcole, les fichiers et processus mentionnés ci-dessus, autres que les journaux systèmes, se trouvent dans le conteneur `bdd`.

Pour se connecter au conteneur `bdd` utiliser la commande :

```
# ssh bdd
```

8. Synchronisation depuis l'Annuaire Académique Fédérateur - AAF

Fonctionnement général de la synchronisation

1. la machine ODI[p.895] génère une archive `tar.gz` par établissement à synchroniser ;
2. dès l'archive terminée, elle est envoyée sur le module Zéphir accompagnée d'une notification ;
3. le module Zéphir envoie l'archive sur le module Scribe auquel elle a été associée ;
4. le module Scribe lance l'import de l'archive (mode automatique) ou la stocke pour l'EAD (mode manuel).

Comment récupérer les fichier tar.gz ?

Information et documentation à retrouver sur le site **intranet** de diffusion de l'académie de Toulouse :

http://nservdiff.in.ac-toulouse.fr/appli/infra/versions/ver_majaaf.html [http://nservdiff.in.ac-toulouse.fr/appli/infra/versions/ver_majaaf.html]

Guide utilisateur 1.5 en version format privateur `.doc` :

http://nservdiff.in.ac-toulouse.fr/appli/infra/documentation/aaf/Guide_UtilisateurV1_5.doc

Guide d'exploitation 1.5 en version format privateur `.doc` :

http://nservdiff.in.ac-toulouse.fr/appli/infra/documentation/aaf/Dossier_exploitationV1_5.doc

Association archive - module Scribe

L'association d'un module Scribe avec son archive se fait pour l'instant manuellement, à l'aide du code python suivant :

```
import xmlrpclib
z = xmlrpclib.Server("https://utilisateur:codeSecret@adresse_zephir:7080")
z.aaf.add_file(idZéphir, 'nomArchive.tar.gz')
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour afficher la liste des archives associées au module Scribe possédant l'identifiant Zéphir `idZéphir` :

```
z.aaf.get_list(idZéphir)
```

Pour supprimer l'association entre l'archive et le module Scribe :

```
z.aaf.del_file('nomArchive.tar.gz')
```

Dans cet exemple, on associe l'archive `0000001a.tar.gz` au module Scribe possédant l'identifiant `58` dans l'application web Zéphir :

```
import xmlrpclib
z = xmlrpclib.Server("https://user:password@adresse_zephir:7080")
z.aaf.add_file(58, '0000001A.tar.gz')
```

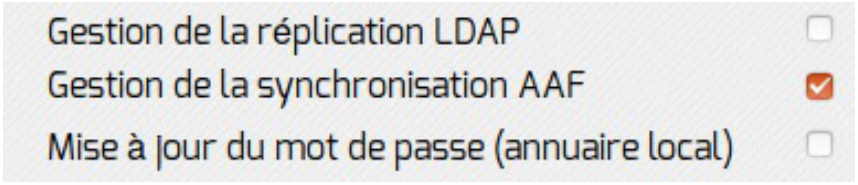
Pour afficher la liste des archives associées au module Scribe possédant l'identifiant 58 dans l'application web Zéphir :

```
z.aaf.get_list(58)
```

Pour supprimer l'association entre l'archive `0000001A.tar.gz` et le module Scribe :

```
z.aaf.del_file('0000001A.tar.gz')
```

L'utilisateur Zéphir utilisé pour effectuer les manipulations décrites ci-dessus doit posséder le droit `Gestion de la synchronisation AAF` dans l'application Zéphir.



Envoi des fichiers sur le module Zéphir

Les archives générées (de la forme `<numéro UAI>.tar.gz`) doivent être envoyées dans le répertoire : `/var/lib/zephir/aaf`.

L'envoi des fichiers peut être réalisé par la méthode de votre choix : `rsync`, `scp`, ...

Une fois l'archive envoyée, il faut notifier cet envoi au module Zéphir.

Cela peut être fait par les lignes python suivantes :

```
import xmlrpclib
z = xmlrpclib.Server("https://utilisateur:codeSecret@adresse_zephir:7080")
z.aaf.notify_upload('numeroUAI.tar.gz')
```

L'utilisateur Zéphir utilisé pour effectuer les manipulations décrites ci-dessus doit posséder le droit `Gestion de la synchronisation AAF` dans l'application Zéphir.

Gestion de l'archive sur le module Scribe

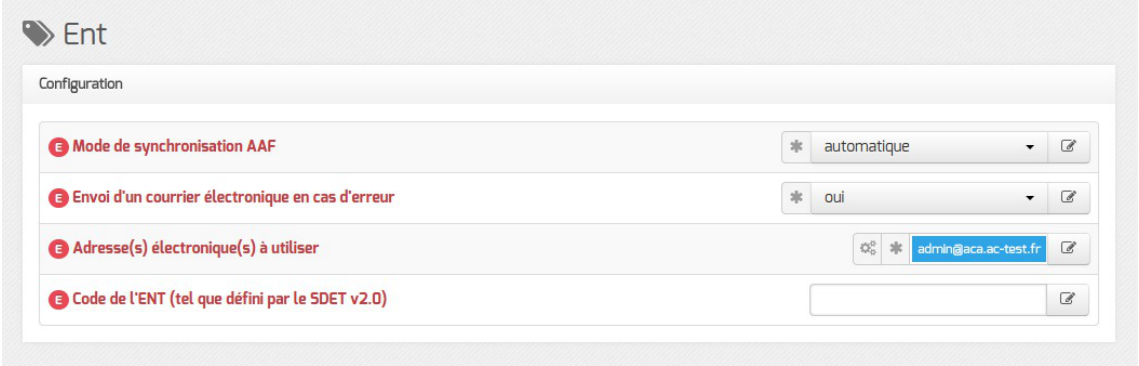
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Dès que le module Zéphir est notifié de l'arrivée d'une nouvelle archive, il prépare son envoi vers le module Scribe qui lui est associé (sauf si l'archive possède la même signature que sa version précédente).

Le module Scribe récupère l'archive lors de sa connexion au module Zéphir.

Il est possible de configurer la façon dont le module importe les données de l'archive récupérée.

Cela se paramètre dans l'interface de configuration du module, en mode expert, dans l'onglet `Ent`.



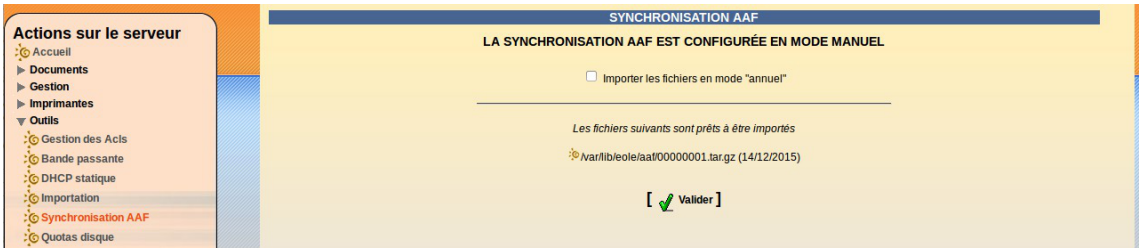
La variable `Mode de synchronisation AAF` permet de choisir entre deux modes :

- **automatique** : l'importation des fichiers est exécutée dès leur réception ;
- **manuel** : l'archive est stockée et l'importation est prête à être exécuté par l'EAD (menu `Outils` / `Synchronisation AAF`).

La variable `Envoi d'un courrier électronique en cas d'erreur` active l'envoi d'un courrier électronique en cas d'erreur lors de l'import manuel ou automatisé des fichiers AAF. Le ou les destinataires de ce message sont à ajouter dans `Adresse(s) électronique(s) à utiliser`.

Si le module Scribe est configuré en mode manuel, l'import des archives envoyées sur le module Scribe se réalise à la demande en allant dans l'EAD.

Le formulaire d'import est accessible par le menu `Outils` / `Synchronisation AAF`.



Importation des fichiers AAF synchronisés via l'EAD

Par défaut l'import est réalisé en mode *Mise à jour des bases*, mais il est possible de l'effectuer en mode *Importation annuelle des bases* en cochant la case `☑ Importer les fichiers en mode "annuel"`.

- *Mise à jour des bases* : ajoute les utilisateurs et groupes manquants sans modifier les groupes existants ;
- *Importation annuelle des bases* : ajoute les utilisateurs et groupes manquants après avoir purgé les options (import des élèves) ou les équipes pédagogiques (import des professeurs).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'import peut également être exécuté en ligne de commande en utilisant le script `synchro_aaf` avec comme paramètre l'un des fichiers cité dans `/var/lib/eole/aaf/aaf_files/`.

Exemple de boucle en bash[p.884] qui permet de traiter tous les fichiers :

```
for f in `cat /var/lib/eole/aaf/aaf_files`; do
    /usr/bin/synchro_aaf $f
done
```

Suivi de la synchronisation et de l'importation

Agent Zéphir

Un agent Zéphir permet de vérifier le bon déroulement de l'envoi des fichiers sur le module.



L'agent de surveillance de la synchronisation des fichiers AAF

Application web Zéphir

Des informations sont également disponibles en allant dans `Logs complets` depuis la page d'état de l'un des serveurs Scribe et en filtrant sur `divers`.



Surveillance de la prise en compte des fichiers AAF dans Zéphir

Rapports d'importation

L'importation des fichiers AAF synchronisés utilise les même scripts que l'importation habituelle, on retrouve donc les rapports de l'importation AAF aux endroits suivants :

- page d'accueil de l'EAD (`/usr/share/ead2/backend/tmp/importation/rapport.txt`) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

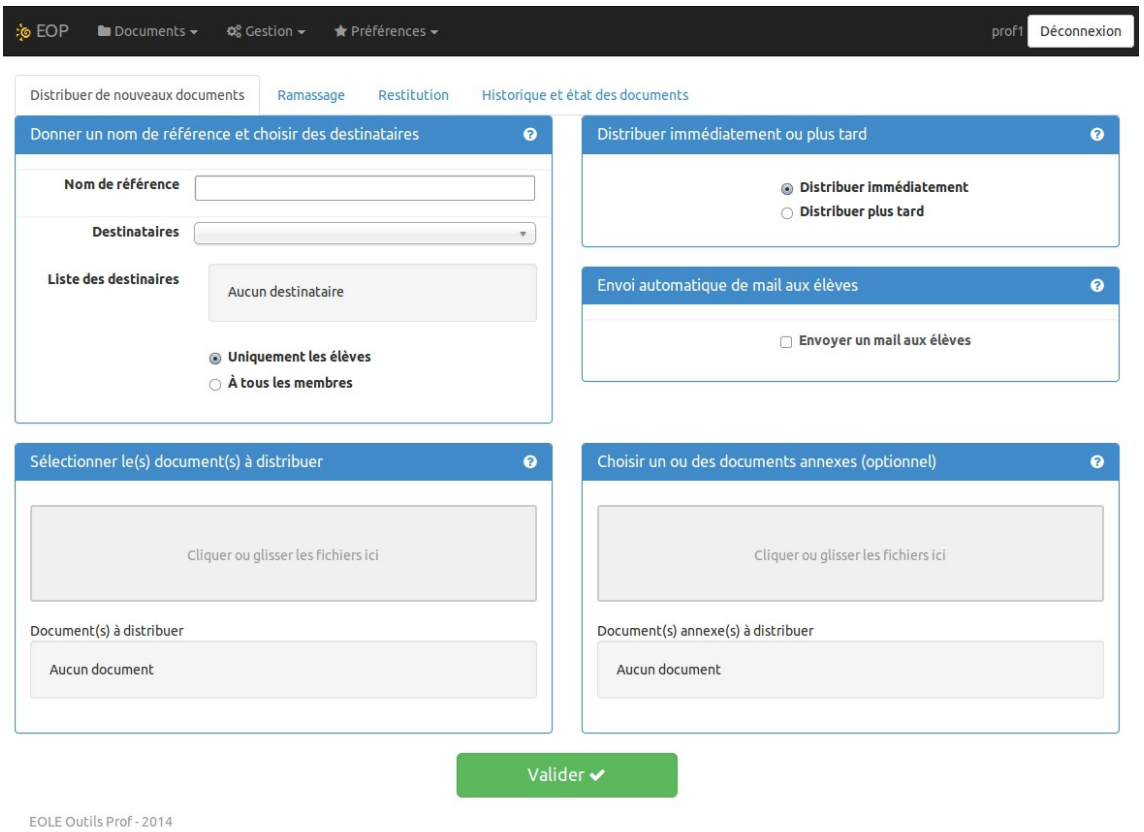
- répertoire personnel de l'utilisateur `admin` : `/home/a/admin/perso/importation` ;
- journaux complets : `/var/log/eole/importation.log`.

9. Outils à destination des enseignants

9.1. EOP : application web à destination des enseignants

9.1.1. Présentation

Présentation



L'objectif de l'application web EOP (EOLE Outils Profs) est de proposer une interface simple contenant un ensemble d'outils à destination des enseignants. Cette nouvelle application, indépendante, ne traite pas uniquement de la gestion des documents et peut être intégrée dans un portail. Le développement est basé sur le framework python Flask[p.890].

http://dev-eole.ac-dijon.fr/projects/eop

Principales fonctionnalités

- gestion de documents (distribution simple, ou distribution et ramassage) ;
- observation et prise de contrôle des postes élèves ;
- possibilité de changer le mot de passe d'un élève ;
- possibilité de changer le mot de passe du compte enseignant.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette version d'EOP est compatible avec les navigateurs modernes ou avec une version d'Internet Explorer 9 et supérieure.

Installation

Cette application est pré-installée sur le module Scribe à partir de la version 2.4.2.

Pour désactiver l'application il faut se rendre dans l'interface de configuration du module en mode normal, dans l'onglet Applications web et passer `Activer EOP (gestion de devoir)` à `non`.
L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Accéder à l'application

Pour accéder à l'application il faut se rendre à l'adresse : `https://<adresse serveur>/eoleapps/eop/documents/`

Rôles des utilisateurs

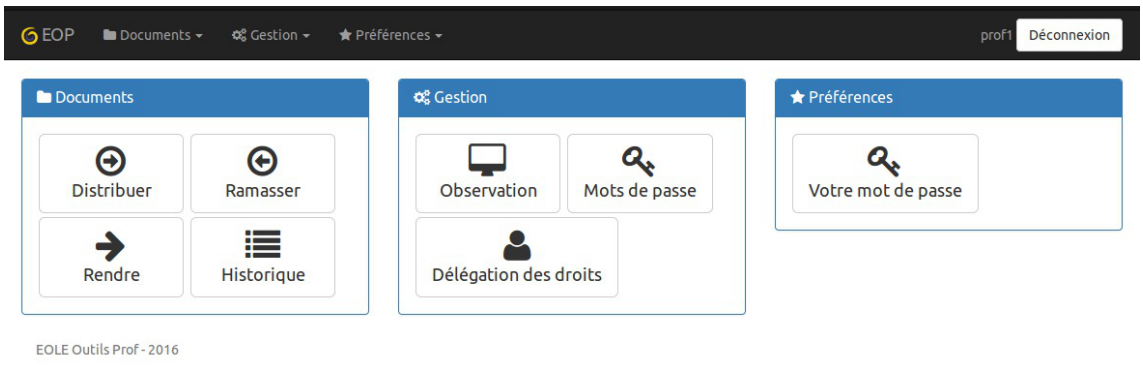
Seuls les enseignants et l'utilisateur `admin` (enseignant également) ont un accès à l'application.
Les professeurs principaux ont accès à quelques fonctionnalités supplémentaires.
Les élèves disposent des documents distribués dans leur répertoire personnel mais n'ont pas d'accès à l'application EOP.

Fonctionnalités

Le bandeau noir de l'interface permet un accès rapide aux différentes fonctionnalités.



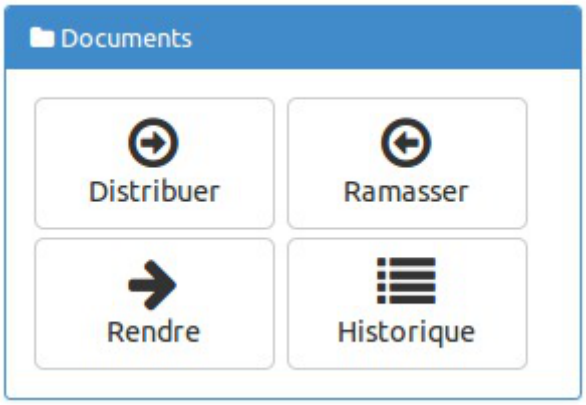
L'icône EOP permet d'afficher les différentes fonctionnalités sous forme de bouton.



À droite de l'interface apparaît l'identifiant utilisé et le bouton `Déconnexion`.

Menu Documents

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Distribuer : permet de gérer la distribution de documents ;
- Ramasser : permet de récupérer un document distribué et nécessitant la modification par les utilisateurs ;
- Rendre : permet d'annoter les documents ramassés et de les restituer ;
- Historique : permet de lister les différents documents et de connaître leur état.

Menu Gestion



- VNC : permet d'observer un ou plusieurs postes ou d'en prendre le contrôle à distance ;
- Mots de passe : visible uniquement avec le rôle de professeur principal, cette option permet de changer le mot de passe d'un ou de plusieurs utilisateurs.
- Délégation de droits : visible uniquement avec le rôle de professeur principal, elle permet de déléguer la gestion des mots de passe (dans EOP et EAD) et des comptes élève (dans l'EAD) pour une classe donnée.

Menu Préférences

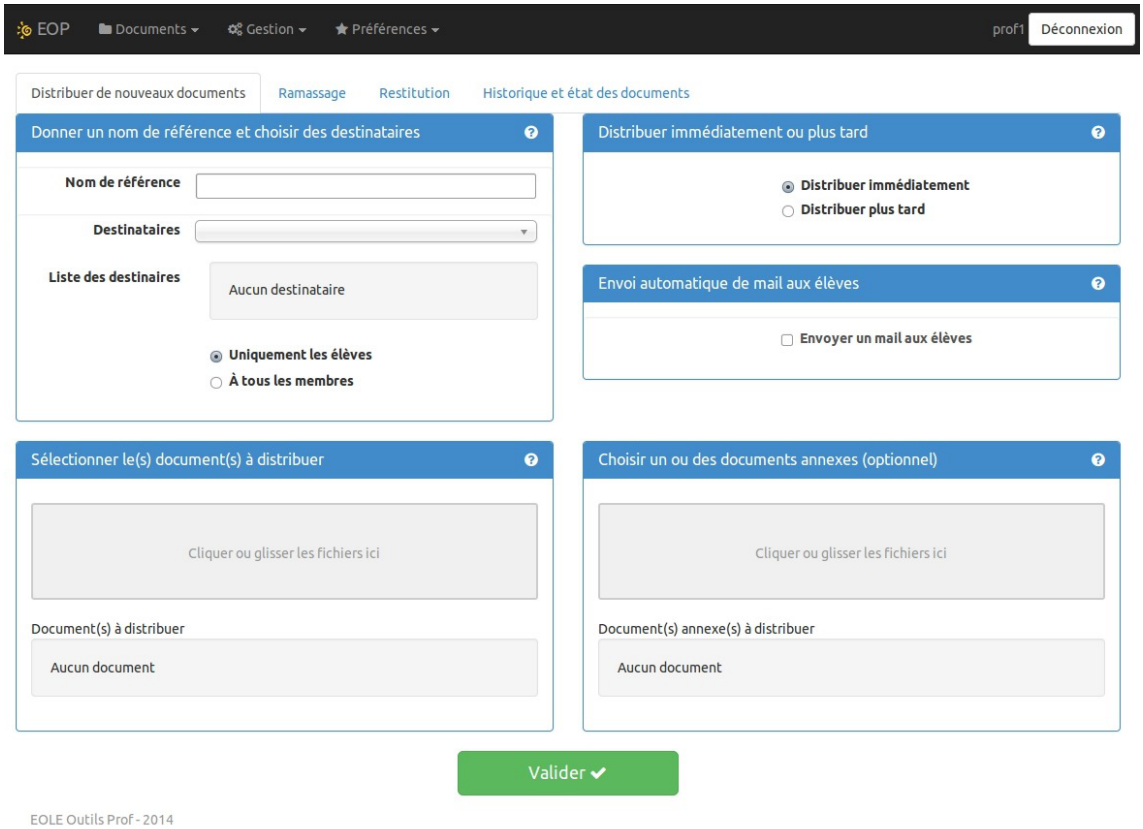
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Mots de passe : permet de modifier son propre mot de passe.

9.1.2. Distribution de documents

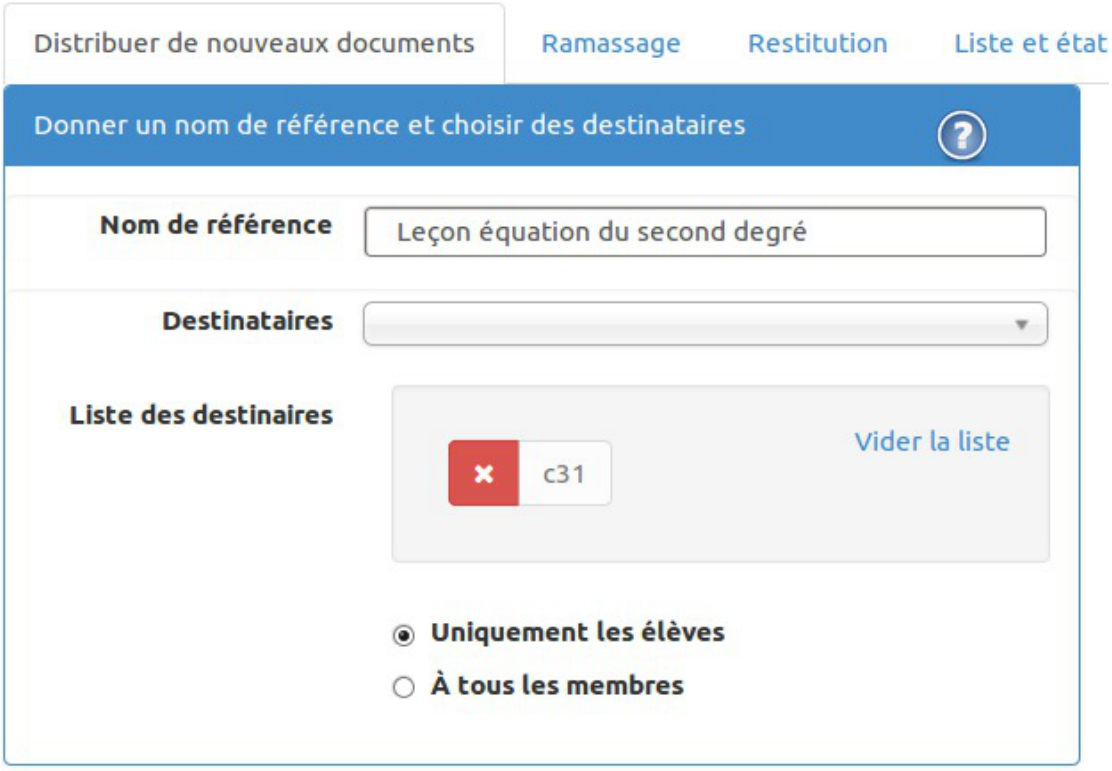
Par défaut l'arrivée sur l'application se fait sur la fonctionnalité et l'onglet Distribuer de nouveaux documents.



Plusieurs encadrés sont à remplir pour procéder à la distribution de documents.

Donner un nom de référence et choisir des destinataires

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Nom de référence

La référence vous permet d'identifier le processus de distribution durant les différentes étapes de sa vie (distribution, ramassage, restitution, suppression). Il permettra également à l'utilisateur d'identifier le répertoire de destination du ou des documents.

Destinataires

Vous devez sélectionner un ensemble de destinataires à qui distribuer la référence, celui-ci peut être une classe, une équipe, un groupe, une matière ou un niveau.

Uniquement les élèves / À tous les membres

Par défaut la référence n'est distribuée qu'aux élèves, en cochant l'option ☑ À tous les membres, vous pouvez distribuer la référence à tous les membres de l'ensemble.

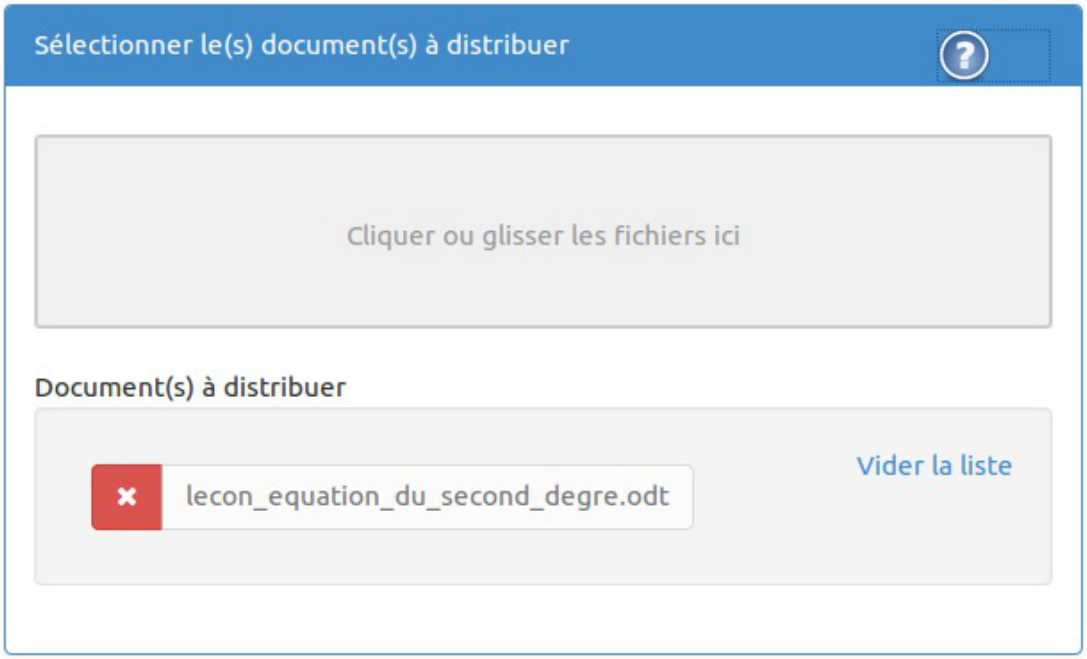
Vider la liste

Il est possible de supprimer des destinataires ajoutés par erreur. Vider la liste permet de supprimer tous les destinataires ajoutés.

Sélectionner le(s) document(s) à distribuer

Le(s) document(s) à distribuer seront accessibles en écriture par les utilisateurs dans leur répertoire personnel dans un sous-répertoire ayant pour nom celui de la référence.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Cliquer

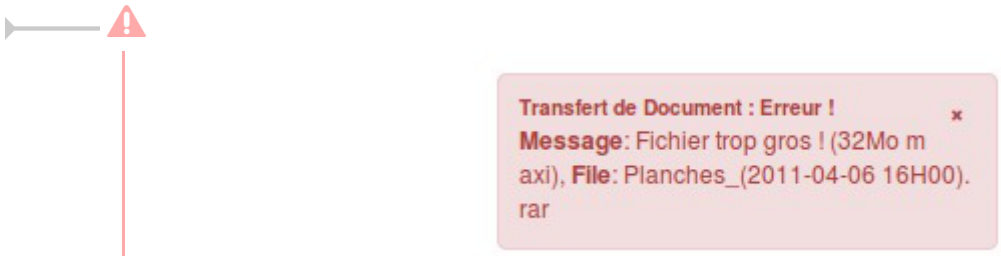
Vous pouvez cliquer dans la zone grise pâle pour ouvrir un navigateur de fichier. Celui-ci vous permet de choisir un ou plusieurs fichiers d'un même répertoire en maintenant la touche `Ctrl + clic`.

Glisser

Vous pouvez faire glisser un ou plusieurs documents dans la zone gris pâle depuis une autre fenêtre.

Vider la liste

Il est possible de supprimer un document téléversé par erreur. Vider la liste permet de supprimer tous les documents téléversés.

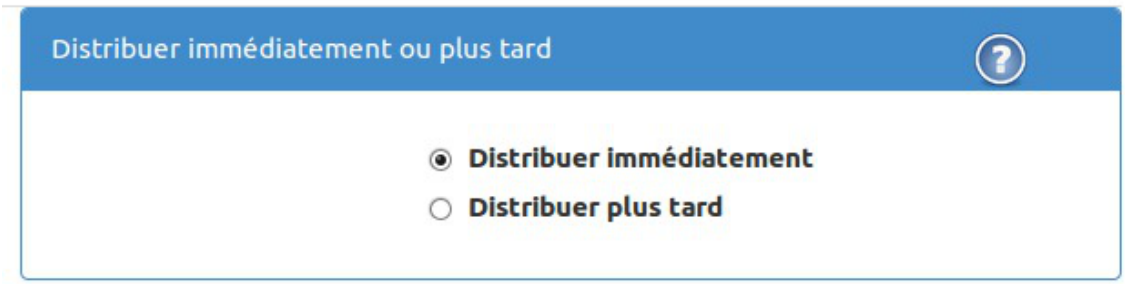


Si le message `Fichier trop gros !` apparaît, en bas à droite de la fenêtre, alors la valeur maximale pour la taille d'un fichier à téléverser doit être ajustée dans l'onglet `Apache` du module Scribe et/ou dans l'onglet `Reverse proxy` du module Amon en mode expert.

Distribuer immédiatement ou plus tard

La distribution peut être différée ou immédiate.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Distribuer immédiatement
La distribution a lieu après avoir cliqué sur le bouton Valider.

Distribuer plus tard
Cette option permet de préparer la distribution de document à distance ou dans l'établissement.
La distribution se fera en utilisant, au moment voulu, l'option `Distribuer` de l'application Gestion-postes à l'intérieur de l'établissement.

Envoi automatique de mail aux élèves

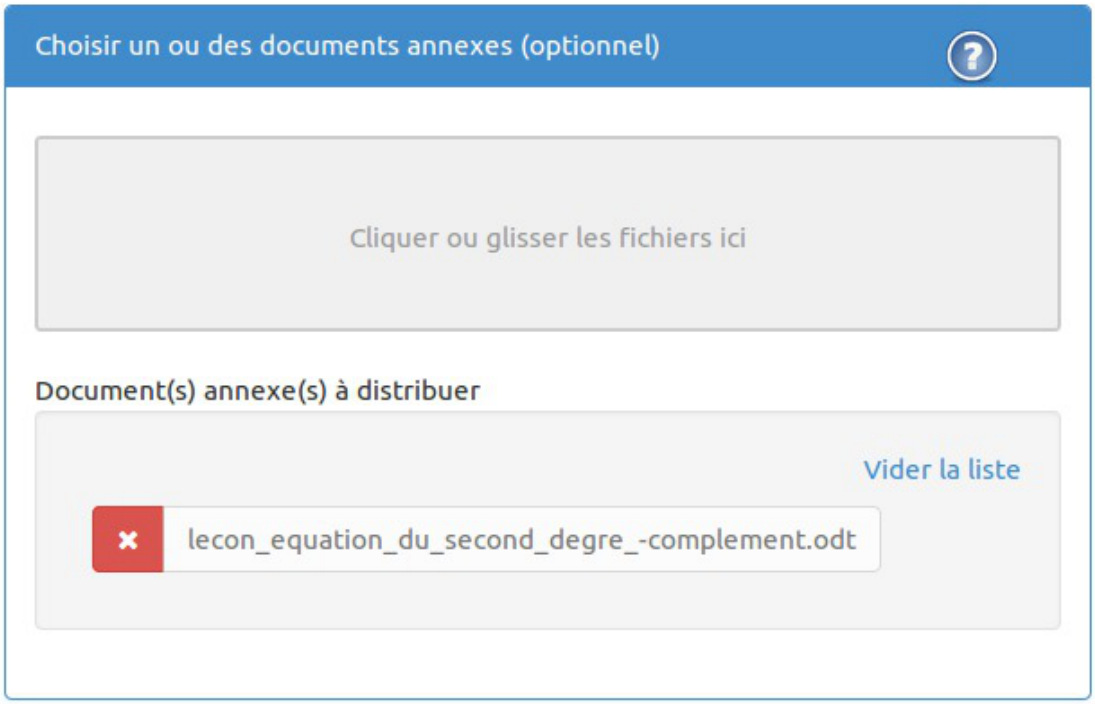
Un courrier électronique peut être automatiquement envoyé de votre part aux élèves destinataires des documents.
Pour cela, cochez la case et complétez le sujet et le corps avant de lancer la distribution.



Choisir un ou des documents annexes (optionnel)

Cette étape est optionnelle. Les annexes sont des documents qui ne seront pas accessibles en écriture par les utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Cliquer

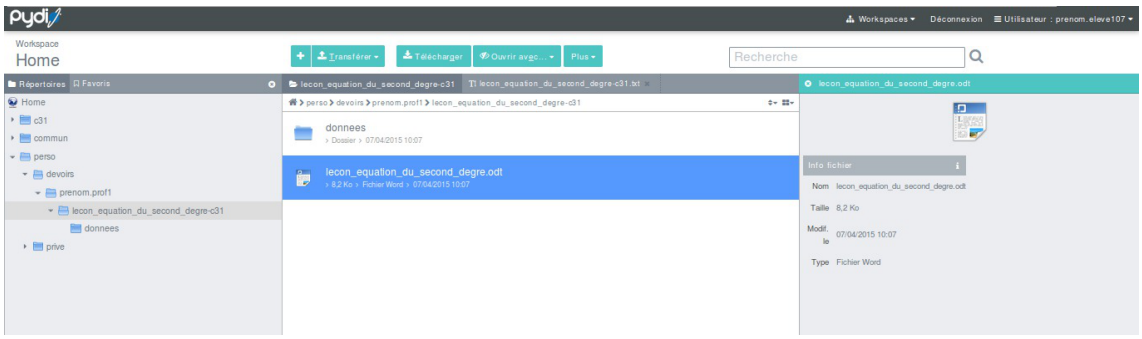
Vous pouvez cliquer dans la zone grise pâle pour ouvrir un navigateur de fichier. Celui-ci vous permet de choisir un ou plusieurs fichiers d'un même répertoire en maintenant la touche Ctrl + clic.

Glisser

Vous pouvez faire glisser un ou plusieurs documents dans la zone gris pâle depuis une autre fenêtre.

Vider la liste

Il est possible de supprimer un document téléversé par erreur. Vider la liste permet de supprimer tous les documents téléversés.



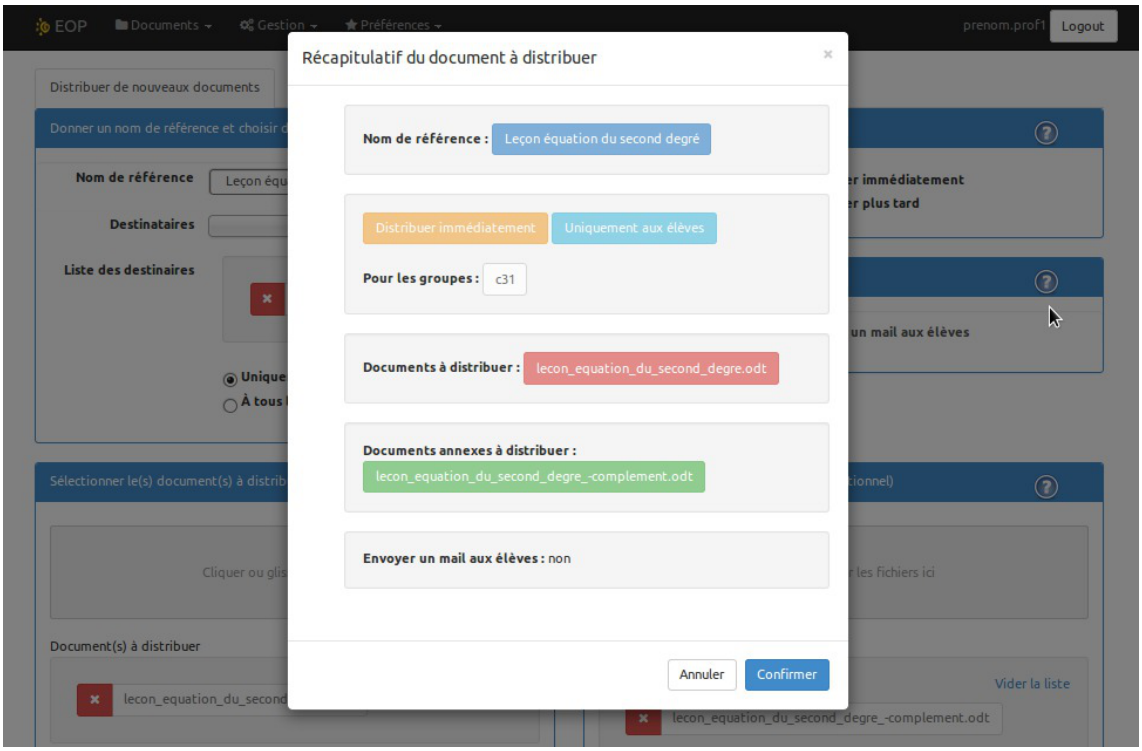
Les documents annexes sont disponibles dans le répertoire `donnees` qui lui se trouve dans le répertoire portant le nom de référence concaténé avec le nom de la classe. Ce répertoire est disponible dans le répertoire `/perso/devoirs/nom de l'enseignant/` de l'élève.

Valider la distribution

Pour valider la distribution il faut cliquer sur le bouton `Valider` en bas de page. La validation se fait après

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

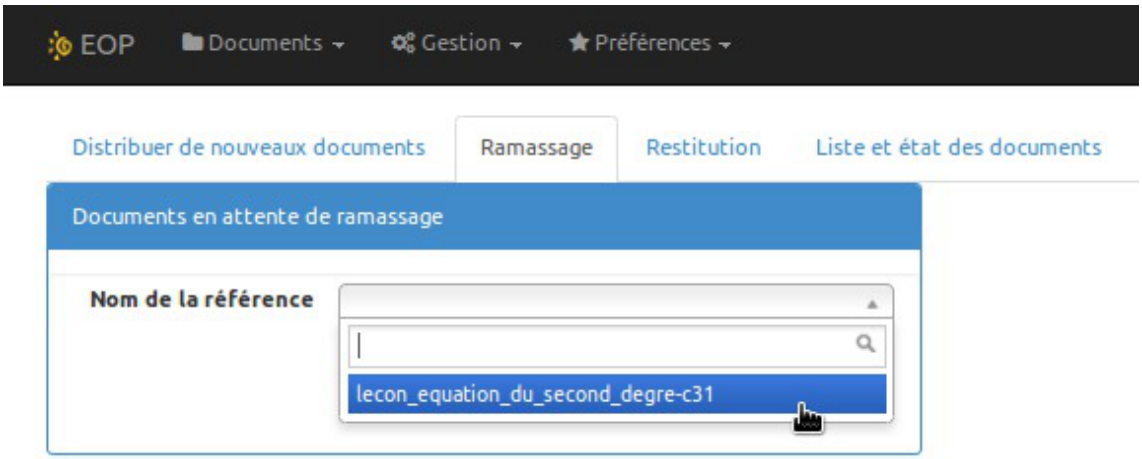
l'acceptation du récapitulatif en cliquant sur le bouton Confirmer.



9.1.3. Gestion des documents

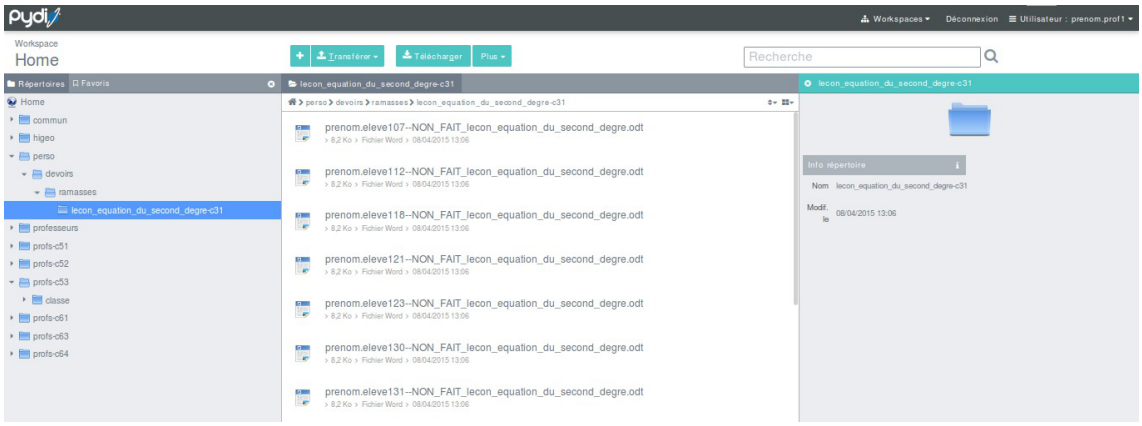
Ramassage

Le ramassage consiste à sélectionner un document qui a été distribué auparavant et à le collecter auprès de chacun des élèves.



Pour se faire il faut se rendre dans l'onglet Documents / Ramassage, sélectionner la référence du document à ramasser et cliquer sur le bouton Ramasser.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

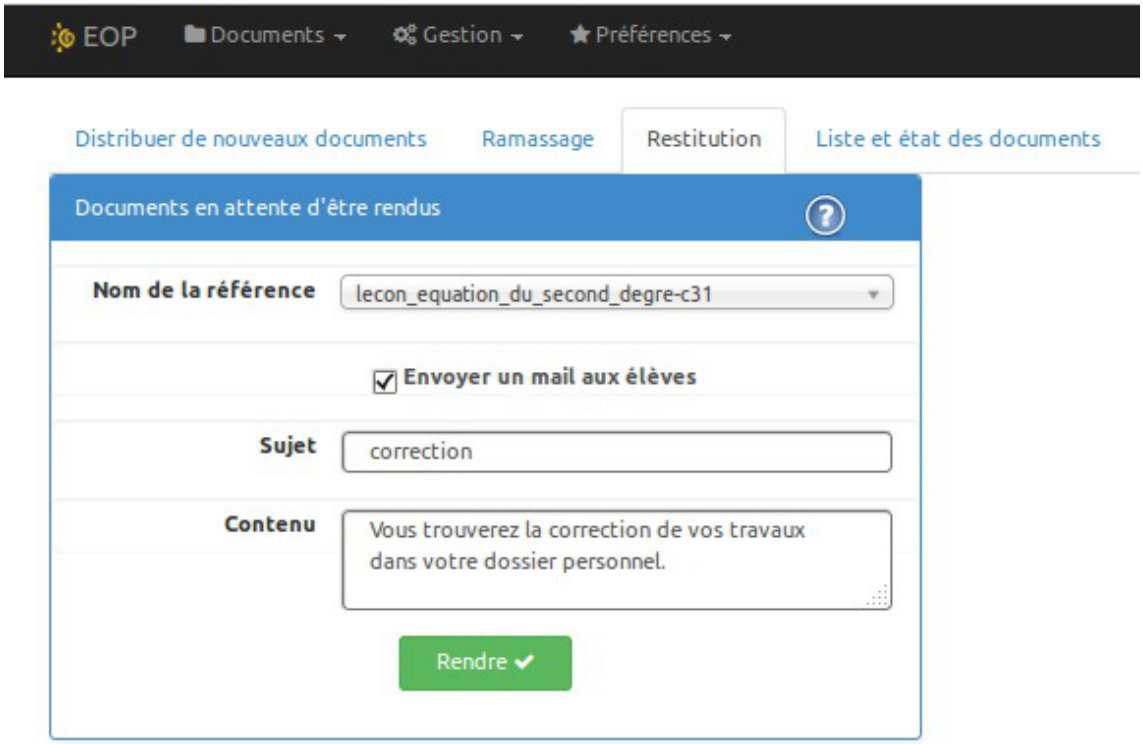


Les documents ainsi collectés sont disponibles dans un répertoire portant le nom de référence concaténé avec le nom de la classe. Ce répertoire se trouve dans le répertoire `/perso/devoirs/ramasses/` de l'enseignant qui a effectué la distribution.

Un message texte qui avertit l'utilisateur que le document a été ramassé est disponible dans le répertoire de l'utilisateur portant le nom de référence concaténé avec le nom de la classe. Ce répertoire se trouve dans le répertoire `/perso/devoirs/nom de l'enseignant/` de l'élève.

Restitution

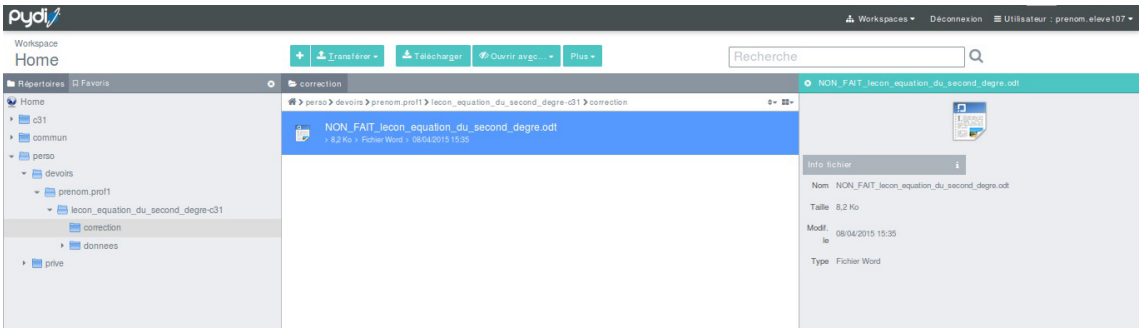
La restitution consiste à sélectionner un document qui a été ramassé auparavant et à le distribuer auprès de chacun des élèves.



Pour se faire il faut se rendre dans l'onglet `Documents` / `Restitution`, sélectionner la référence du

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

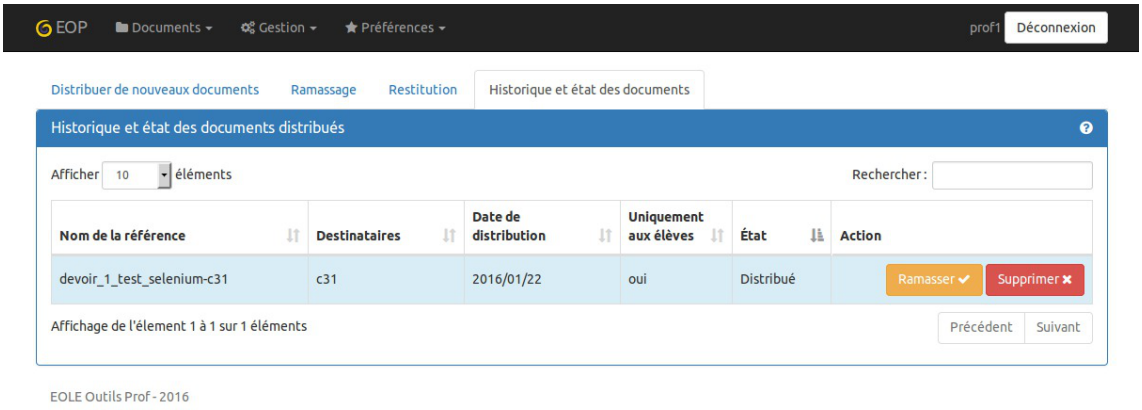
document à restituer. Un message peut accompagner la restitution afin de prévenir l'utilisateur. Pour se faire cocher l'option `Envoyer un mail aux élèves`, saisir le titre et le contenu du courrier électronique. Enfin cliquer sur le bouton `Rendre`.



Les documents restitués sont disponibles dans le répertoire `correction` se trouvant dans le répertoire portant le nom de référence concaténé avec le nom de la classe. Ce répertoire se trouve dans le répertoire `/perso/devoirs/nom de l'enseignant/` de l'élève qui a reçu la restitution.

État des documents

L'onglet État des documents consiste à visualiser les documents et leur état.



Ce tableau récapitulatif reprend tous les documents distribués.

Vous pouvez les trier en cliquant sur les en-têtes de colonnes.

Vous pouvez aussi filtrer le tableau en entrant les premiers caractères du mot souhaité dans le champ de recherche.

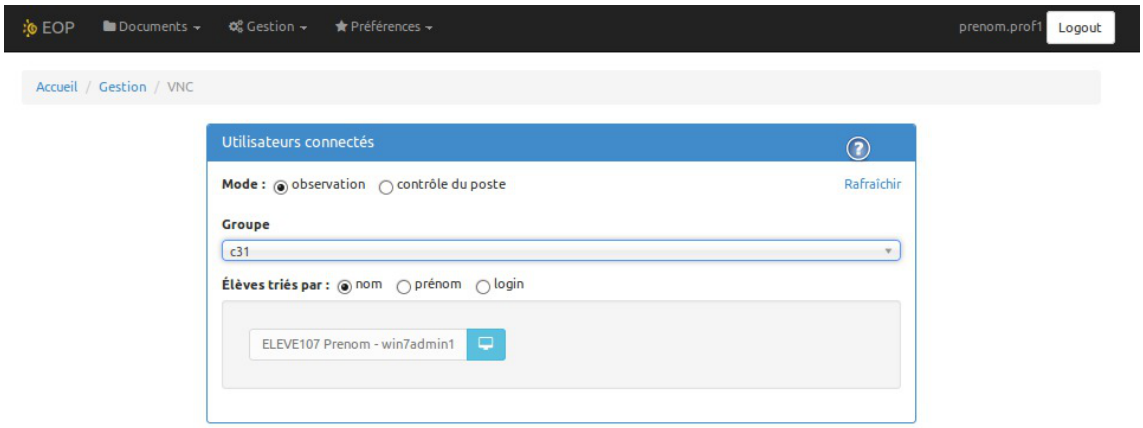
Dans la colonne action les boutons `Rendre`, `Ramasser` et `Supprimer` permettent d'agir sur l'état des documents.

Le bouton `Supprimer` permet d'effacer le cache d'une référence (documents et annexes) qui prend de la place sur le serveur. Attention, une fois le cache supprimé, les élèves ne peuvent plus accéder aux annexes.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

9.1.4. Observation et/ou contrôle à distance

Il est possible d'observer un poste et même de prendre le contrôle sur celui-ci.



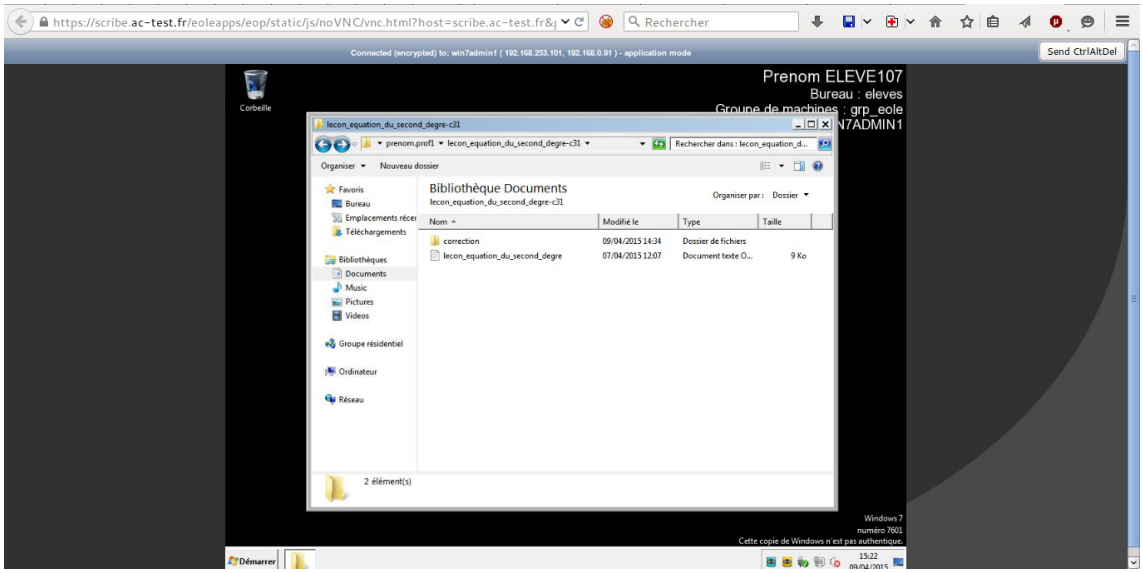
Choisir le mode à utiliser :

- observation ;
- contrôle du poste.

Choisir ensuite le groupe dans la liste.

Le tri des postes peut se faire par le nom, le prénom ou l'identifiant de l'utilisateur.

Cliquer sur l'icône écran du poste désiré. Un nouvel onglet s'ouvre avec la console VNC.



Il faut, à la première utilisation de VNC par l'enseignant, valider un certificat pour l'utilisation du port 6080 en cliquant sur le lien figurant dans l'aide ou en tapant directement dans le navigateur l'adresse suivante : `https://<adresse serveur>:6080`.

9.1.5. Bloquer Internet / Masquer les partages (Mode devoir)

Les professeurs peuvent restreindre l'accès à Internet et/ou aux partages ainsi que monter le partage

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

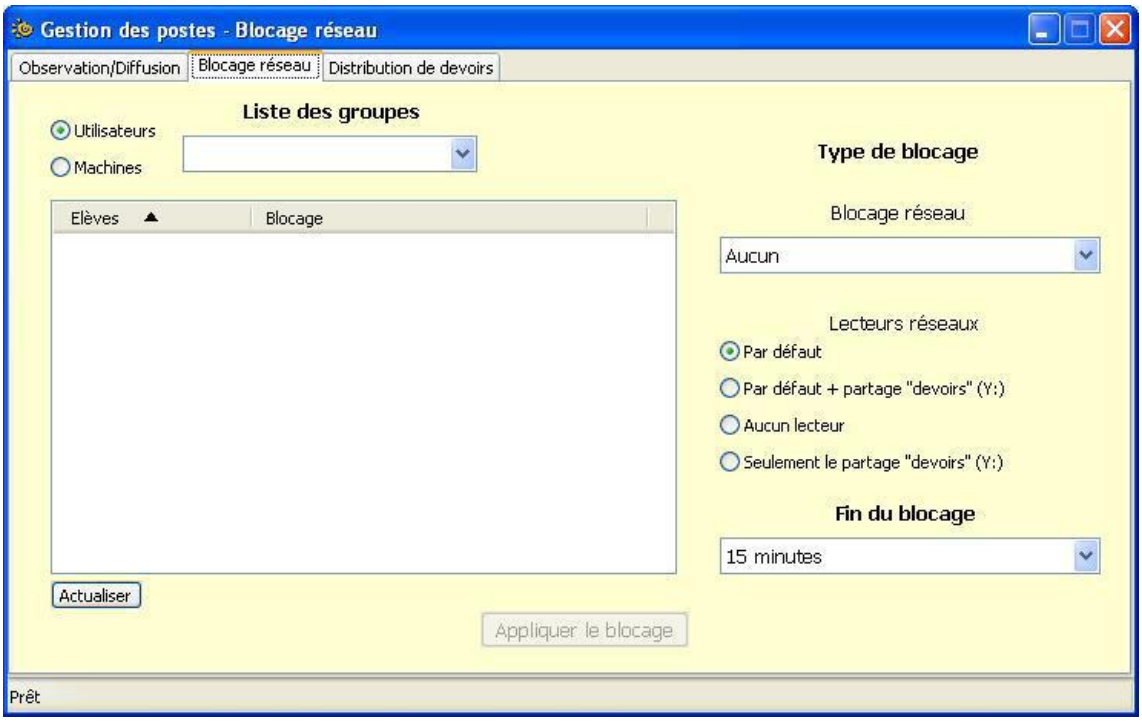
devoir pendant une période donnée.

Ces restrictions sont appliquées immédiatement si l'élève est connecté, sinon elles sont appliquées à l'ouverture de session.

Lorsque la période d'interdiction est écoulée l'environnement de l'élève est automatiquement remis en mode normal s'il est encore connecté.

Le blocage Internet se fait depuis l'application Gestion-postes via la liste déroulante `Type de blocage`.

Le blocage Internet interdit tous les accès réseaux en dehors des services DNS, VNC et du service Samba (ports 137-139 et 445) à destination du module Scribe. Cela afin permettre l'ouverture d'une session sur le domaine et d'accéder aux partages. Aucun accès direct ou par proxy à Internet n'est possible.



Le blocage réseau peut s'appliquer à un utilisateur ou à une machine.

Il est possible de sélectionner plusieurs utilisateurs en même temps en gardant la touche Maj ou Ctrl enfoncée.

En plus du blocage de l'accès à Internet, l'application Gestion-postes permet de masquer les lecteurs réseaux spécifiques au module Scribe pour une durée donnée afin que l'élève n'ait plus accès à son dossier personnel, ni aux dossiers groupes, ni aux dossiers communs (choix `Aucun lecteur réseau`).

Comme pour le blocage de l'accès Internet, le masquage des partages a une durée limitée. À la fin de cette période, si l'élève est encore connecté sur un client, il retrouvera son environnement initial automatiquement.

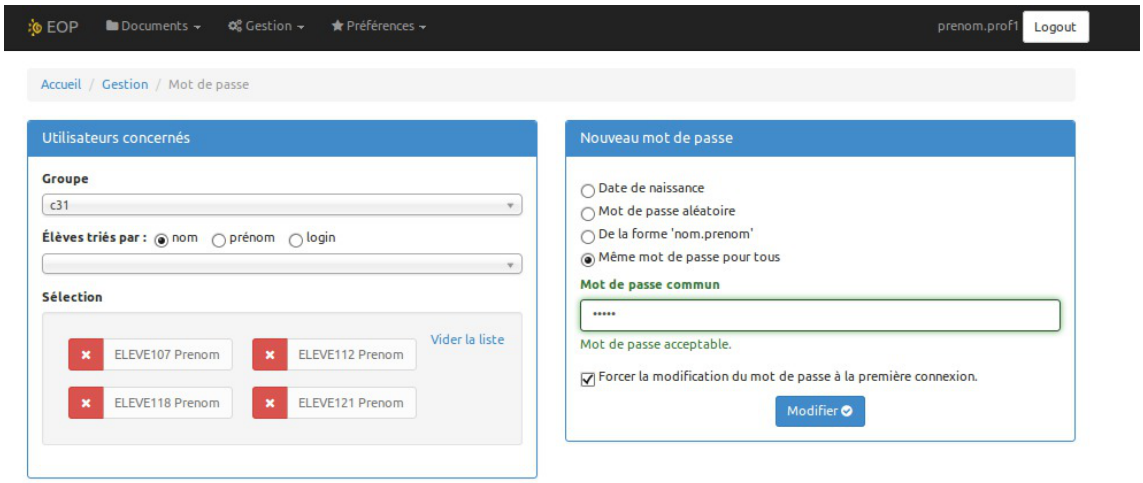
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Voir aussi...

L'application Gestion-postes [p.495]

9.1.6. Changement de mot de passe par lot

Cette fonctionnalité n'est accessible, par défaut, que pour les enseignants identifiés comme étant professeur principal.



Il est possible d'accorder à tous les professeurs le droit de changer le mot de passe de n'importe quel élève. Pour cela, se rendre dans l'interface de configuration du module, en mode expert et dans l'onglet `Applications web`, répondre `oui` à la question `Permettre aux enseignants de changer le mot de passe de tous les élèves`.



Utilisateurs concernés

Choisir un groupe dans la liste des groupes, il est possible de sélectionner tous les élèves du groupe ou de les sélectionner un par un. Pour faciliter la recherche il est possible de trier les élèves par nom, prénom ou identifiant. Les élèves sélectionnés sont ajoutés dans le champ `Sélection`. Une croix blanche sur fond rouge permet de supprimer un compte de la liste. Le lien `Vider la liste` permet de vider toute la liste.

Il faut choisir le type de mot de passe qui sera appliqué aux comptes sélectionnés :

- `Date de naissance` ;
- `Mot de passe aléatoire` : le ou les mots de passe seront affichés à la validation du changement et enregistrés dans le répertoire personnel de l'enseignant sous forme de fichier `.csv` ;
- `De la forme nom.prenom` ;
- `Même mot de passe pour tous` : permet de choisir le mot de passe.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une case à cocher permet d'imposer que le mot de passe par défaut soit changé à la première connexion.

La validation du changement de mot de passe se fait avec le bouton `Modifier`, un message informe du changement :

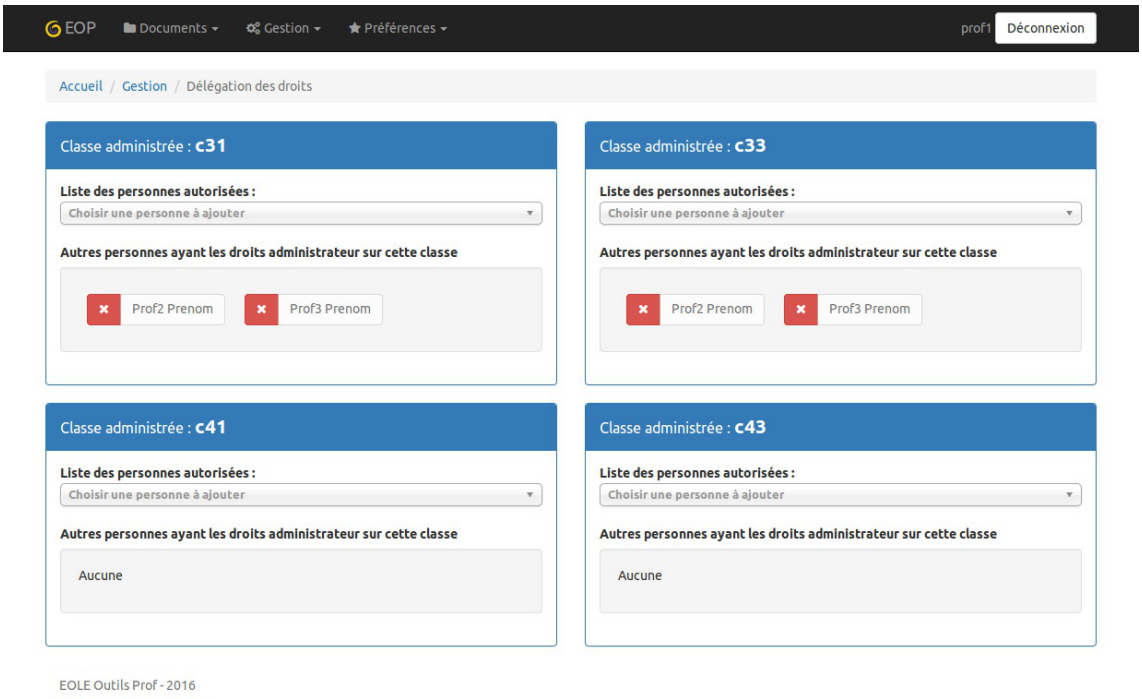
```
Les mots de passe des utilisateurs suivants ont été modifiés avec succès :
ELEVE130 Prenom : 7gUo4*T
Modifications enregistrées dans votre répertoire personnel dans le fichier
mot-de-passe_9_4_0.csv.
```

9.1.7. Délégation de droits

Cette fonctionnalité n'est accessible que pour les enseignants identifiés comme étant professeur principal.

Pour un administrateur de classe, il est possible de déléguer à un autre enseignant le droit de gestion des comptes élève et des mots de passe.

Cette délégation permet de modifier les mots de passe des comptes élèves dans EOP et l'EAD mais permet une gestion plus complète dans l'EAD (inscription à des groupes, fixation de quotas disque…).



La vue affiche toutes les classes dont l'enseignant est responsable. Dans chaque classe est affichée une liste des personnes ayant également un droit de gestion.

Pour déléguer un droit de gestion à un autre enseignant, il faut choisir son nom dans le menu déroulant de la classe désirée. Une fois sélectionné il s'ajoute à la liste des administrateurs sans demande de confirmation.

Pour retirer ce droit à un enseignant, il faut cliquer sur la croix rouge correspondant à son nom. Aucune validation n'est nécessaire.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

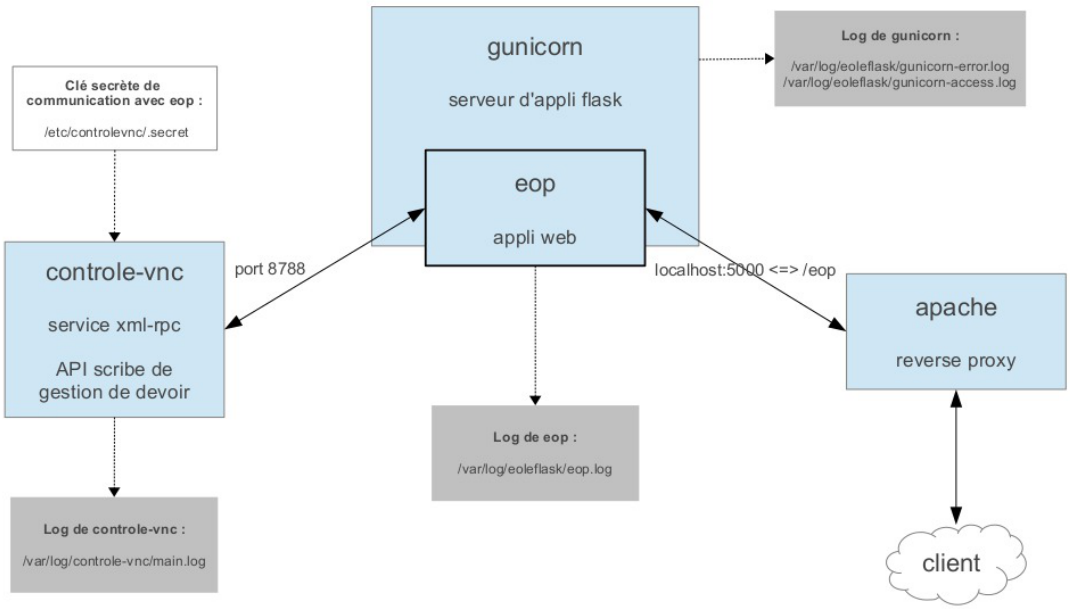
Un enseignant ne peut pas se retirer la qualité de responsable de classe.

9.1.8. Documentation technique

Principales fonctionnalités

- Observation des postes élèves (VNC avec websokify, en cas de problème : cliquer sur le lien dans l'aide et accepter le certificat) ;
- L'authentification est centralisée et gérée par eoleflask-aaa, donc plus de cron pour effacer les fichiers de sessions sur le serveur
- Une section EOP dans le diagnose fait un TCPCheck des ports 8788 de controle-vnc et 6080 de websockify.

EOP est une application `flask` servie par `gunicorn`, dialoguant avec `controle-vnc` grâce à une clé secrète et gérée par apache en reverse-proxy.



En cas de dysfonctionnement il faut vérifier :

- l'état du service `eoleflask` ;
- l'état du service `controle-vnc`.

Si le module est en mode conteneur il faut utiliser les commandes suivantes dans le conteneur web, pour se rendre dans le conteneur web : `# ssh web` .

Vérifier le service eoleflask.

Vérifier les logs dans `/var/log/eoleflask/gunicorn-error.log` et `/var/log/eoleflask/gunicorn-access.log`.

- S'il y a une erreur `NoApplicationError: No application loaded` alors il faut vérifier la présence d'un lien symbolique dans `/etc/eole/flask/enabled/` pointant vers le fichier `/etc/eole/flask/available/eop.conf`.
- S'il y a une erreur `CookieError: Invalid Attribute envole.user` , il faut mettre à jour

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`eole-posh` ou supprimer le cookie `$envole.user`.

Relancer le service :

```
# service eoleflask restart
```

Vérifier le service controle-vnc.

Contrôler les logs dans `/var/log/controle-vnc/main.log`.

Vérifier que le service est bien à l'écoute sur le port 8788 :

```
# netstat -ndtal | grep 8788
```

Et que le port 8788 n'est pas bloqué par le pare-feu (seulement pour le mode conteneur) :

```
# iptables -L | grep 8788
```

S'assurer de la correspondance de la clé secrète contenue dans `/etc/controlevnc/.secret` et la variable `SECRET_KEY` du fichier `/etc/eole/flask/available/eop.conf`.

En mode conteneur, dans le cas d'un module AmonEcole par exemple, le fichier de log `/var/log/controle-vnc/main.log` se trouve dans le conteneur `fichier`.

Vérifier le service apache.

Vérifier que les modules apache pour le proxy inverse sont bien activés :

```
# a2enmod proxy proxy_http
```

```
# service apache restart
```

Tester EOP sans passer par le proxy inverse (de l'extérieur par tunnel SSH) :

```
# ssh -L 9999:127.0.0.1:5000 root@<adresse IP du module>
```

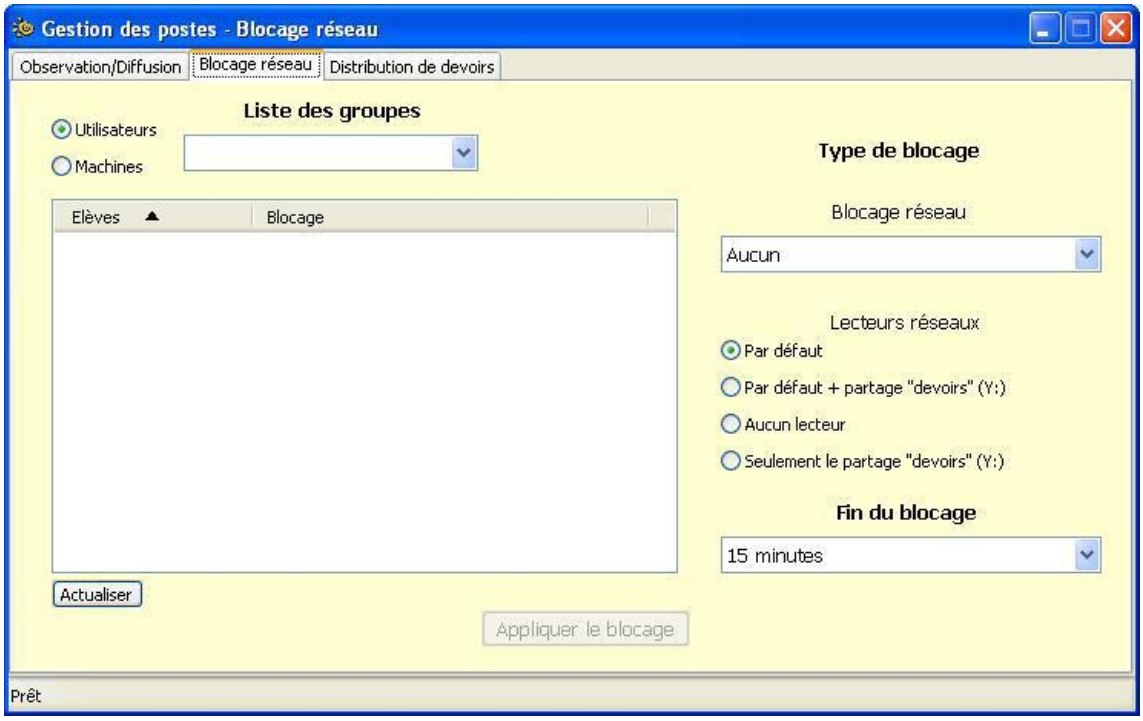
Puis entrer dans un navigateur l'URL : `http://localhost:9999/documents`

Les journaux de l'application EOP sont accessibles dans le fichier `/var/log/eoleflask/eop.log`.

9.2. L'application Gestion-postes

Gestion-postes est une application pour le système d'exploitation Microsoft Windows, accessible uniquement par les enseignants (`P:\Gestion-postes`) qui permet diverses opérations sur une sélection de postes ou d'utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'application propose trois outils accessibles via trois onglets :

- le premier onglet sert à l'observation et la diffusion d'un poste. Il n'est possible d'observer que des élèves, en revanche un professeur peut diffuser son poste sur celui d'un autre professeur. Il est bien entendu indispensable que l'observateur et l'observé soient tous les deux connectés ;
- le second onglet contient le "*mode devoir*" : blocage de l'accès aux partages et/ou à Internet pour des élèves. Il **n**'est **pas** indispensable que les élèves à bloquer soient connectés. Le blocage s'appliquera dès leur ouverture de session ;
- le troisième onglet permet de distribuer des documents. Ces documents peuvent être distribués à tous les groupes (niveau, classe, équipe pédagogique, matière, groupe...) et peuvent être accompagnés de données en lecture seule qui ont l'avantage de ne pas être dupliquées sur le serveur.



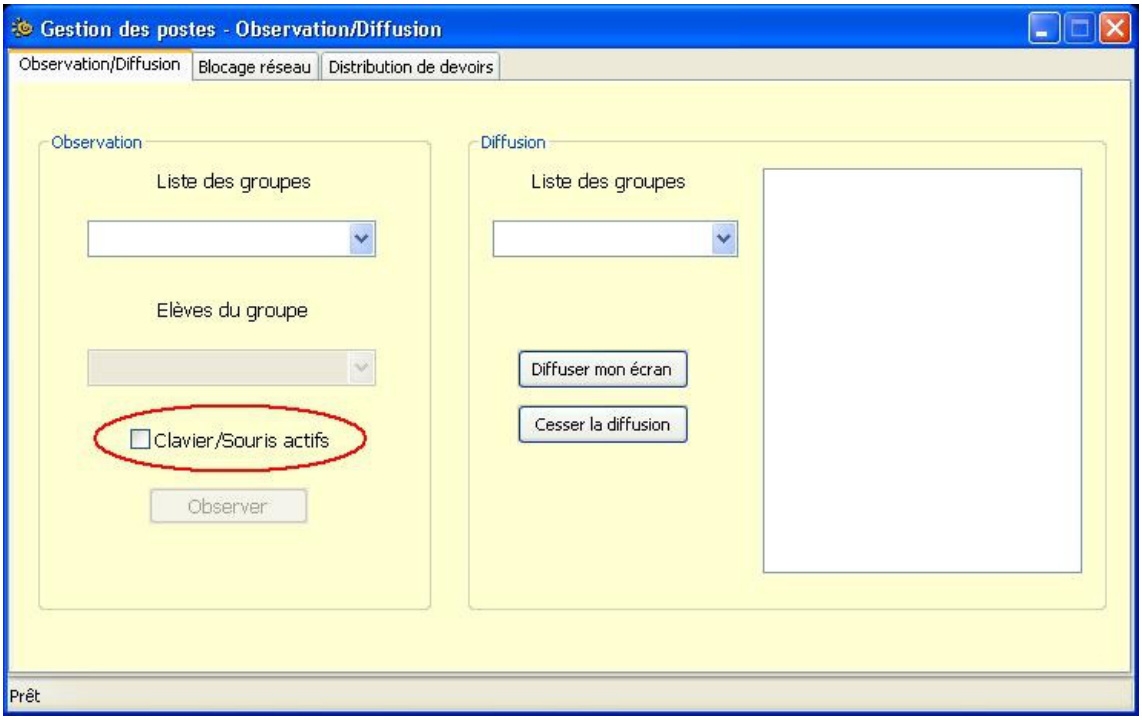
Il n'existe pas d'équivalent pour des clients GNU Linux. Par contre, l'application EOP est accessible au travers d'un navigateur web.

9.2.1. Observation / Diffusion du poste

Observation

L'observation consiste à afficher le poste d'un élève dans une fenêtre sur le poste du professeur. La sélection d'un élève à observer se fait par classe ou par groupe, seuls les élèves connectés sont listés.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Observation, activation de la prise en main du poste (clavier et souris de l'observateur actifs)

La liste des élèves connectés affiche l'identifiant de l'élève et le nom de la machine sur laquelle il est connecté.



Une fois l'élève sélectionné, cliquer sur Observer. La requête est transmise au serveur et à la station de l'élève ce qui peut prendre quelques instants.

L'application permet d'observer plusieurs élèves en même temps, cependant le nombre dépend de la qualité et de la vitesse du réseau.

Le niveau d'observation VNC[p.904] est paramétrable dans l'EAD : Outil / VNC.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Trois niveaux d'observation :

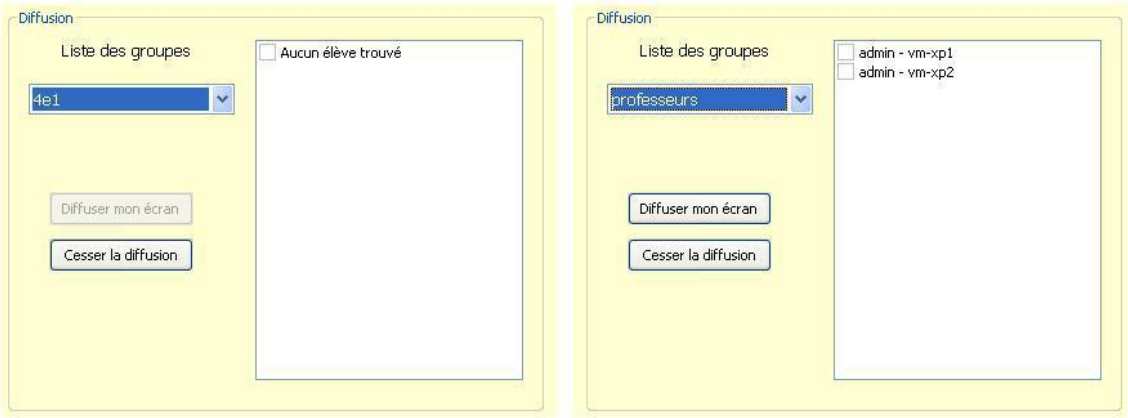
- Désactivé ;
- Visualisation simple ;
- Visualisation et contrôle.

En mode *Visualisation et contrôle*, l'utilisateur pourra choisir via la coche *Clavier/Souris actifs* s'il veut pouvoir prendre la main sur la station élève.

Une ré-ouverture de session sur le poste client est nécessaire afin de prendre le changement du mode de contrôle de VNC en compte.

Diffusion

La diffusion est l'affichage du poste du professeur sur un ou plusieurs postes élève et/ou professeur. La sélection se fait par classe, par groupe ou par membre du groupe *professeurs*. Comme pour l'observation, seuls les utilisateurs connectés sont listés.



Le bouton Cesser la diffusion arrête la diffusion immédiatement sur tous les postes.

Toute nouvelle diffusion (nouveau clic sur le bouton Diffuser mon écran) **interrompra** la diffusion précédente.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La qualité du réseau influe directement sur le nombre maximum de diffusions simultanées possibles.

9.2.2. Bloquer Internet / Masquer les partages (Mode devoir)

Les professeurs peuvent restreindre l'accès à Internet et/ou aux partages ainsi que monter le partage *devoir* pendant une période donnée.

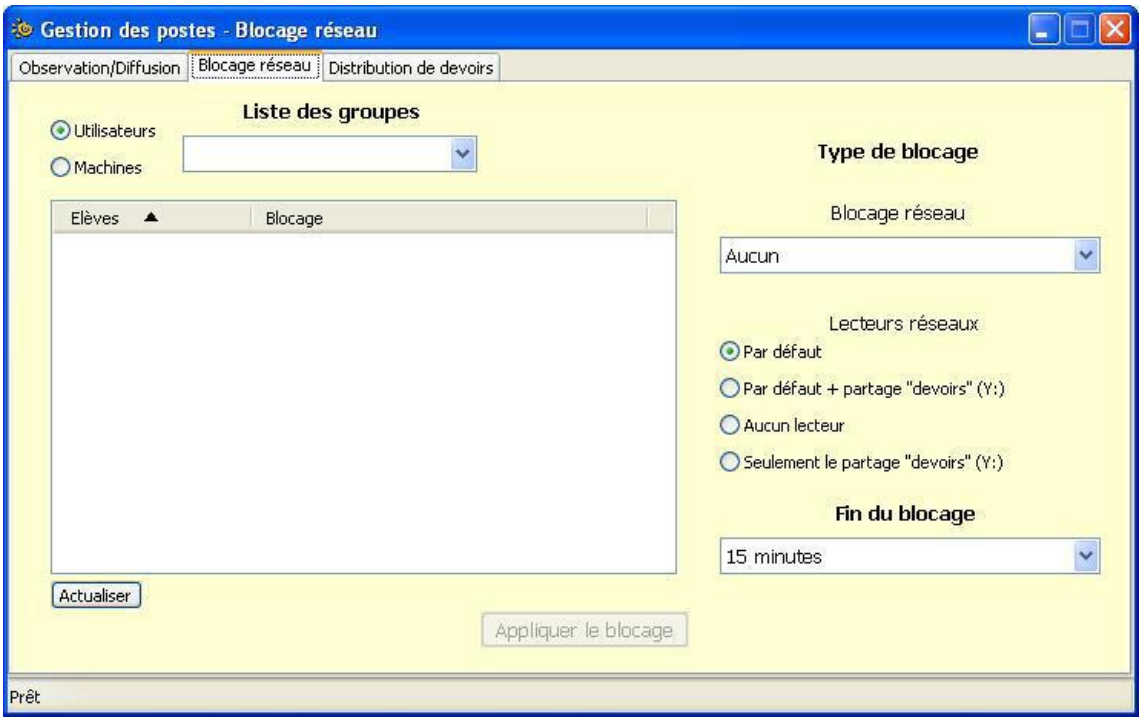
Ces restrictions sont appliquées immédiatement si l'élève est connecté, sinon elles sont appliquées à l'ouverture de session.

Lorsque la période d'interdiction est écoulée l'environnement de l'élève est automatiquement remis en mode normal s'il est encore connecté.

Blocage Internet

La sélection du blocage Internet se fait via la liste déroulante `Type de blocage`.

Le blocage Internet interdit tous les accès réseau en dehors des services DNS, VNC et du service Samba (ports 137-139 et 445) à destination du module Scribe. Cela afin de permettre l'ouverture d'une session sur le domaine et d'accéder aux partages. Aucun accès à internet, direct ou par proxy, n'est possible.



Le blocage réseau peut s'appliquer à un utilisateur ou à une machine.

Il est possible de sélectionner plusieurs utilisateurs en même temps en gardant la touche Maj ou Ctrl enfoncée.

Masquer les lecteurs réseaux

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En plus du blocage de l'accès à Internet, l'application permet de masquer les lecteurs réseau spécifiques au module Scribe pour une durée donnée afin que l'élève n'ait plus accès à son dossier personnel ni aux dossiers groupes et dossiers communs (choix `Aucun lecteur réseau`).

Les documents sont distribués dans le dossier "devoirs" situé sur le serveur. Il est accessible en chemin UNC [p.904] par `\\<adresse_du_serveur>\<login_utilisateur>\devoirs`

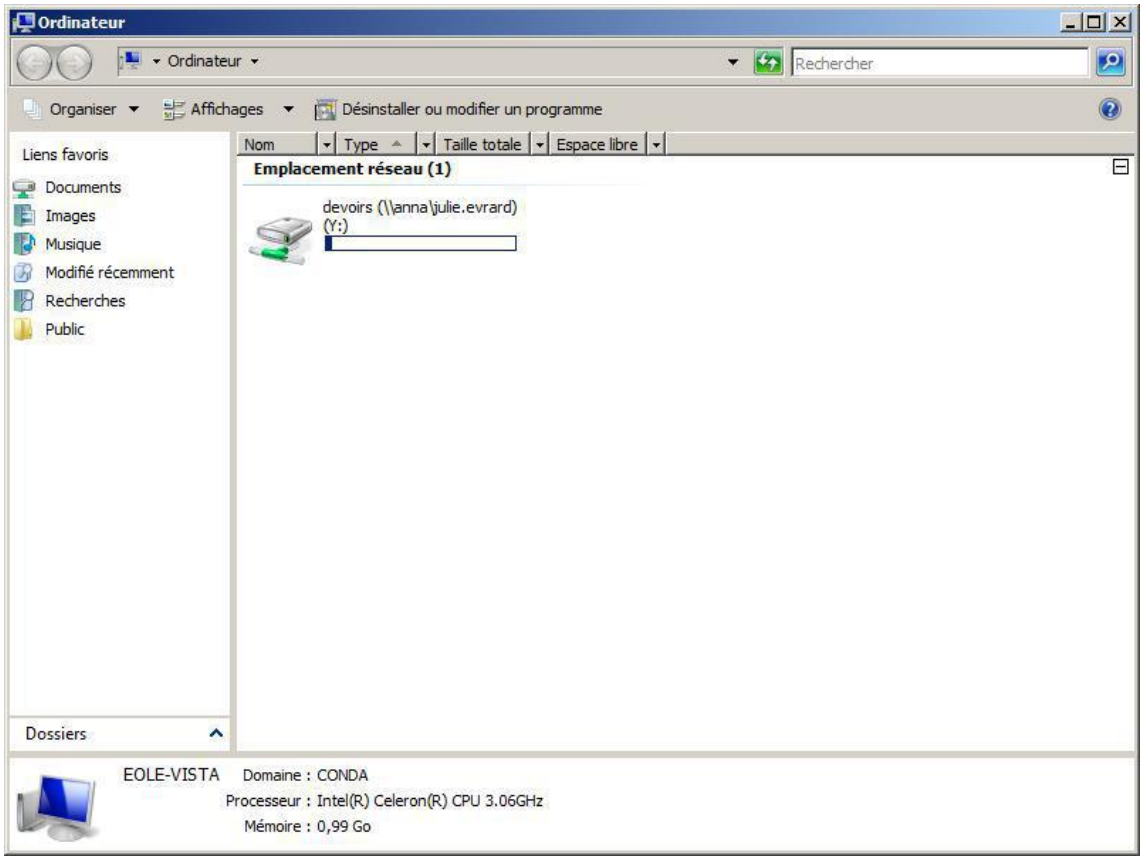
L'application propose de monter ce dossier comme nouveau lecteur nommé `Y:`

Sélectionner le bouton radio `Seulement le partage "devoirs"` masquera tous les lecteurs puis connectera le dossier "devoirs" de l'utilisateur au lecteur `Y:` dans le poste de travail.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur et l'empêche de diffuser ou de récupérer le ou les documents. Aucun utilisateur ne peut donc prendre connaissance des documents à l'avance.

Pour masquer tous les lecteurs et connecter le dossier "devoirs" de l'utilisateur au lecteur `Y:` il faut sélectionner le bouton radio `Seulement le partage "devoirs"`.

Associé au blocage réseau, ce choix permet d'isoler l'utilisateur. Cela l'empêchera de récupérer et de diffuser le devoir vers d'autres utilisateurs.



Comme pour le blocage de l'accès Internet, le masquage des partages a une durée limitée. À la fin de cette période, si l'élève est encore connecté sur un client, il retrouvera son environnement initial automatiquement.

Gestion-postes offre la possibilité de spécifier une liste de lecteurs à afficher même si l'un des choix `Aucun lecteur` ou `Seulement le partage "devoirs"` a été fait. Pour ce faire il faut placer un fichier nommé `lecteurs.txt` dans `P:\gestion-postes\`

Le fichier doit contenir une liste de lettres de lecteur à afficher sans les deux points ":" et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> séparées par des virgules ",".
> Exemple de contenu du fichier `lecteurs.txt` :
> `c,d,s`

9.2.3. Distribution de devoirs

La distribution peut être composée de deux éléments :

- le ou les documents sous forme d'un ou plusieurs fichiers. Ils seront copiés dans chacun des dossiers personnels `devoirs`/ `nom_de_l'enseignant` / `<nom_du_devoir>` des utilisateurs du groupe sélectionné. Les utilisateurs auront un accès en lecture et en écriture à ces fichiers (modification/suppression) ;
- les données jointes au(x) document(s) qui sont des fichiers supplémentaires dont la modification est impossible. Ils sont copiés une seule fois à un endroit spécifique du serveur. Des liens symbolique vers ces fichiers sont créés dans le sous-répertoire `donnees` du répertoire `devoirs`/ `nom_de_l'enseignant` / `nom_devoir` de chacun des utilisateurs.

Si la distribution de document est un travail éducatif, la distribution s'effectue en suivant les 4 étapes suivantes :

- distribuer ;
- ramasser ;
- rendre : distribution des devoirs corrigés ;
- supprimer : effacement des fichiers du devoir.

Distribuer

La distribution de document commence par la sélection d'un ou plusieurs fichiers dans `Devoir à distribuer`. L'ajout de fichiers dans `Donnée` est facultatif, ces fichiers supplémentaires accompagneront le devoir mais leur modification sera impossible.

Il faut nommer le devoir dans le champ `Nom du devoir` , c'est sous ce nom qu'il apparaîtra pour l'utilisateur et pour le gérer (ramassage).

Ensuite il faut sélectionner le groupe auquel le devoir doit être distribué. Tous les groupes sont présents dans la liste, y compris les groupes incluant des utilisateurs *professeurs*.

La case `Uniquement aux élèves du groupe` est cochée par défaut. Décochée, elle permet d'envoyer les documents aux autres membres du groupe, comme par exemple aux enseignants.

Par défaut, l'option `Dans le dossier 'perso\devoirs'` étant sélectionnée, les documents seront distribués dans le répertoire personnel des utilisateurs.

L'option `Dans le partage 'devoirs' (non accessible par défaut)` permet de préparer la distribution différée de documents. Ce travail de préparation peut donc se faire aussi bien à l'extérieur qu'à l'intérieur de l'établissement. La distribution ne sera effective qu'au travers du logiciel `Gestion-postes`.

Cliquer sur `Distribuer`, une boite de dialogue affiche le nombre de devoirs prêts à être distribués et demande confirmation.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Lorsque la distribution est terminée, un message affiche le nombre de documents effectivement distribués et le nom du répertoire de stockage. Ce nom est automatiquement associé au devoir, il correspond à <identifiant_du_distributeur>-<numéro_devoir>. Ce sous-dossier est présent dans le répertoire "devoirs" de l'utilisateur. Il contient l'ensemble des documents et des liens vers les données.



L'opération peut prendre du temps dans le cas de fichiers volumineux et de nombreux membres dans le groupe cible.

Veillez à ne pas fermer l'application pendant la distribution.

N'étant copiées qu'une fois puis liées dans les dossiers "devoirs", les données ont l'avantage d'économiser de l'espace disque sur le serveur.

Ramasser

Sélectionner le devoir à ramasser. Dans la liste déroulante, le nom du groupe auquel a été distribué le devoir est affiché à côté du nom du devoir.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

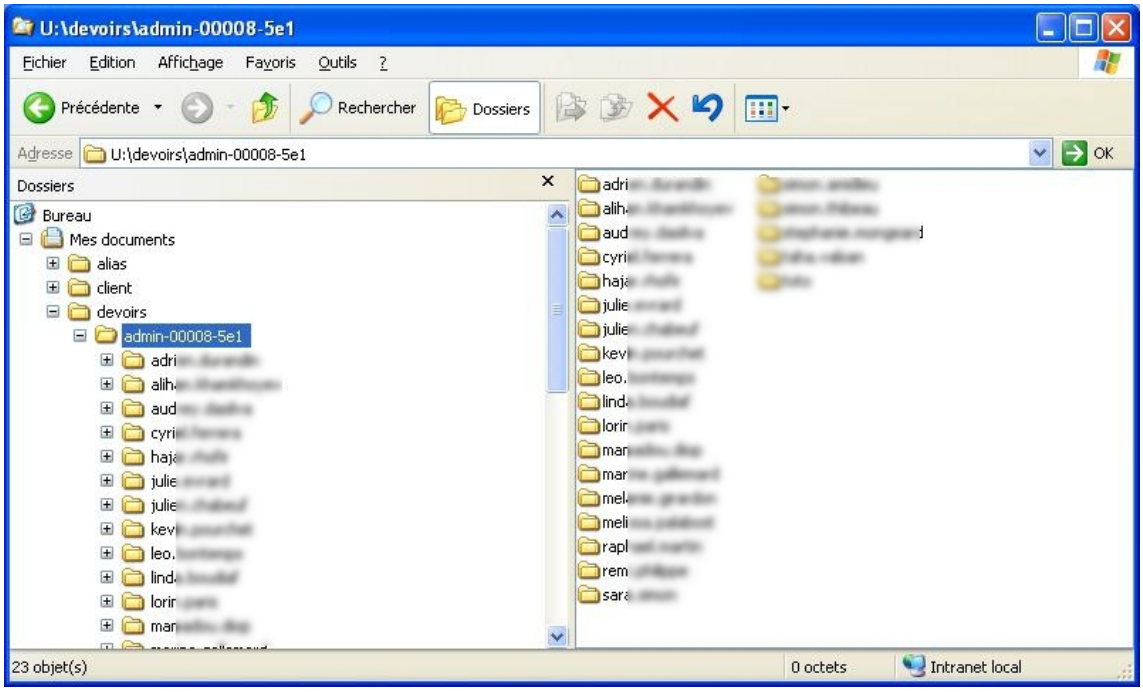


À la fin du ramassage, un message rend compte de l'opération. Si un élève a supprimé le dossier du devoir, celui-ci ne pourra pas être ramassé, un répertoire du nom de l'élève sera quand même créé mais sera vide.



L'action ramassage des devoirs effectue une copie des fichiers du devoir (sans les données) dans le répertoire "devoirs" du dossier personnel de celui qui exécute le ramassage et prend la forme `U:\devoirs\<nom_devoir>-<groupe_cible>\<identifiant_de_l'élève>\`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Lors du ramassage d'un devoir, tous les fichiers et dossiers contenus dans `U:\devoirs\<nom_devoir>\` (sauf le répertoire `donnees`) sont recopiés. Il est donc possible de donner comme devoir la création d'un nouveau fichier.

Rendre les copies corrigées

Tout comme sur une version papier, la correction peut s'effectuer sur la copie en éditant directement le fichier mais elle peut aussi bien se faire sous forme d'ajout de fichier. En effet, c'est tout le dossier qui sera copié dans le répertoire personnel de l'élève lors de la restitution de la correction. La restitution se fait dans le répertoire personnel des utilisateurs à savoir `U:\devoirs\<nom_devoir>\correction\`

Une boîte de dialogue informe du résultat de l'opération.

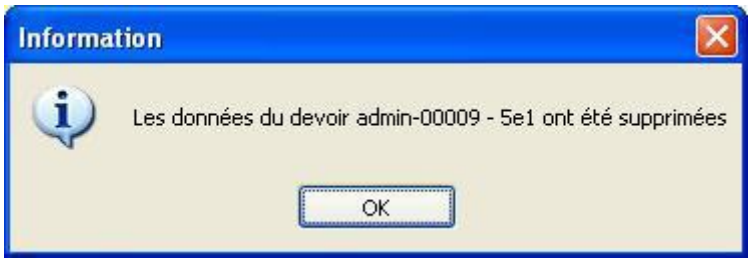


Suppression des données

Lorsqu'un enseignant distribue des données en plus des documents, elles sont copiées dans `U:\devoirs\.distribues` et des liens vers ces fichiers sont ensuite créés dans le répertoire `nom_du_devoir` \ `donnes` de chacun des destinataires.

Il est possible de supprimer ces fichiers lorsqu'ils sont devenus inutiles.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- La suppression des données entraînera également la suppression du dossier `<nom_du_devoir>` \ `donnees` dans le dossier des destinataires.
- Cette fonctionnalité permet de supprimer les données liées à une distribution de document qui ne seraient plus utiles par la suite. Elle permet donc d'économiser de la place sur le serveur de stockage.

9.3. Distribution de documents dans l'EAD

L'EAD offre la possibilité aux enseignants de distribuer des documents et des travaux éducatifs (évaluation, bilan, contrôle ou devoir contrôlé).

Les fonctionnalités sont équivalentes à celles disponibles dans le logiciel `Gestion-postes` mais contrairement à celui-ci, qui n'est accessible que depuis les clients Windows de l'établissement, elles sont disponibles à travers le portail Envole et donc accessibles depuis l'extérieur de l'établissement.



Vue de la distribution de document dans l'EAD

La distribution de documents au travers de l'EAD permet de faire une distribution immédiate ou différée des documents. Dans le cas d'une distribution différée (voir Choix du répertoire de destination), les documents sont préparés avec l'EAD et leur accès sera activé au moment opportun avec `Gestion-Postes`.

La distribution peut être composée de deux éléments :

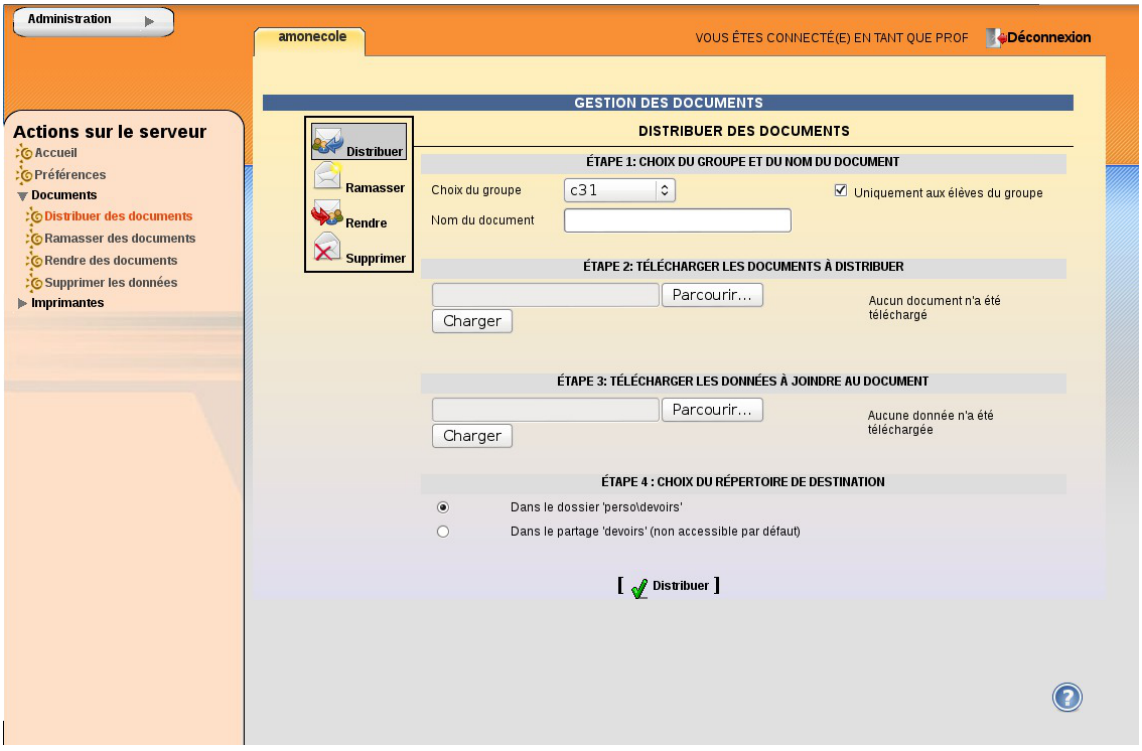
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le ou les documents sous forme d'un ou plusieurs fichiers. Ils seront copiés dans chacun des dossiers personnels `devoirs` / `nom_de_l'enseignant` / `<nom_du_devoir>` des utilisateurs du groupe sélectionné. Les utilisateurs auront un accès en lecture et en écriture à ces fichiers (modification/suppression) ;
- les données jointes au(x) document(s) qui sont des fichiers supplémentaires dont la modification est impossible. Ils sont copiés une seule fois à un endroit spécifique du serveur. Des liens symbolique vers ces fichiers sont créés dans le sous-répertoire `donnees` du répertoire `devoirs` / `nom_de_l'enseignant` / `nom_devoir` de chacun des utilisateurs.

Si la distribution de document est un travail éducatif, la distribution s'effectue en suivant les 4 étapes suivantes :

- distribuer ;
- ramasser ;
- rendre : distribution des devoirs corrigés ;
- supprimer : effacement des fichiers du devoir.

9.3.1. Distribuer des documents



Vue de l'étape 1 : Distribuer

Étape 1 : Choix du groupe et du nom du document

Il faut avant tout choisir, dans le menu déroulant `Choix du groupe`, la classe, la matière ou l'équipe à qui l'ont veut distribuer un ou plusieurs documents. Puis on choisit un nom `Nom du document` pour l'espace de travail. Il apparaîtra dans le répertoire personnel de chacun des utilisateurs sous la forme `devoirs` / `nom_de_l'enseignant` / `<espace_de_travail>` et contiendra les documents de travail et les données.

Le nom du document ne doit comporter ni espace ni caractère accentué.

La case `Uniquement aux élèves du groupe` est cochée par défaut. Décochée, elle permet

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

d'envoyer les documents aux autres membres du groupe, comme par exemple aux enseignants.

Étape 2 : Télécharger les documents à distribuer

Le bouton `Parcourir` permet de choisir un document sur son ordinateur. Après avoir cliqué sur le bouton `Charger`, le document apparaît dans la liste de droite. Il est possible de répéter l'opération pour autant de fichiers que l'on souhaite distribuer.

Étape 3 : Télécharger les données à joindre au document

Le bouton `Parcourir` permet de choisir un document sur son ordinateur. Après avoir cliqué sur le bouton `Charger`, le document apparaît dans la liste de droite. Il est possible de répéter l'opération pour autant de fichiers que l'on souhaite distribuer. Cette étape n'est pas obligatoire.

Étape 4 : Choix du répertoire de destination

Par défaut, l'option `Dans le dossier 'perso\devoirs'` étant sélectionnée, les documents seront distribués dans le répertoire personnel des utilisateurs.

L'option `Dans le partage 'devoirs' (non accessible par défaut)` permet de préparer la distribution différée de documents. Ce travail de préparation peut donc se faire aussi bien à l'extérieur qu'à l'intérieur de l'établissement. La distribution ne sera effective qu'au travers du logiciel `Gestion-postes`.

Dernière étape : Distribuer

Valider le bouton `Distribuer` pour que la distribution soit effective.



Il est possible de distribuer les mêmes documents à plusieurs groupes :

Étape 1 : Choix du groupe et du nom du document

Il faut choisir un autre groupe dans le menu déroulant et obligatoirement changer le nom de l'espace de travail `Nom du document`.

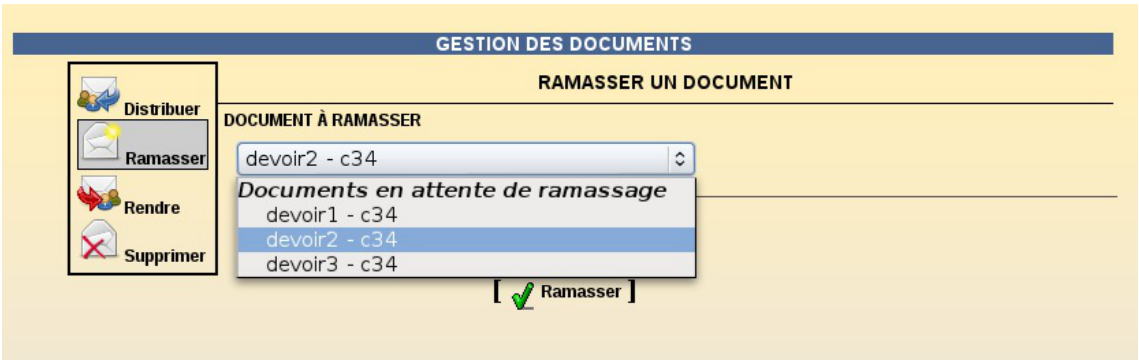
Étape 2 : Télécharger les documents à distribuer

S'il n'y a qu'un document, son chemin est encore dans le champ parcourir. Il suffit alors de cliquer sur le bouton `Charger`. À défaut, il faut recharger les différents documents à distribuer.

Étape 3 : Télécharger les données à joindre au document

S'il n'y a qu'une donnée, son chemin est encore dans le champ parcourir, il suffit de cliquer sur le bouton `Charger`. À défaut, il faut recharger les différentes données à distribuer.

9.3.2. Ramasser des documents

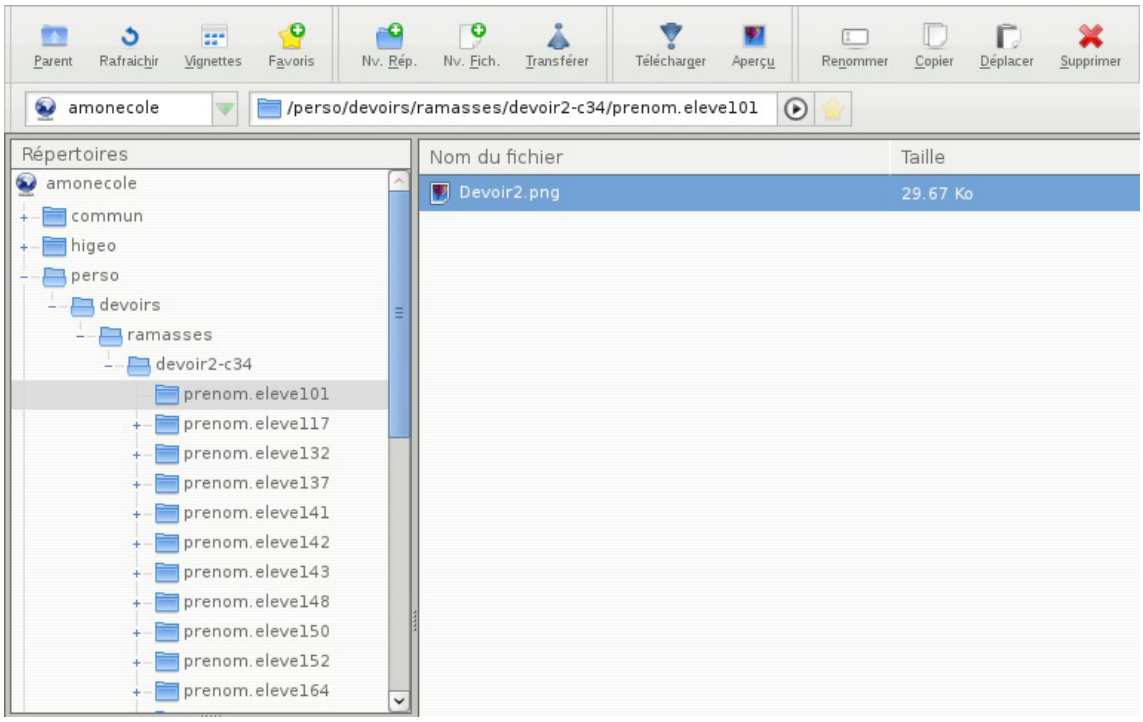


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette fonctionnalité permet de ramasser les travaux des utilisateurs.

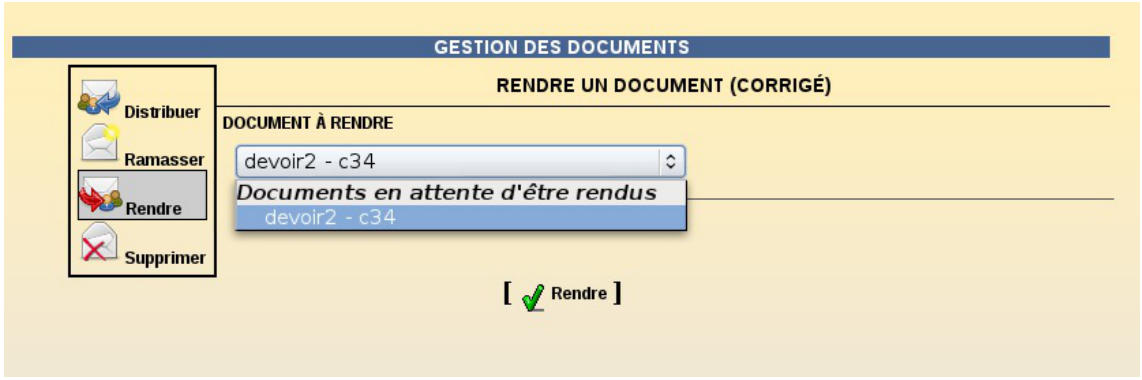
Les documents ramassés se retrouvent dans l'arborescence du dossier personnel de l'utilisateur les ayant ramassés :

… / perso / devoirs / ramasses / Nom de l'espace de travail (Nom du document) / Identifiant des élèves /



Vue des documents ramassés dans Ajaxplorer

9.3.3. Rendre des documents



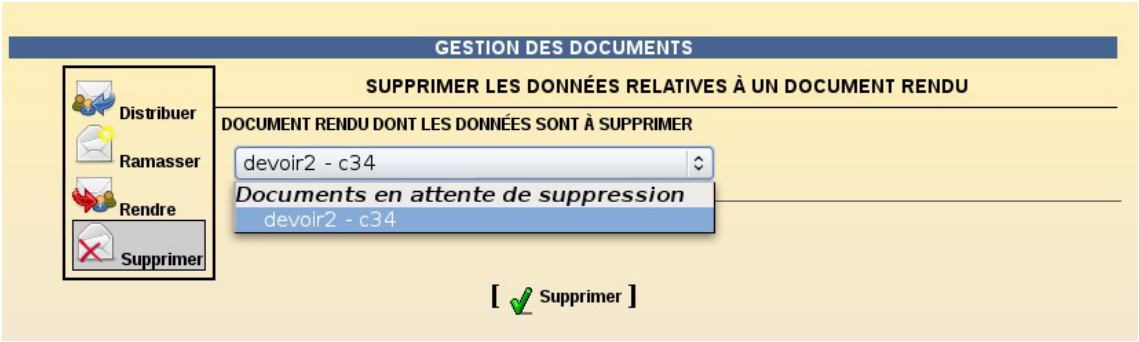
Cette fonctionnalité permet de rendre le travail corrigé. Un document ne peut être rendu que s'il a été auparavant ramassé.

9.3.4. Supprimer les données

Lorsqu'un enseignant distribue des données en plus des documents, elles sont copiées dans U:\devoirs\.distribues et des liens vers ces fichiers sont ensuite créés dans le répertoire nom_du_devoir \ donnes de chacun des destinataires.

Il est possible de supprimer ces fichiers lorsqu'ils sont devenus inutiles.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- La suppression des données entraînera également la suppression du dossier <nom_du_devoir> \ donnees dans le dossier des destinataires.
- Cette fonctionnalité permet de supprimer les données liées à une distribution de document qui ne seraient plus utiles par la suite. Elle permet donc d'économiser de la place sur le serveur de stockage.

Voir aussi...

L'application Gestion-postes [p.495]

10. Les sauvegardes

10.1. Généralités sur la sauvegarde

La sauvegarde[p.901] 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.899] :

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

10.1.1. 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.

10.1.2. 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 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.

10.1.3. 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.

10.1.4. 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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
  - http://www.arkeia.com/products/arkeianetworkbackup/index.php
- **Bacula** - Bacula
  - http://bacula.org
- **Bareos** - Bareos
  - http://www.bareos.org

10.2. 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.898]
- les ACLs[p.882]

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

10.2.1. 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.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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, 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.

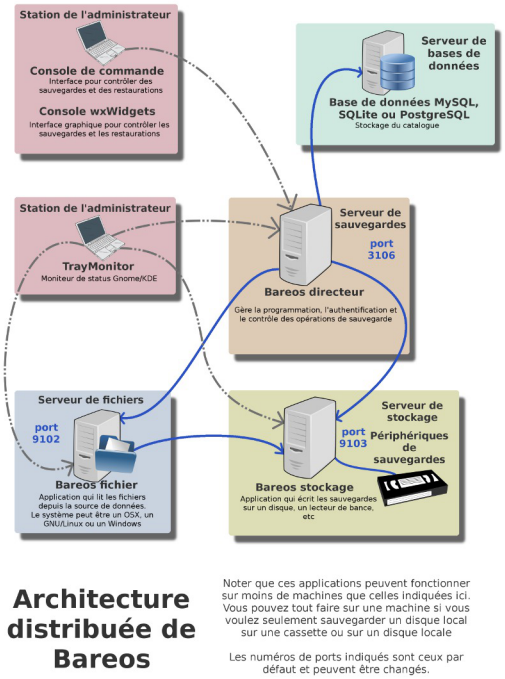
Bareos lit les fichiers de configuration au démarrage, et inscrit les valeurs dans la base de données du Catalogue. C'est le Catalogue qui définit la configuration utilisée par Bareos, donc il faut préférer le résultat des commandes console aux valeurs des fichiers.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1150008.9

10.2.2. Architecture de Bareos

Bareos est construit suivant une **architecture distribuée** :



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** ;

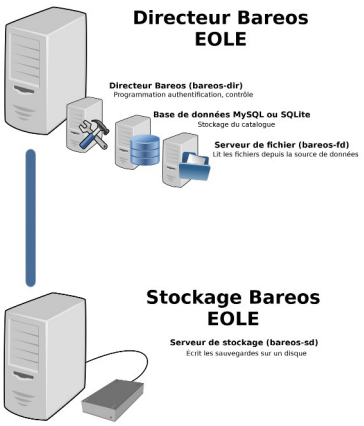
La communication entre chaque serveur est associée à un mot de passe. Ces différents serveurs peuvent être :

- 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*.

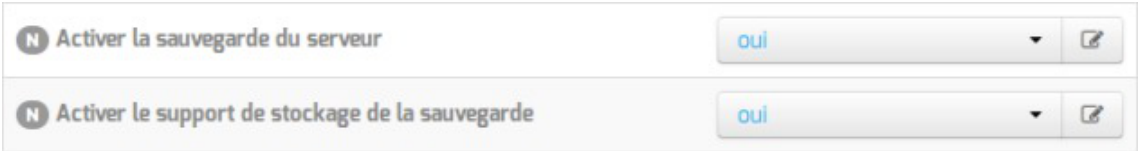
10.2.3. Configuration des sauvegardes

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.

10.2.3.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

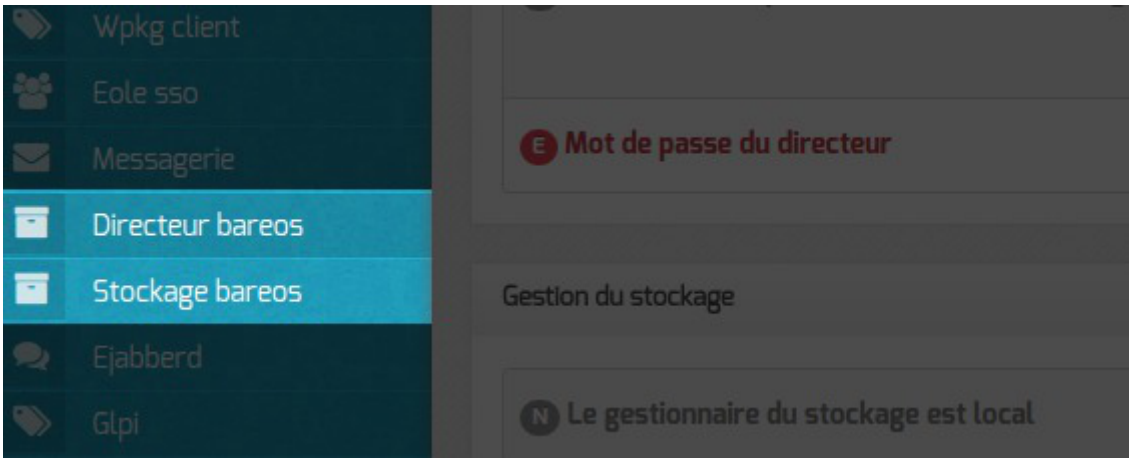
- L'activation du support de stockage de la sauvegarde permet d'accueillir des sauvegardes locales ou

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.

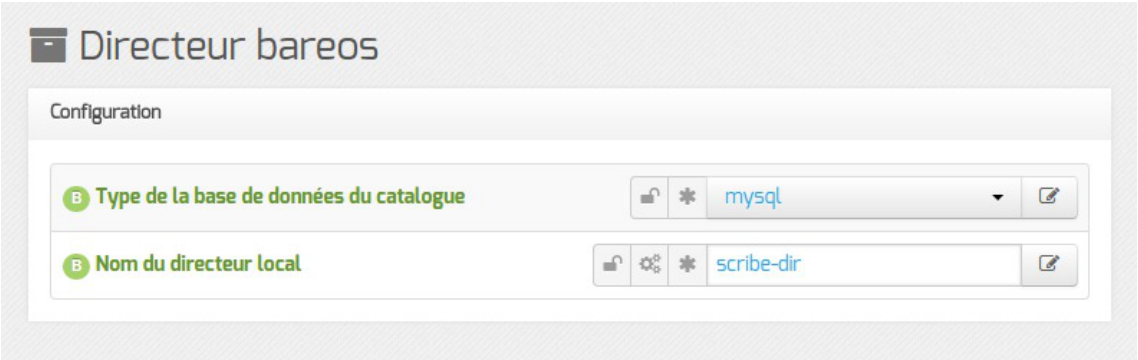


Si le support de stockage de la sauvegarde est activé (`Activer le support de stockage de la sauvegarde` à `oui`) un onglet `Stockage bareos` apparaît dans l'interface de configuration du module.

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.

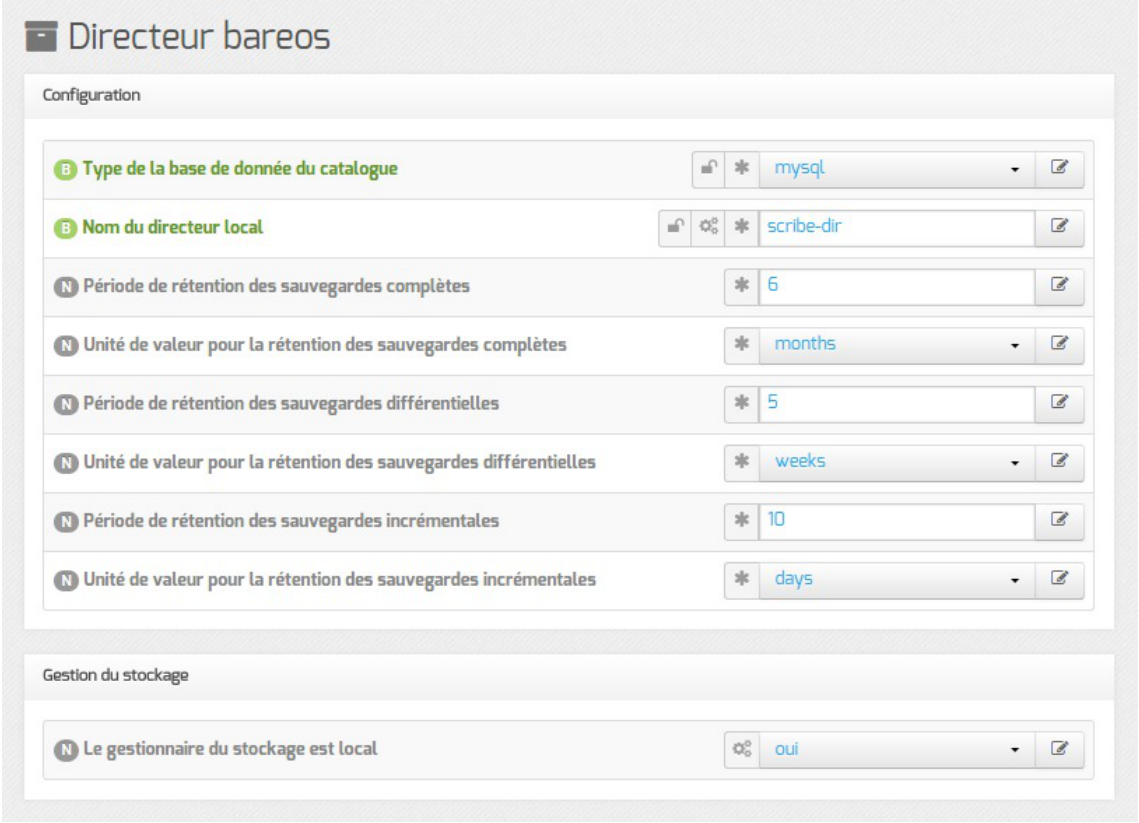
Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web `bareos-webui` nécessite MySQL.

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.888] 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

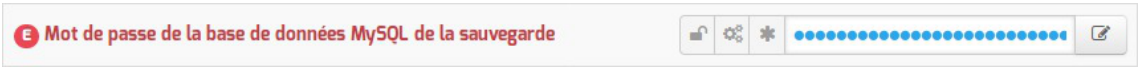
Dans le cas d'un serveur distant (`Activer le serveur de stockage localement` à `non`), il faut configurer l'adresse IP et le mot de passe du serveur de stockage distant.

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.

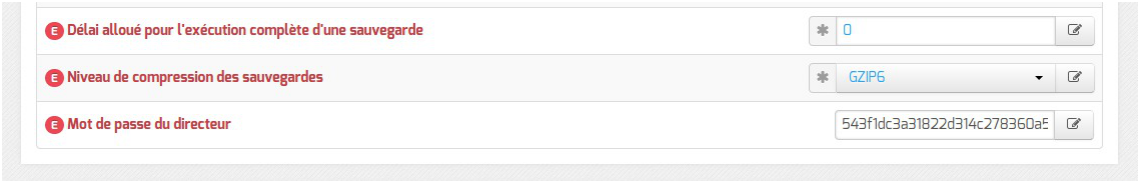
Le déport du service `bareos-sd` sur un autre serveur que `bareos-dir` ne permet pas de gérer correctement les verrous des tâches d'administration sur ce serveur : `bareos-dir` ne permet pas de signaler efficacement à `bareos-sd` qu'une sauvegarde est lancée et qu'il doit poser un verrou empêchant les autres tâches d'administration.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En mode expert, il est possible de 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



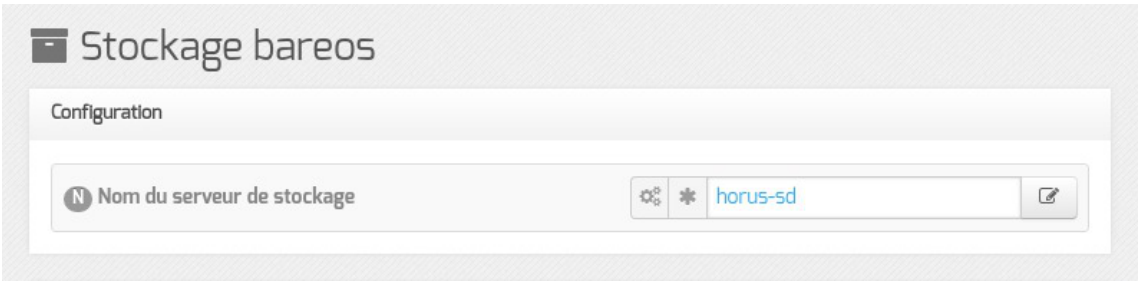
Type de compression et délai alloué

Le délai permet d'arrêter le job après un temps d'exécution fixé en seconde, par défaut le job n'a pas de 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.

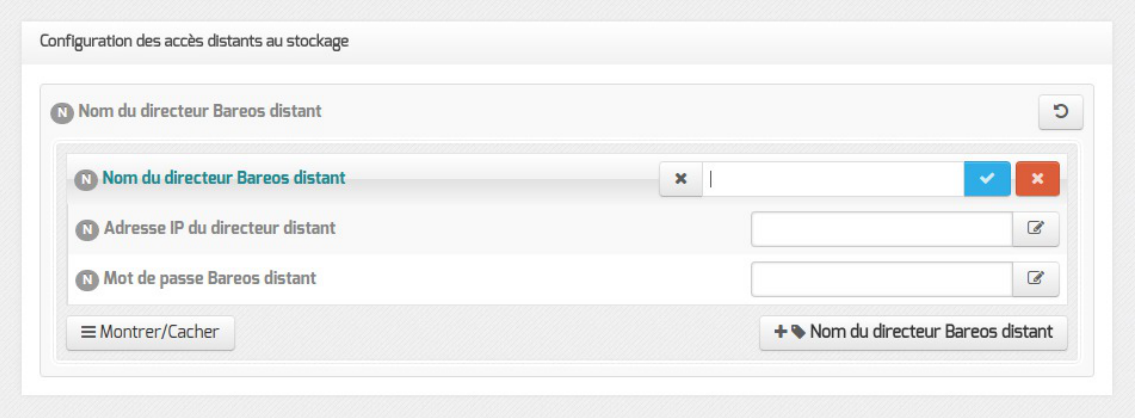


Pour ajouter un ou plusieurs directeurs distants à se connecter il faut cliquer sur `Nom du directeur Bareos distant`, le détail de l'autorisation s'affiche.

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.619]

10.2.3.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 :

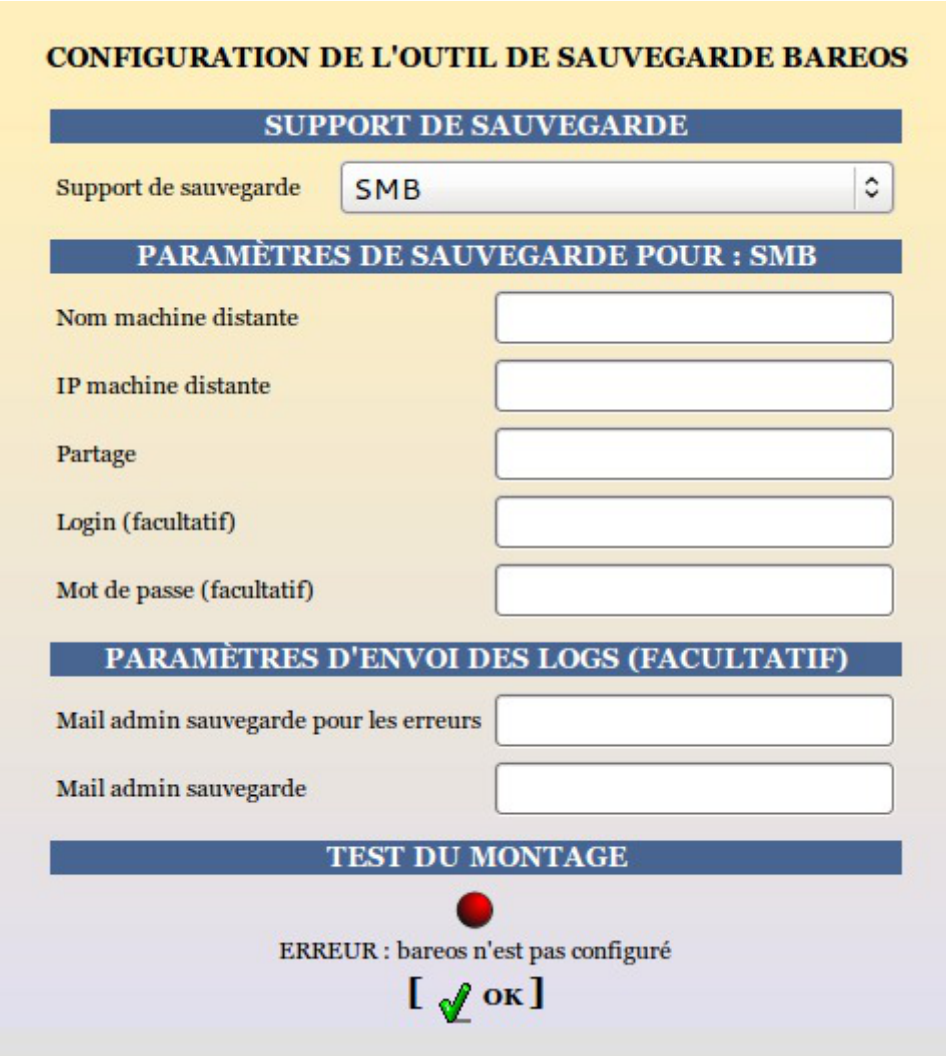
- SMB
- Disque USB local
- Configuration manuelle du support

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.901].
  Il est préférable de déporter le serveur de stockage Bareos plutôt que d'utiliser le protocole SMB [p.901].
  Ce type de sauvegarde sera utilisé, par exemple, pour les NAS [p.894].
  Les informations suivantes sont demandées :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- `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`.



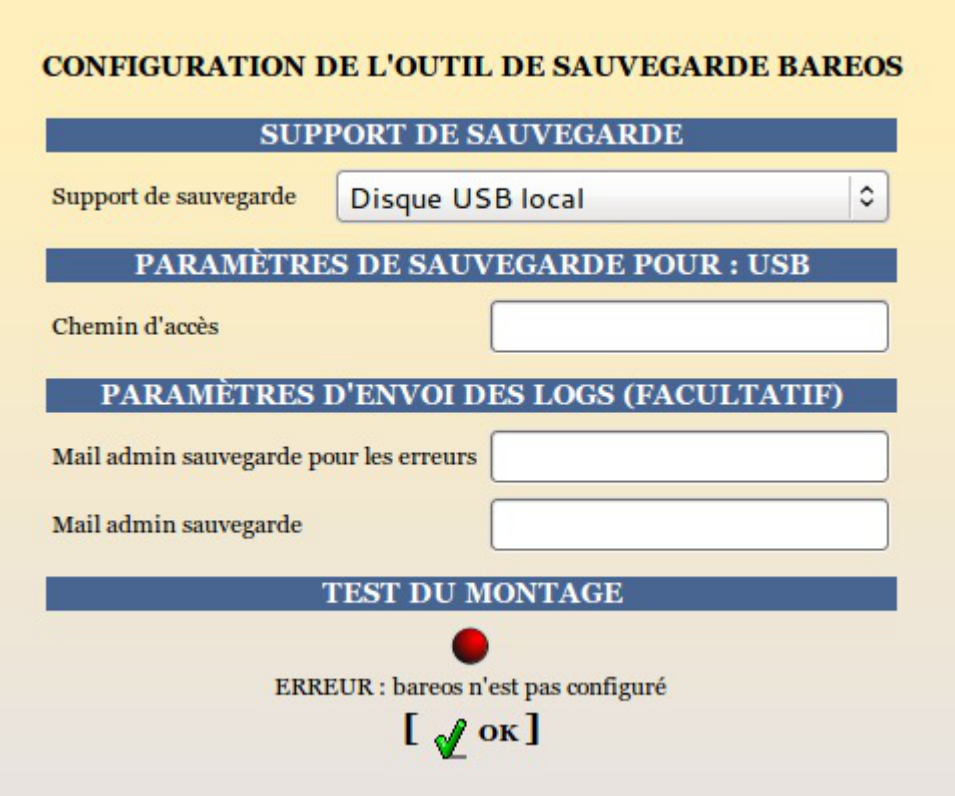
Configuration d'un support de sauvegarde distant dans l'EAD

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).

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.

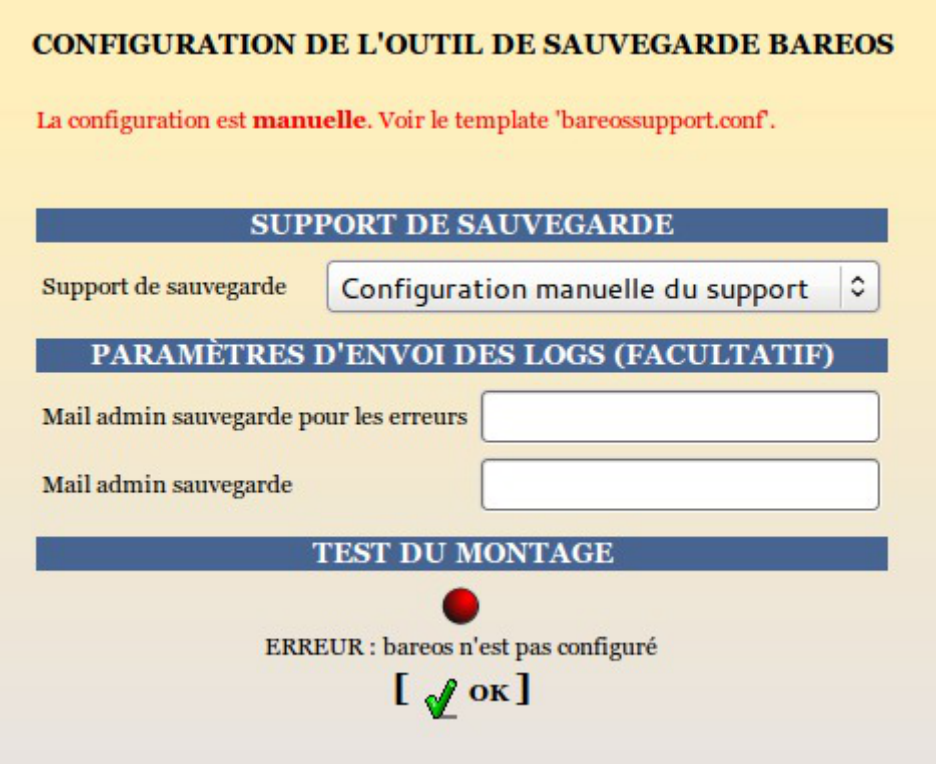
Pour information, le fichier template concerné `bareossupport.conf` est dans `/usr/share/eole/creole/distrib/`

Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE[p.897].

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.891] : 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}
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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.



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}'
```

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.901].



Il est possible de déclarer plusieurs destinataires en séparant les adresses par des virgules.

Exemple : `admin@ac-dijon.fr,technicien@ac-dijon.fr`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

10.2.3.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 :

```
# 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.897].

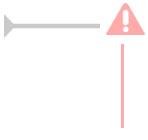


`nom_machine` ne doit pas comporter de majuscule

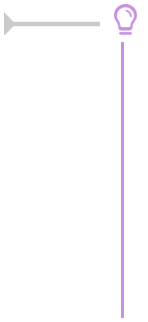


Pour tester le support de sauvegarde (USB local ou SMB), il est possible d'utiliser le script `bareosmount.py` :

```
# 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.891] : 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 :

  - `/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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
DISTANT_LOGIN_MOUNT='/bin/mount -t cifs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev,sec=nt
//{4}/{5} {6}'
```

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` :

```
# bareosconfig.py -d
Support : {'usb_path': '/dev/sdb1', 'support': 'usb'}
Mail : {}
Programmation : non configuré
```

10.2.4. 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.

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.

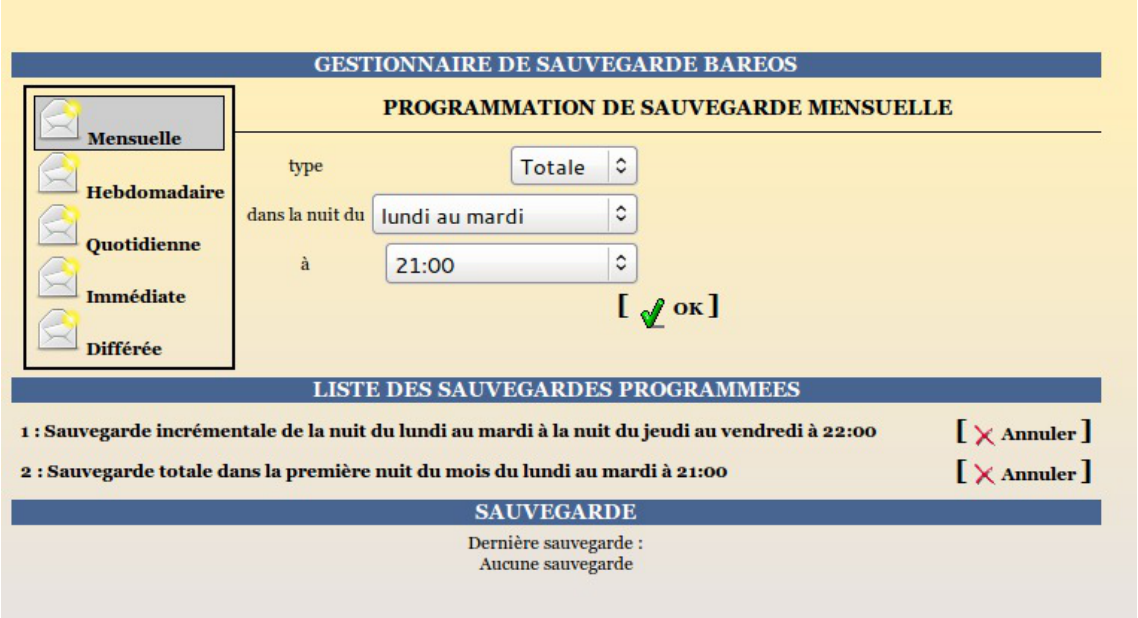
Les sauvegardes se programment pour une nuit de la semaine. Une nuit va de 12h à 11h59.

Pour les sauvegardes quotidiennes, il est possible de choisir une plage de jours.

Programmation depuis l'EAD

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

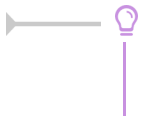
Il est nécessaire de choisir le type de sauvegarde totale (Full), différentielle (Differential) ou incrémentale (Incremental)).

Si aucune sauvegarde n'a été effectuée préalablement sur le serveur, la première sauvegarde sera automatiquement une sauvegarde totale.

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.err.log



`bareosconfig.py --help` donne la liste des options de bareosconfig.py

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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>
```

10.3. 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.

10.3.1. Restauration complète

> La restauration d'un serveur se fait 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# 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
```

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 nom du directeur
```

```
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.

Démontage du support

Pour démonter le support de sauvegarde :

```
# bareosmount.py --umount
```

Instanciation

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 ?
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
[oui/non]
```

Ne pas tenir compte du message d'erreur suivant :

```
ERREUR : /var/lib/eole/config/shedule.conf not exist
```

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
```

```
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`.

10.3.2. Restauration partielle

Rechercher un fichier à restaurer

Pour rechercher un fichier ou un répertoire dans le support de sauvegarde (sur la dernière sauvegarde

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

```
# 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```

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
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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 : /
$ 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
[...]
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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

`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.

10.4. 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,

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
}
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` .

10.5. 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

10.6. 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.



Mire d'authentification de bareos-webui

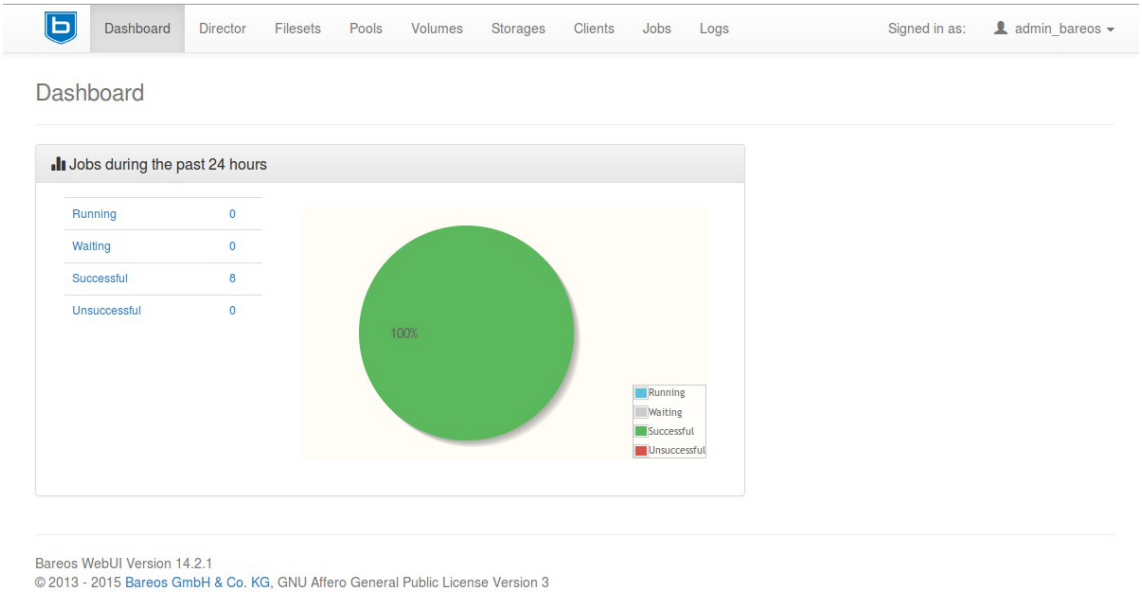
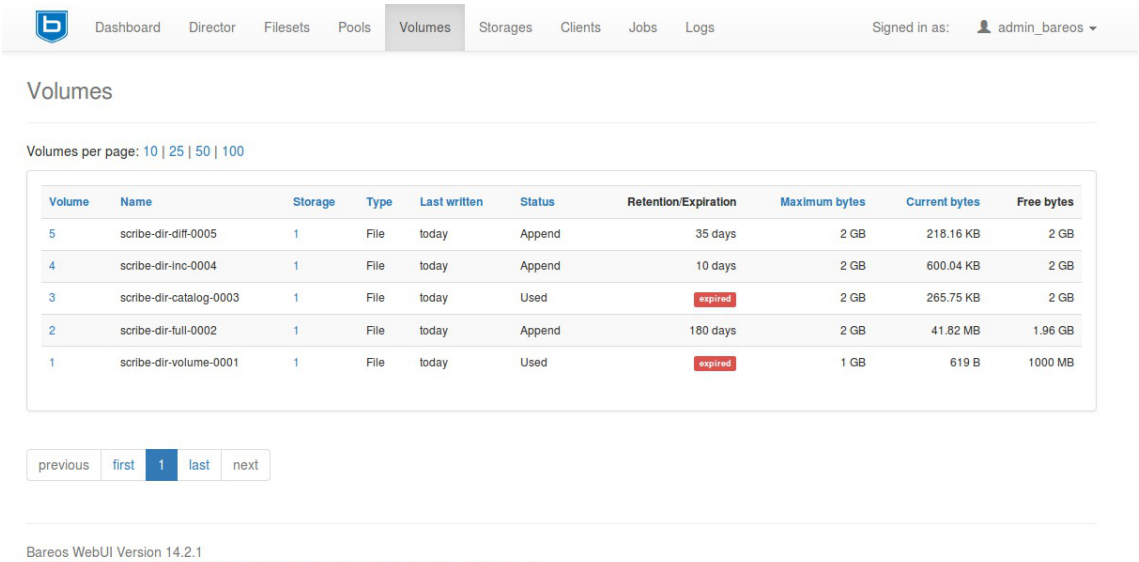
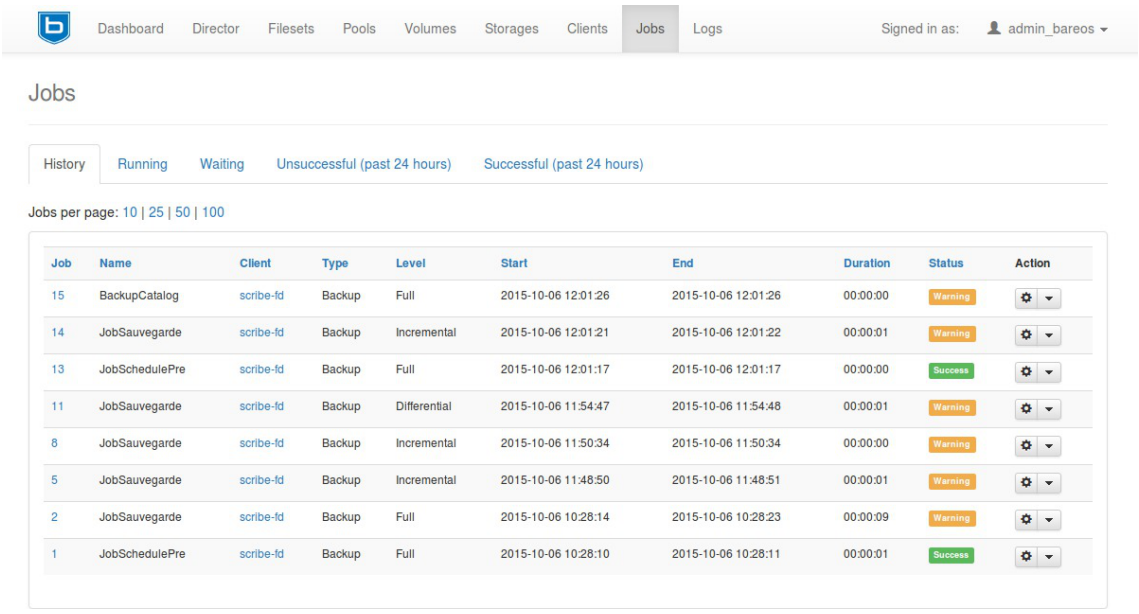


Tableau de bord de bareos-webui

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Affichage des volumes dans bareos-webui



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
```

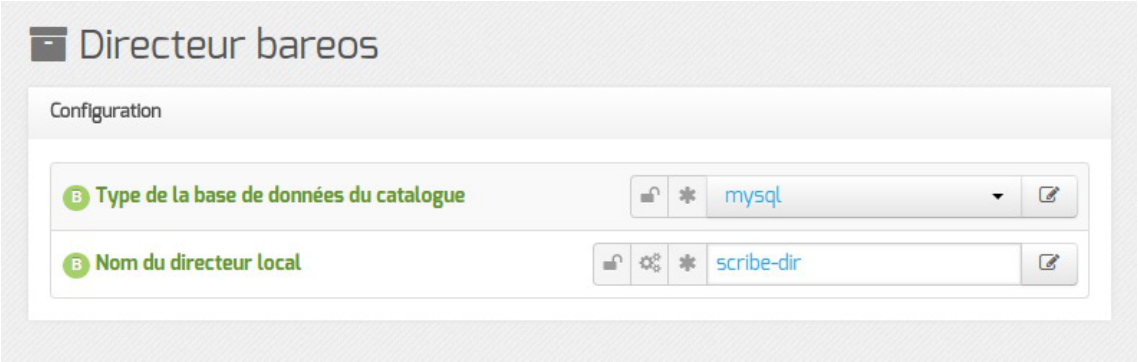
Le paquet est pré-installé sur les modules Scribe, Horus et AmonEcole.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

```
# 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.323]

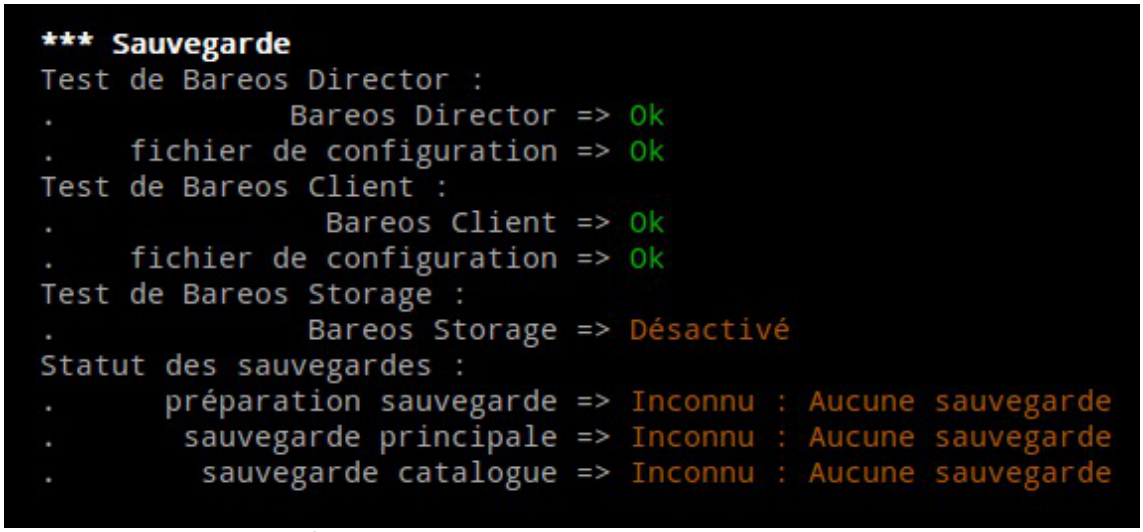
10.7. Diagnostic, rapport et résolution de problème

10.7.1. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



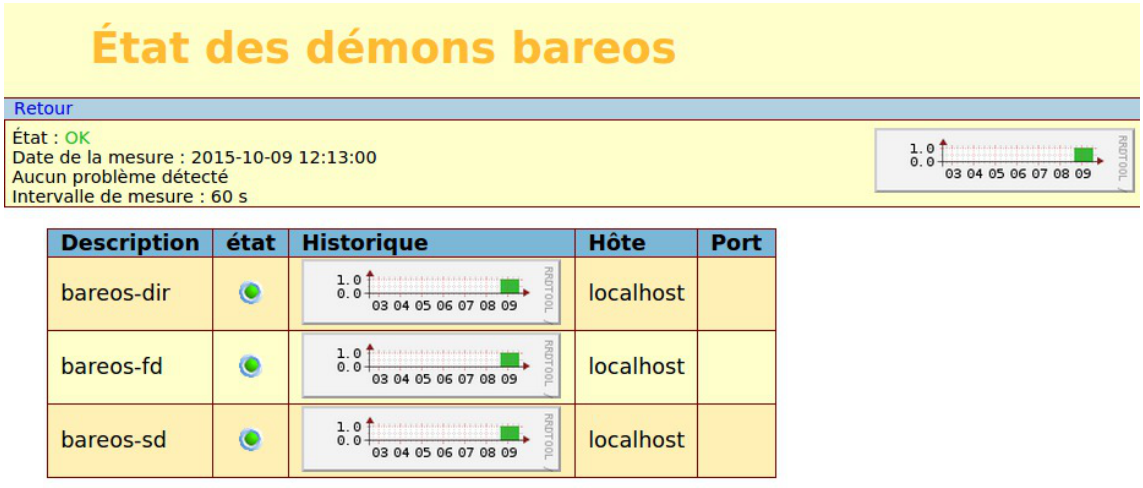
État des sauvegardes et des services avec diagnose

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

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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)

Échec du test de montage :
point de montage : Erreur
permissions : Erreur
montage : Erreur
root@scribe:~#
```

10.7.2. 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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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 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=0:603259372 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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
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"
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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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`.

10.8. Annexes

Voici un complément d'information (outils d'administration, liens, ...) pour aller plus loin avec Bareos.

10.8.1. 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`

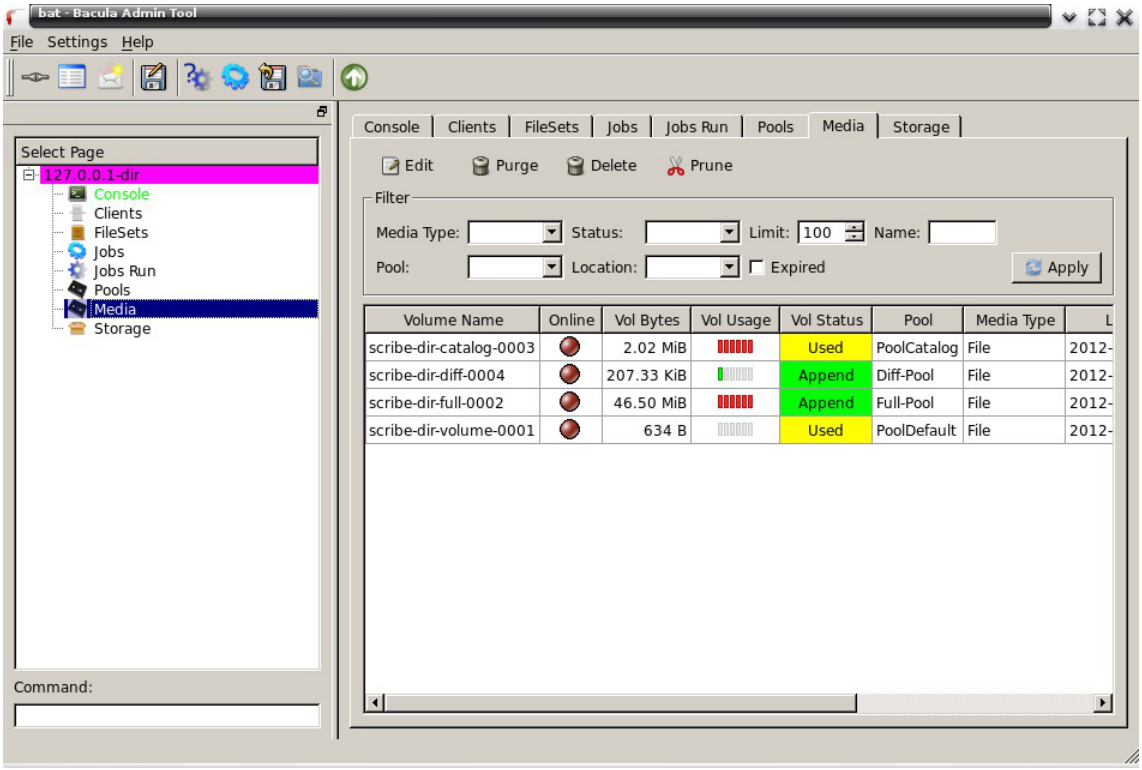
  BAT se lance avec la commande suivante :

  `# 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>
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

10.8.2. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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

10.8.3. 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.

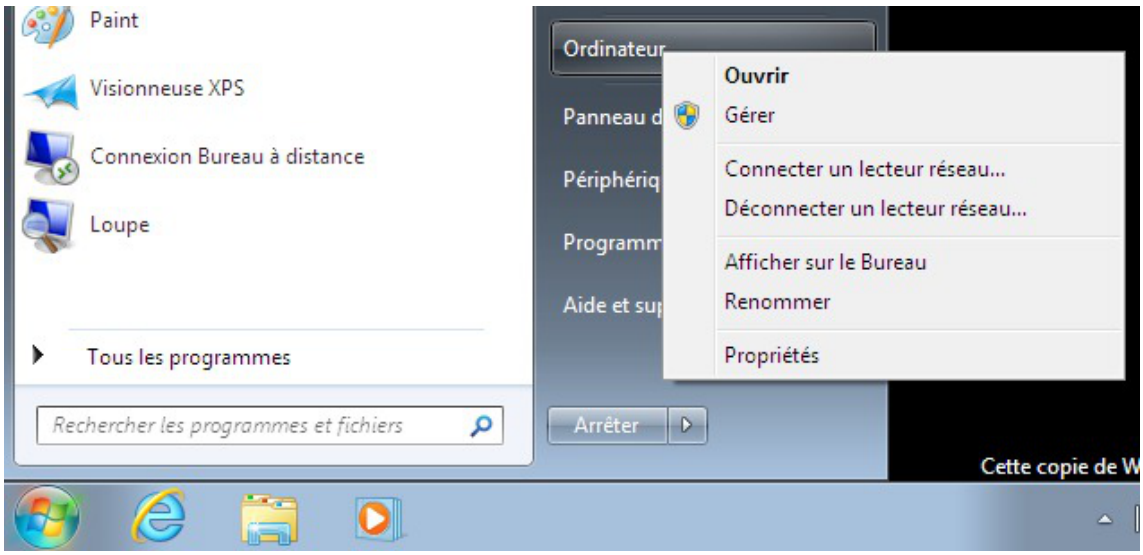
Voici comment créer un partage avec les droits d'accès adéquats sur un poste équipé de Windows Seven.

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.

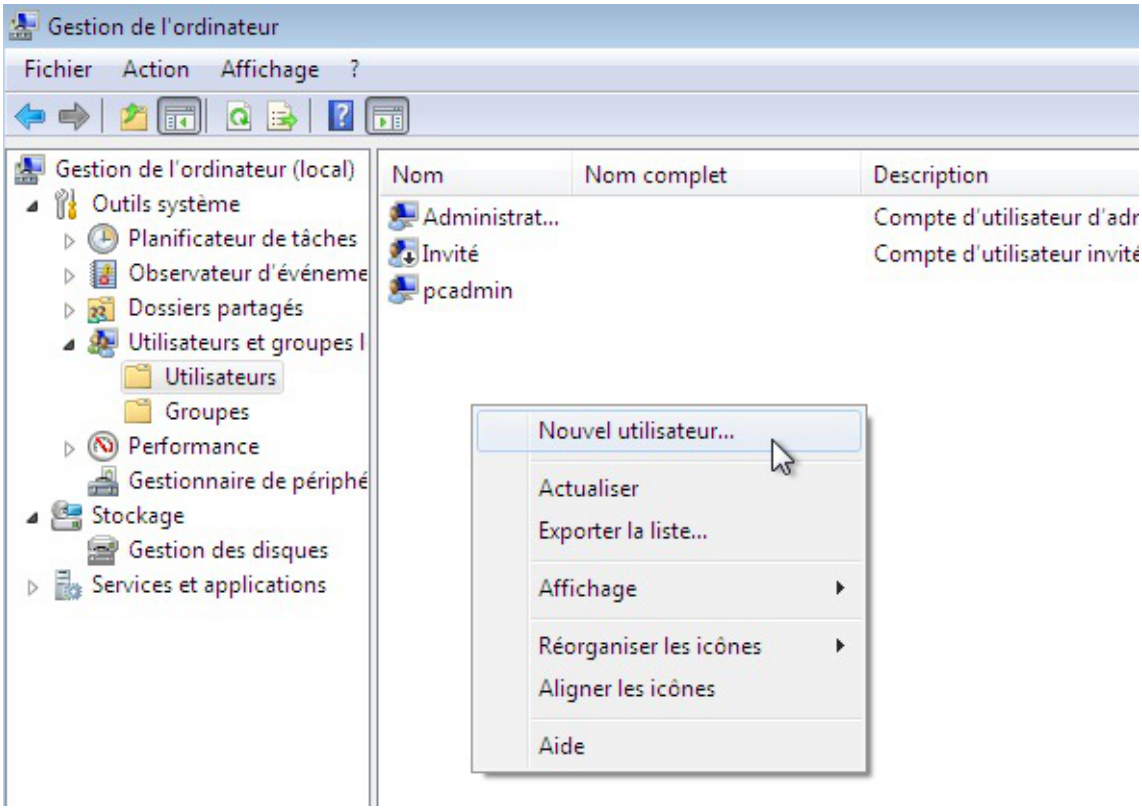
Puis ouvrir la console de **Gestion de l'ordinateur** : Menu démarrer → Ordinateur → clic droit Gérer.



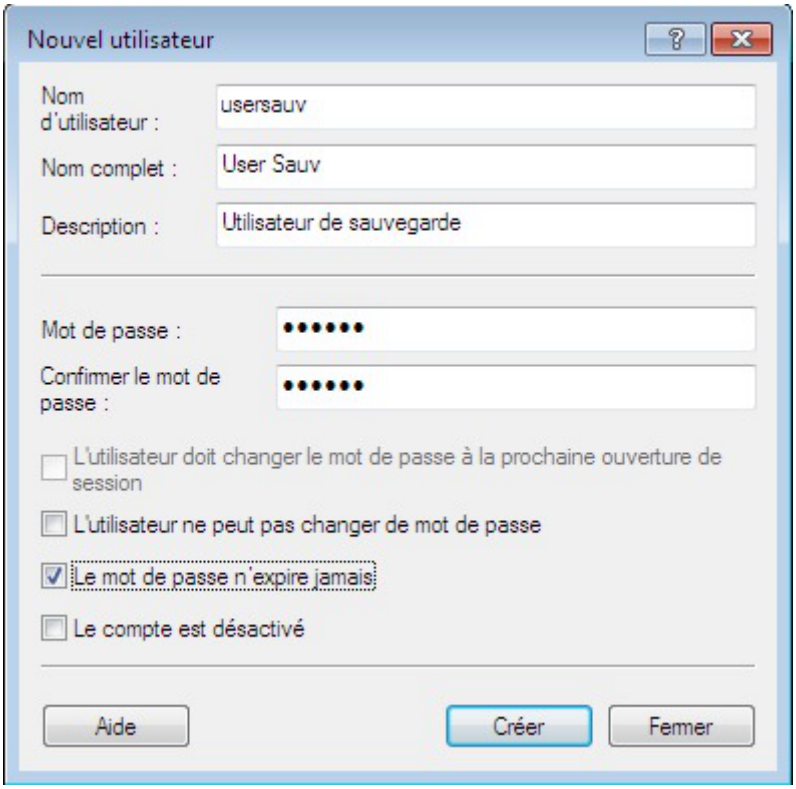
Aller dans le menu : Outils système → Utilisateurs et groupes locaux → Utilisateurs, puis effectuer un clic

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

droit dans l'espace vide.



Configurer l'utilisateur comme ceci :



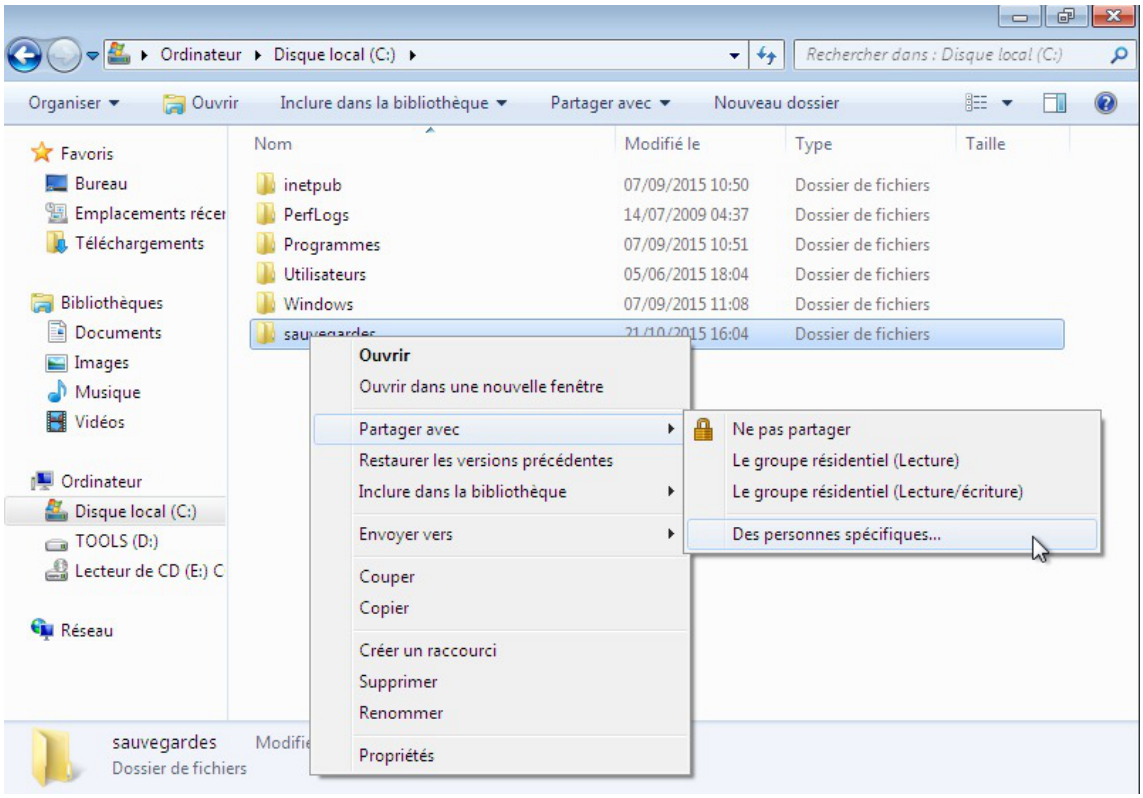
Finaliser l'opération en cliquant sur le bouton `Créer`.

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

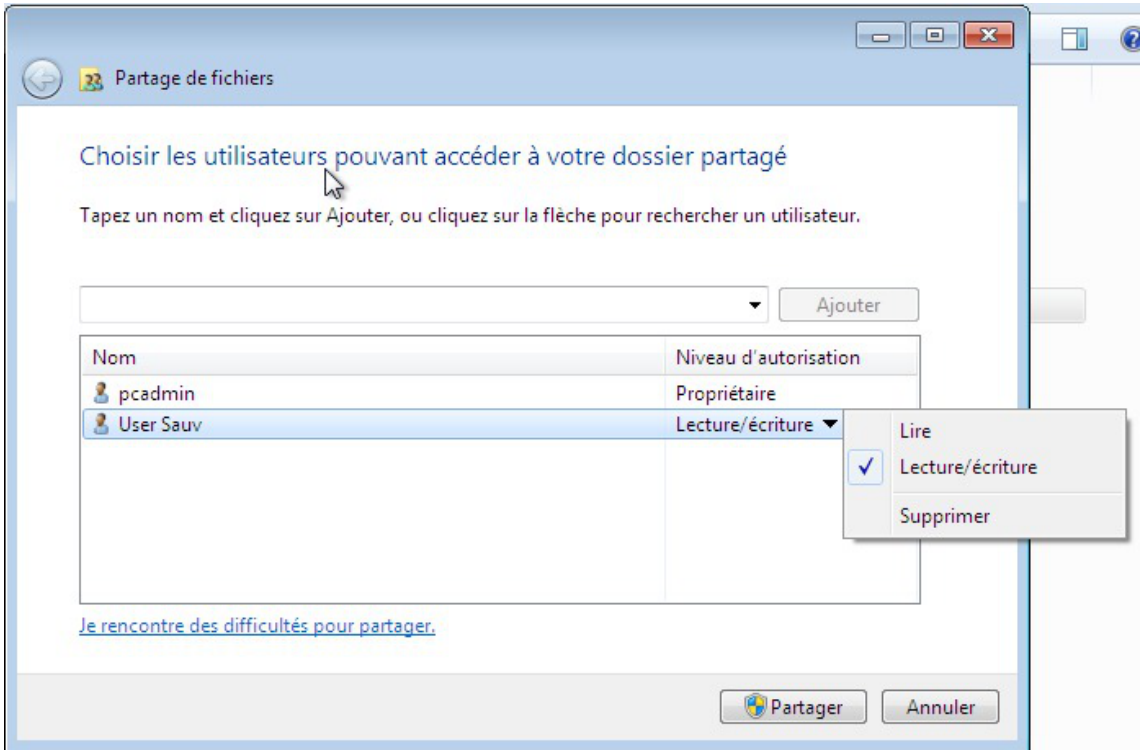
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

dossier et sélectionner `Partager avec` puis `Des personnes spécifiques...`



Entrer le nom de l'utilisateur créé précédemment et cliquer sur le bouton `Ajouter`.

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**.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> En cas d'erreur du type *Windows n'a pas pu trouver <utilisateur>*, vérifier que le nom saisi correspond bien au **nom d'utilisateur**.

10.8.4. 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.

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.

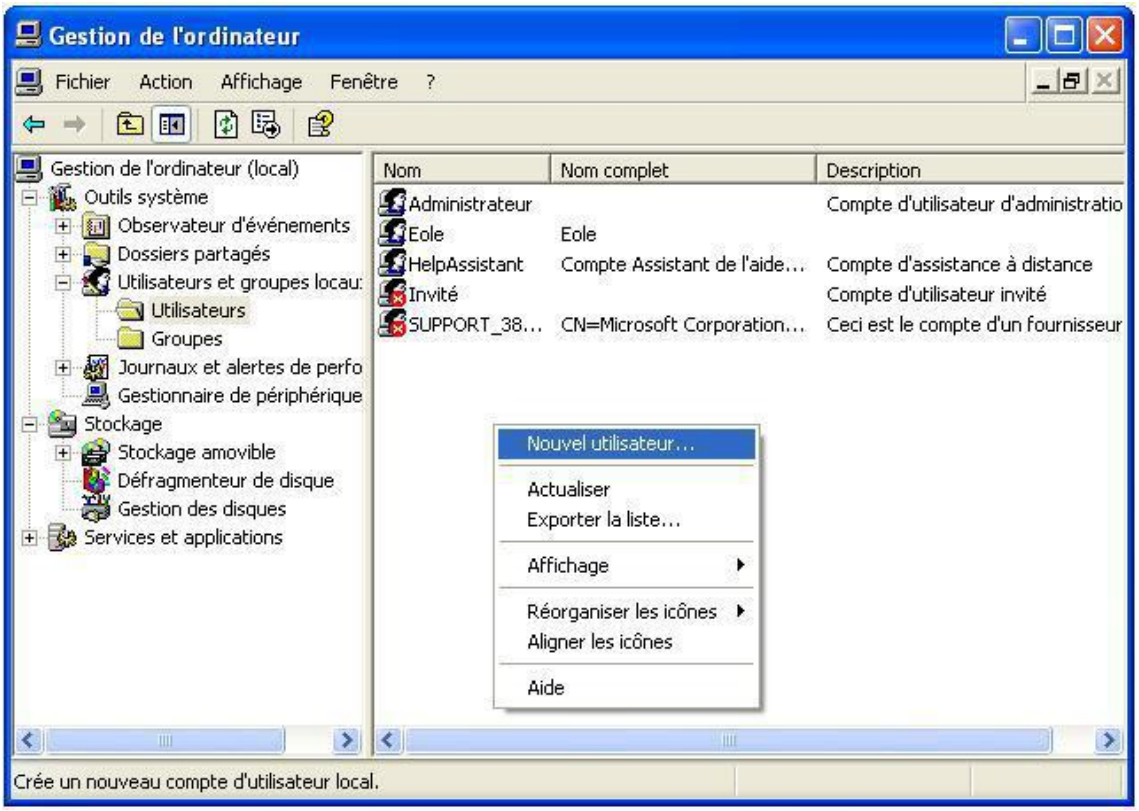
Création d'un compte sur le poste Windows XP

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**.

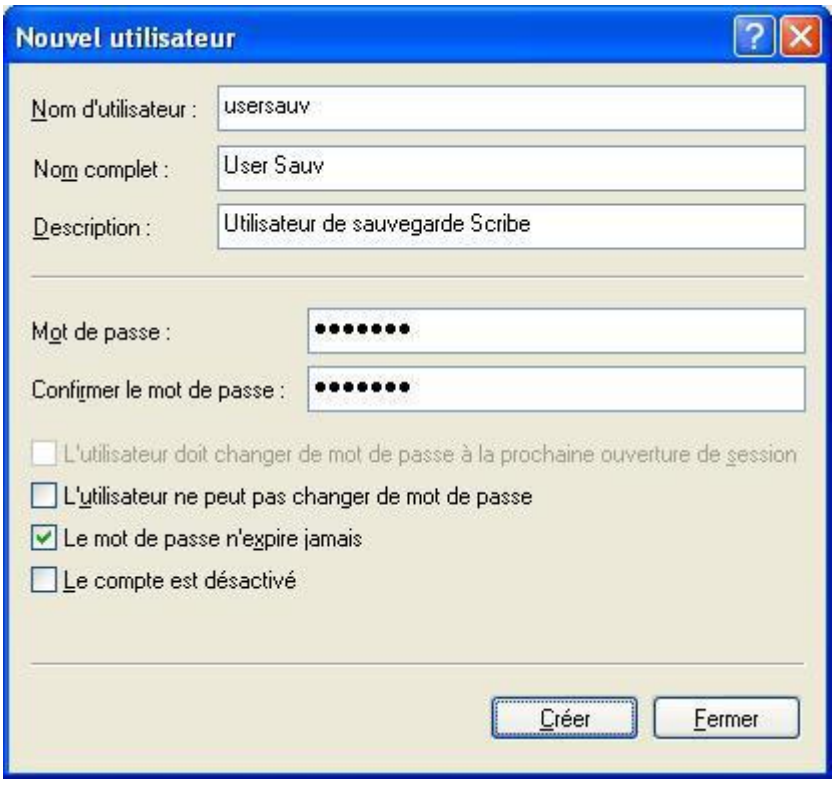


Ensuite, créez un nouvel utilisateur : Menu "**Action**" ou clic droit dans l'espace vide de la colonne de droite.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



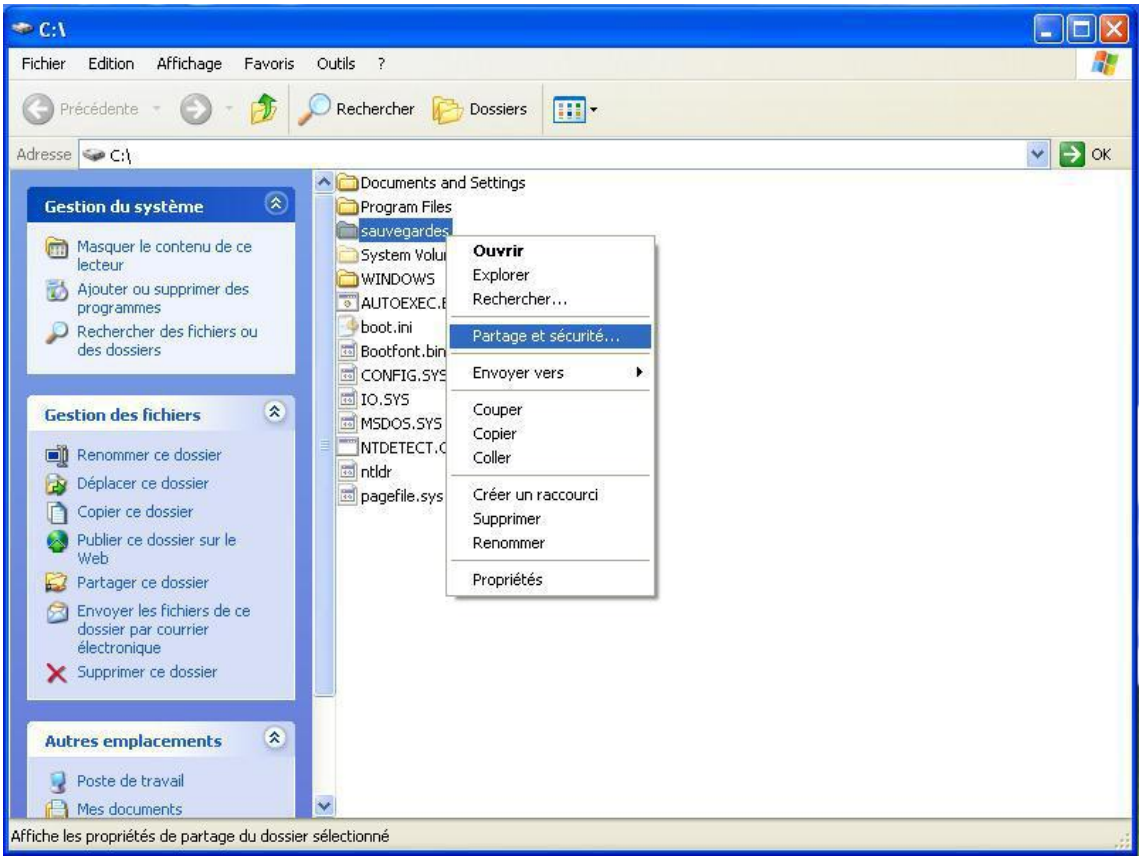
... avec les options configurées.



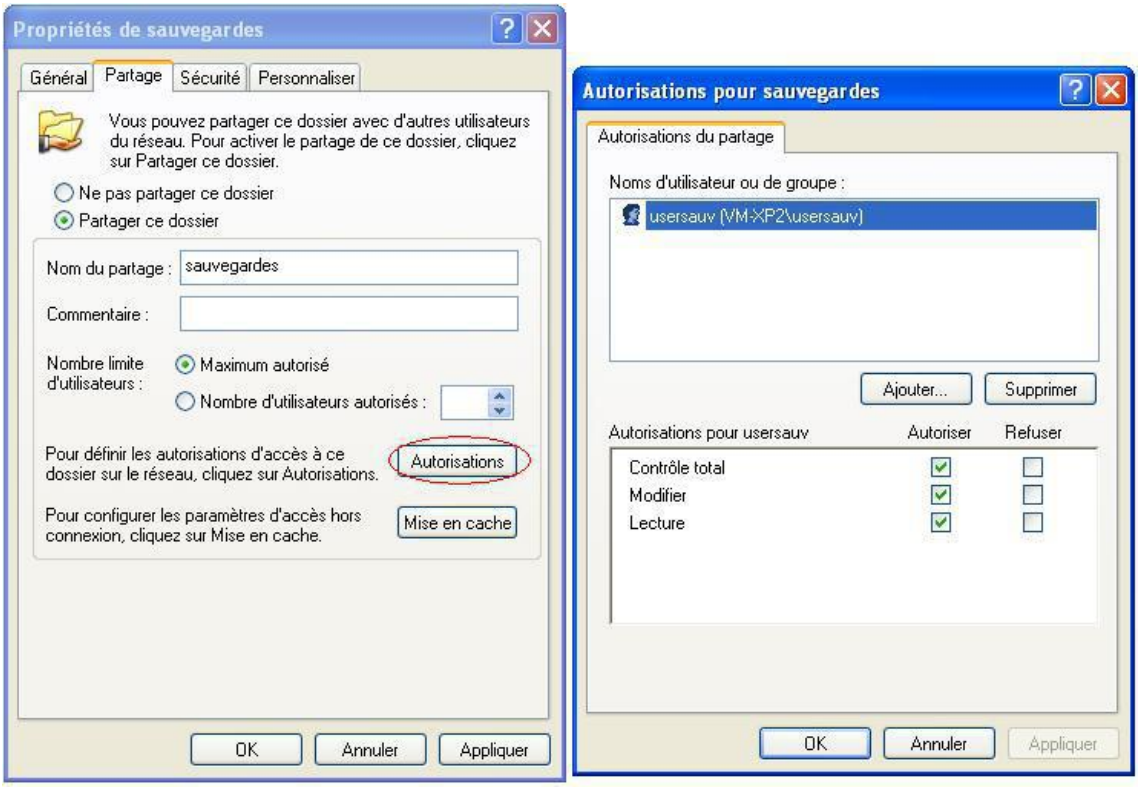
Partage du dossier et réglage des droits d'accès

Après avoir créé un dossier "*sauvegardes*" à l'emplacement de votre choix, partagez-le à l'aide d'un clic droit sur le dossier.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

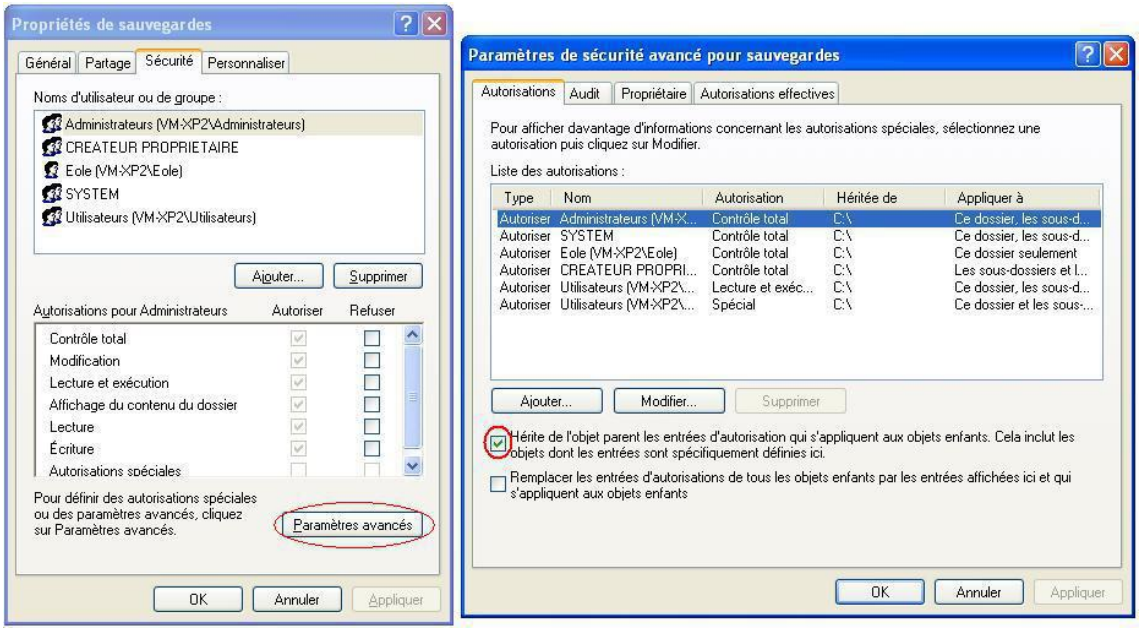


Puis cliquez sur **Autorisations**. Supprimez les autorisations par défaut ("*Tout le monde*") puis ajoutez "*usersauv*" avec "**Contrôle total**".

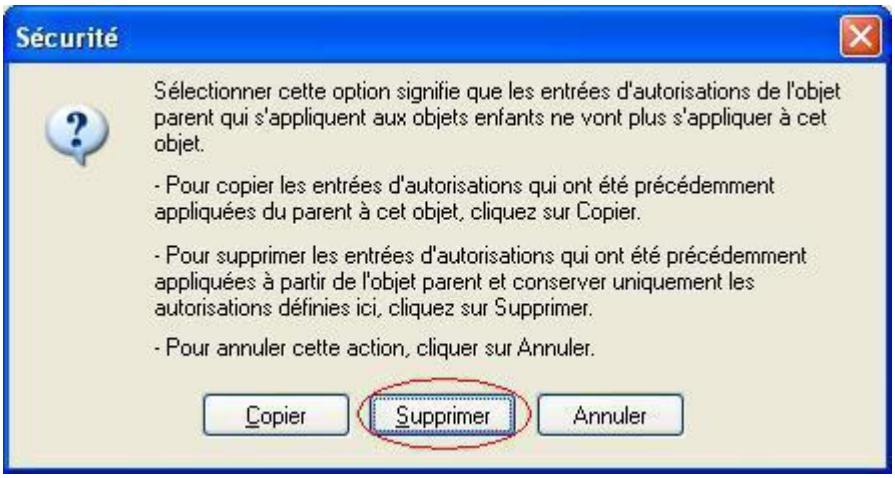


Fermez la fenêtre des autorisations puis allez dans l'onglet "**Sécurité**" et cliquez sur "**Paramètres avancés**".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Décochez "**Hérite de l'objet parent...**", une fenêtre s'ouvre alors, sélectionnez "**Supprimer**".

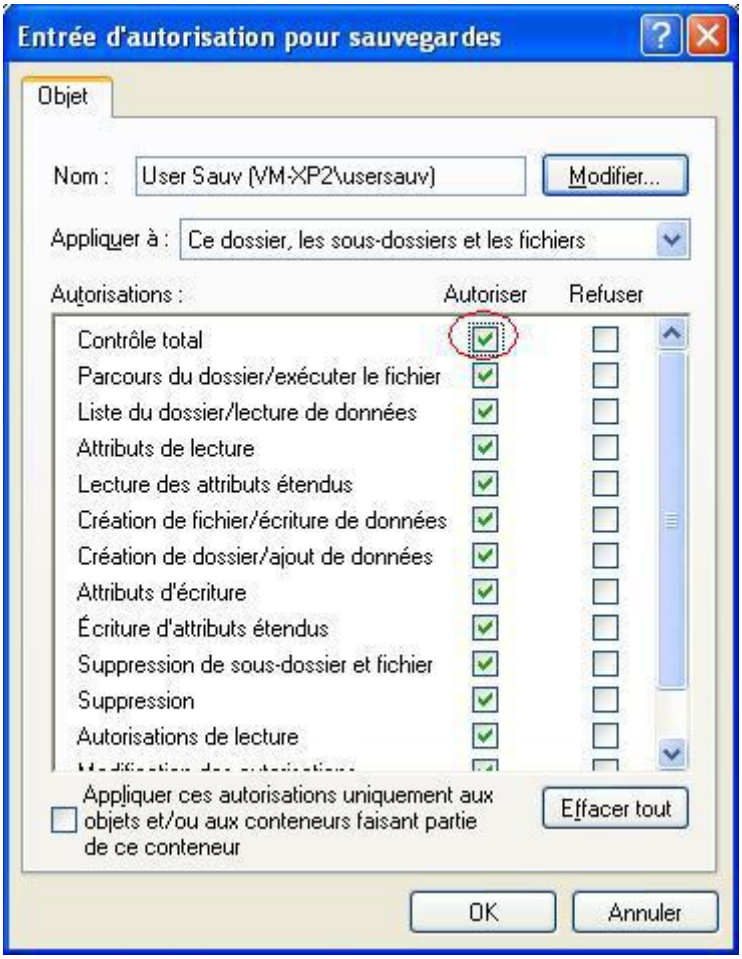


Ajoutez ensuite l'utilisateur "*usersauv*" toujours avec le "**Contrôle total**".



Enfin, affectez le "**Contrôle total**".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



11. 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.887].

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).

11.1. L'interface simplifiée

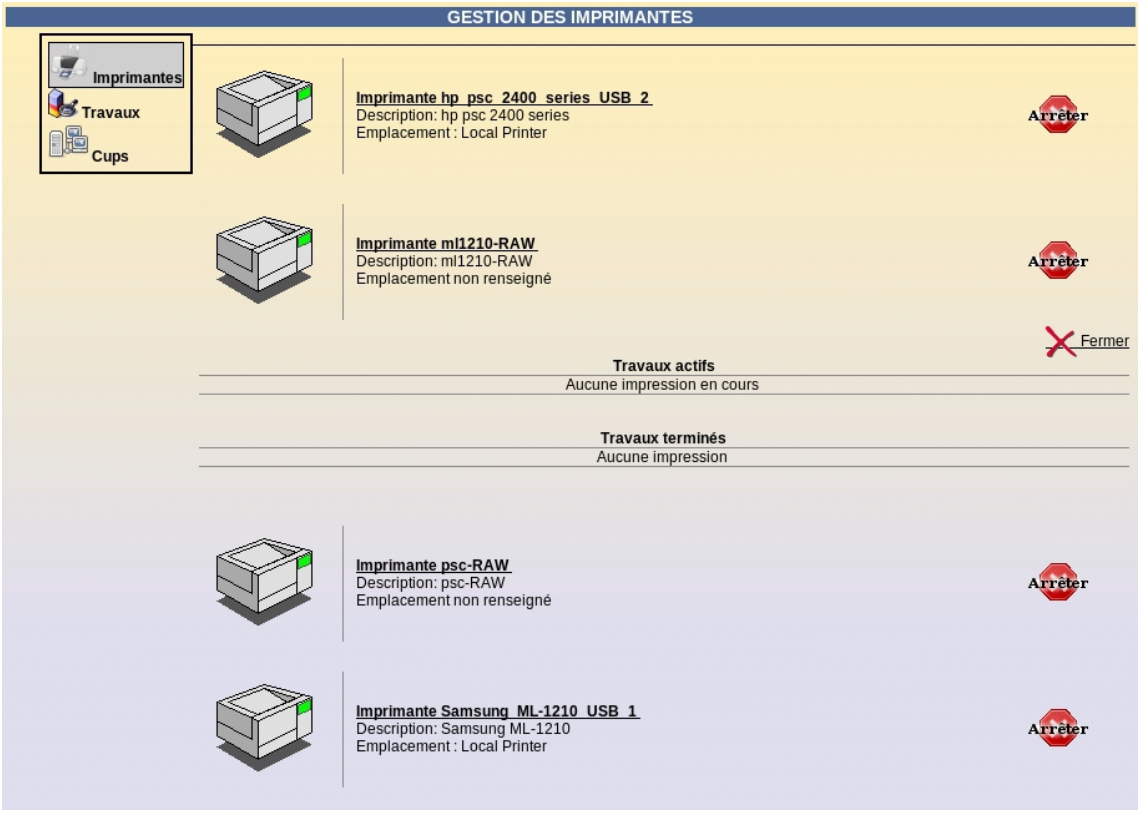
L'interface de gestion des imprimantes intégrée à l'EAD permet de gérer les imprimantes déjà installées.

L'administrateur et les enseignants peuvent :

- consulter l'état des imprimantes ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- consulter/interrompre/relancer les travaux d'impression ;
- arrêter/démarrer des imprimantes.



11.2. L'interface de gestion CUPS

CUPS (Common UNIX Printing System) fournit une interface web pour faciliter l'installation et la gestion des imprimantes sur le serveur.

Cette interface est totalement accessible aux utilisateurs *root*, *<nom du module>*, *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.

CUPS est le serveur d'impression intégré à la solution EOLE.

Nous ne verrons ici que la partie serveur de la configuration des imprimantes.

11.2.1. Création de l'imprimante

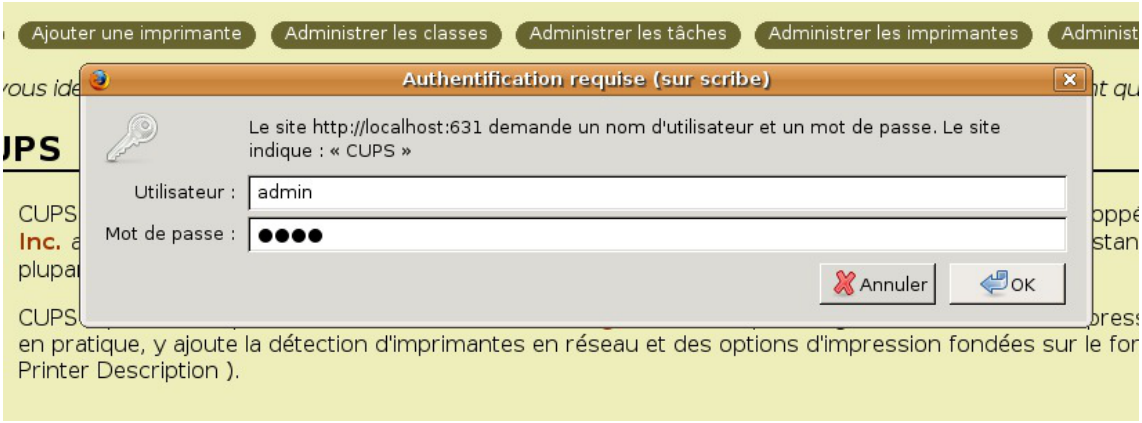
11.2.1.a. Ajouter une nouvelle imprimante

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`.

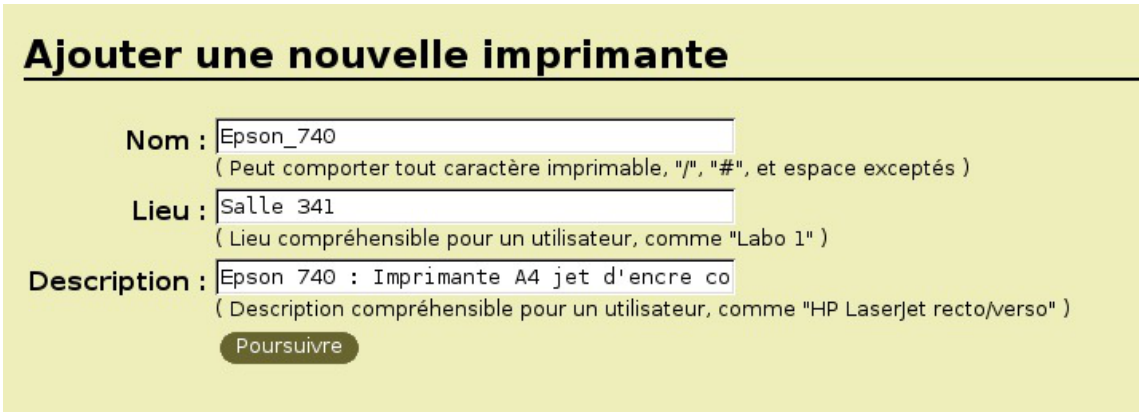
Il est nécessaire de s'identifier avec un utilisateur *root*, *<nom du module>*, *admin* ou appartenant au groupe *PrintOperators*.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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

11.2.1.b. Choix du matériel

Il y a trois grands types d'imprimantes :

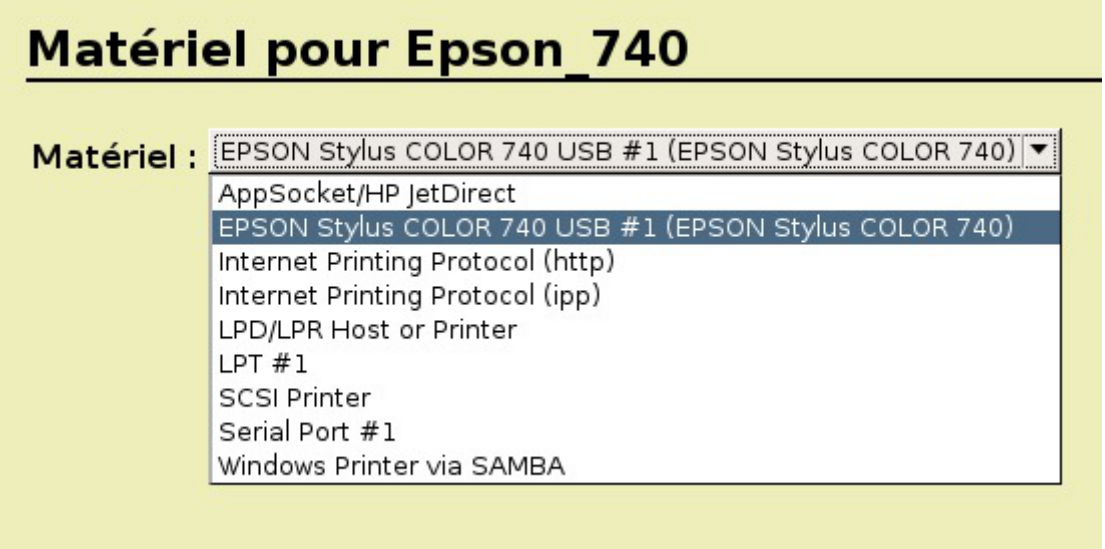
- les imprimantes locales (avec un port USB, parallèle, ...) ;
- les imprimantes réseaux ;
- les imprimantes partagées sur un poste client Windows.

> 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

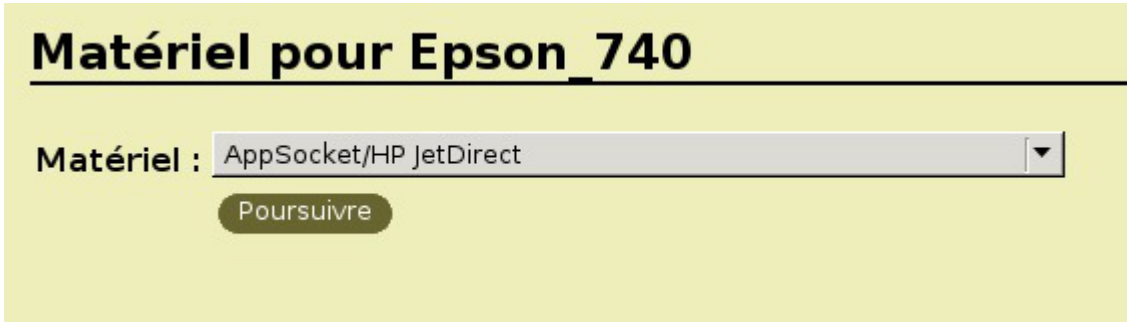
> Les imprimantes réseaux

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

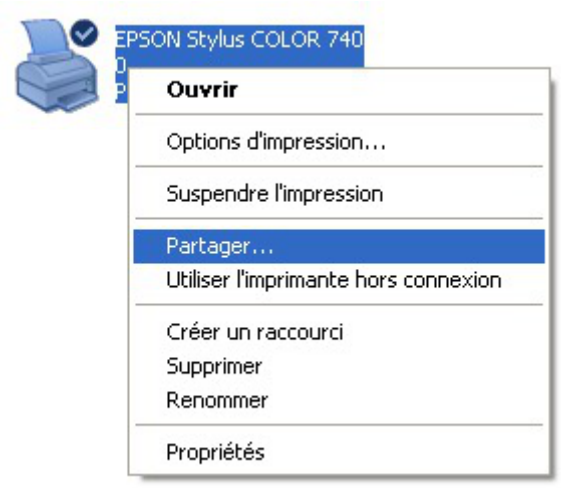
Création d'un partage d'imprimante sous Windows XP

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.

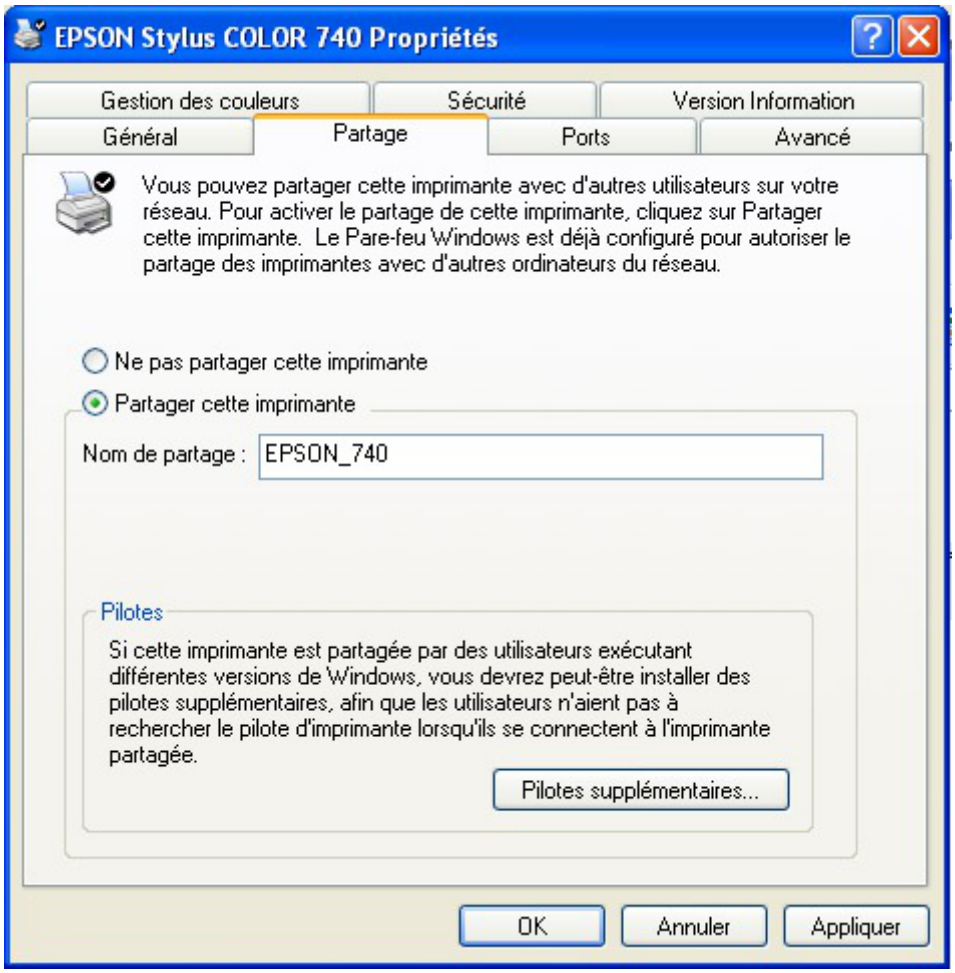
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Dans le menu Windows `Démarrer/Imprimantes et télécopieurs` cliquer droit sur votre imprimante et choisir `Partager...`.



Partager une imprimante sous Windows

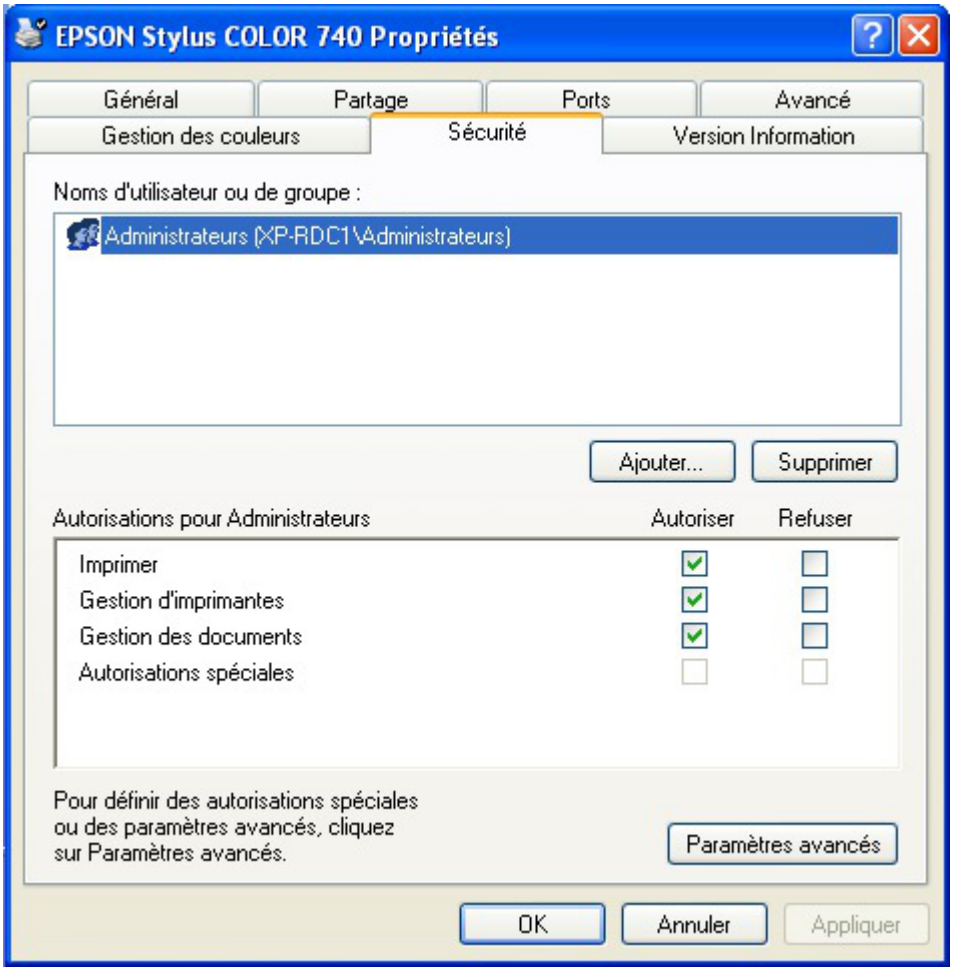
Il suffit alors de cocher `partager cette imprimante` et de donner un *Nom de partage*.



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)

11.2.2. Choix du pilote

Il existe deux catégories de choix pour les pilotes d'impression.

- utilisation du pilote client Windows ;
- utilisation du pilote CUPS.

11.2.2.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.

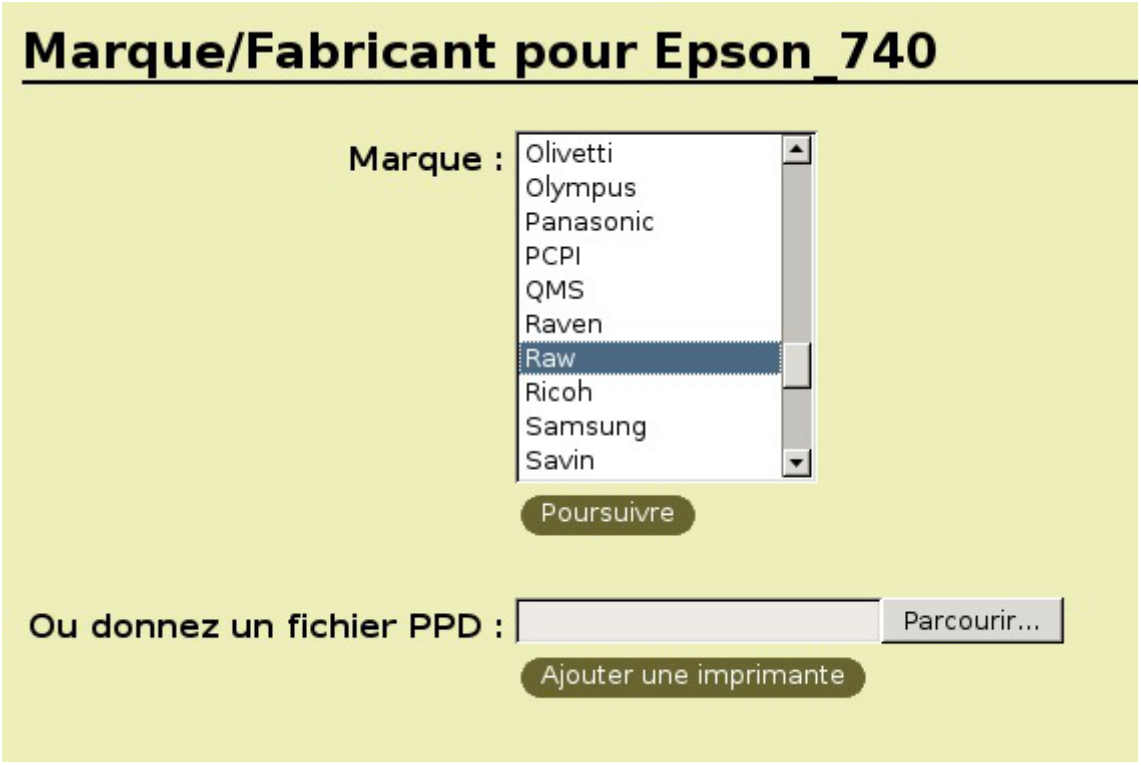
Le pilote CUPS est plus simple à mettre en place. Il est particulièrement adapté aux réseaux hétérogènes. Par contre, les pilotes ne sont souvent pas écrits directement par les constructeurs.

11.2.2.b. Utilisation des pilotes clients Windows

Configuration de CUPS

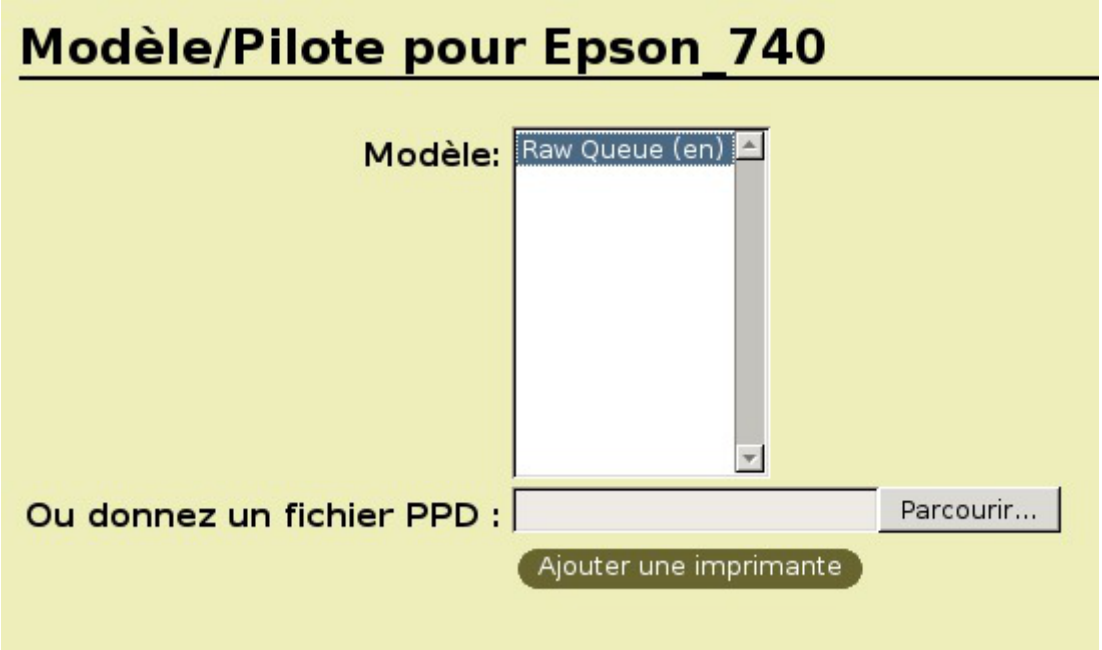
Dans la liste des marques, choisir "*Raw*" quelque soit le modèle de l'imprimante et "*Raw Queue*" comme modèle.

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 ...*".

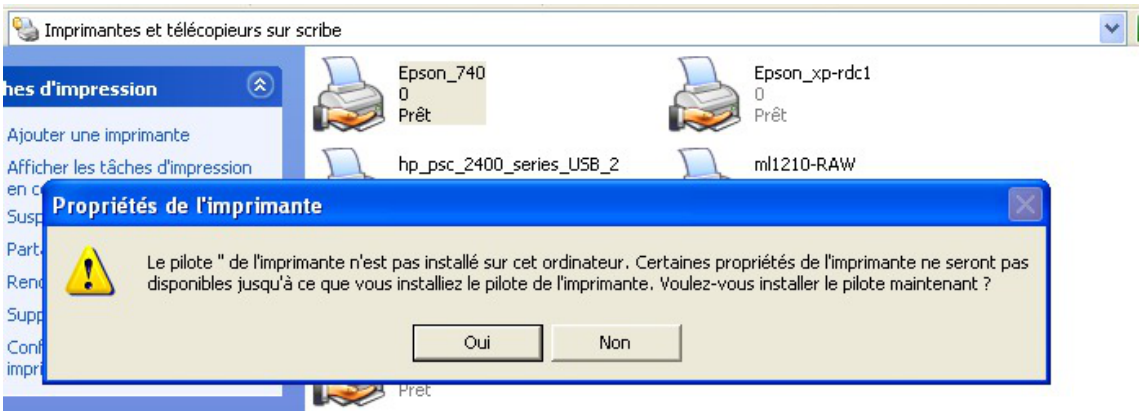
Cliquer droit et choisir `propriétés`.



Propriété de l'imprimante sous Windows

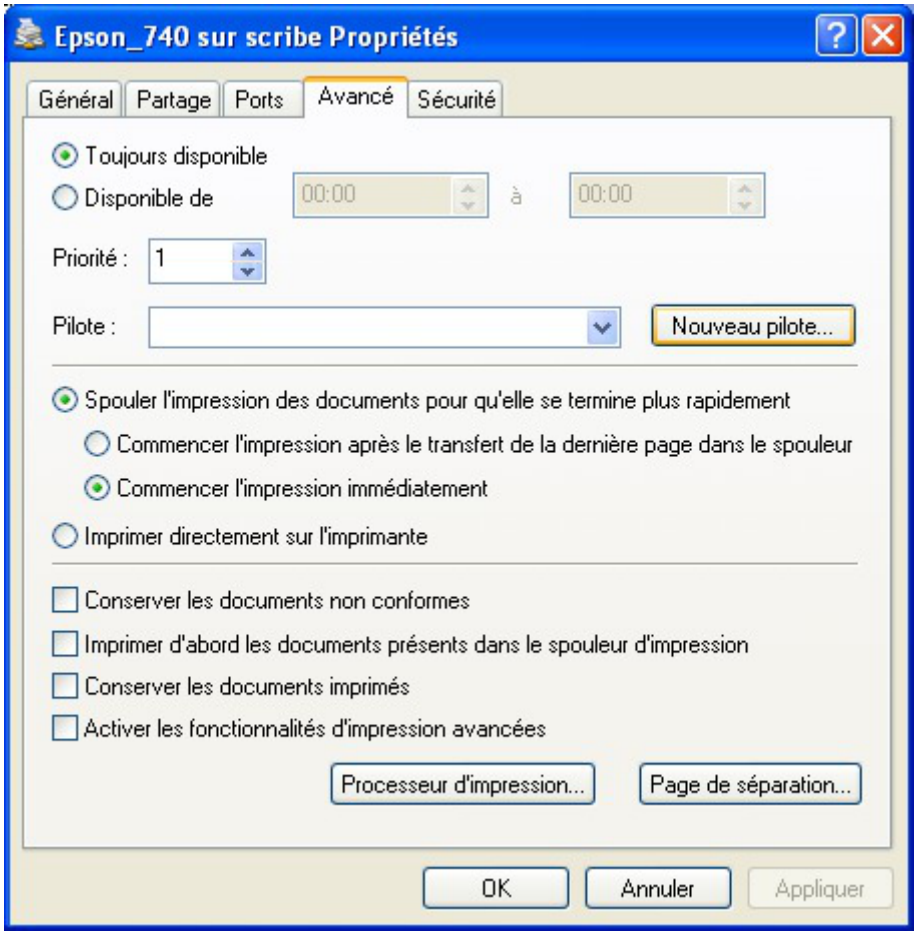
Répondre `non` à la question "*Voulez-vous installer le pilote maintenant*".

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.

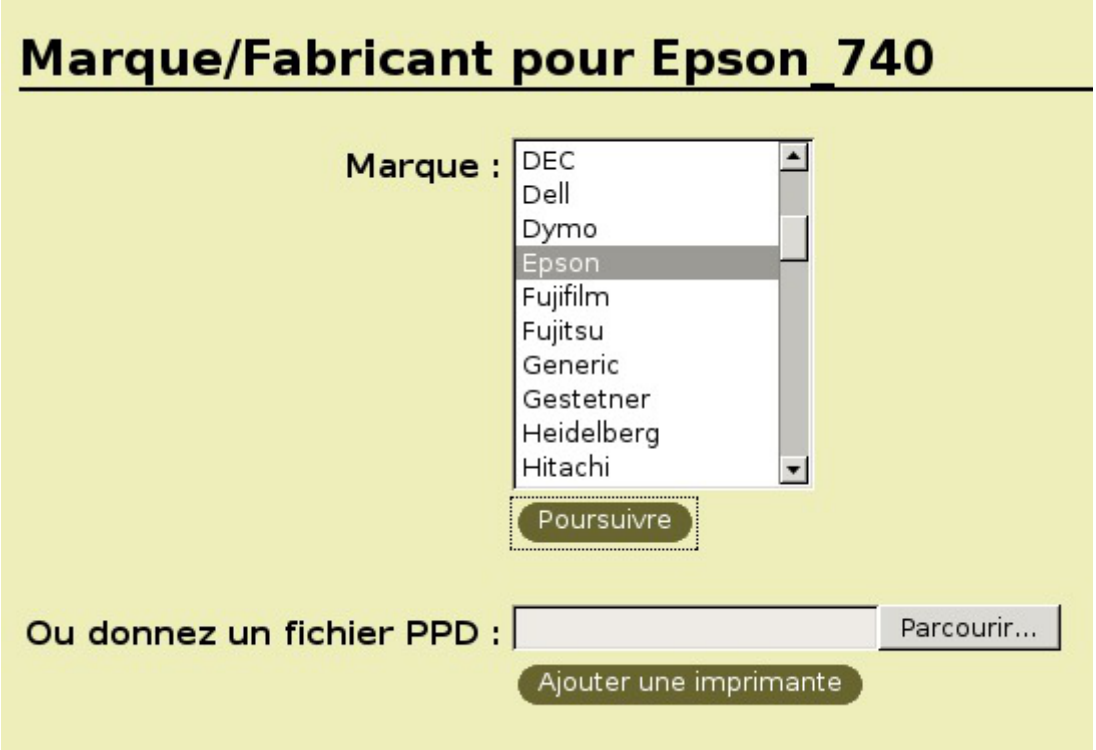
Dans l'onglet "Partage" il est possible d'installer des "Pilotes supplémentaires..." pour les autres versions de Windows.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

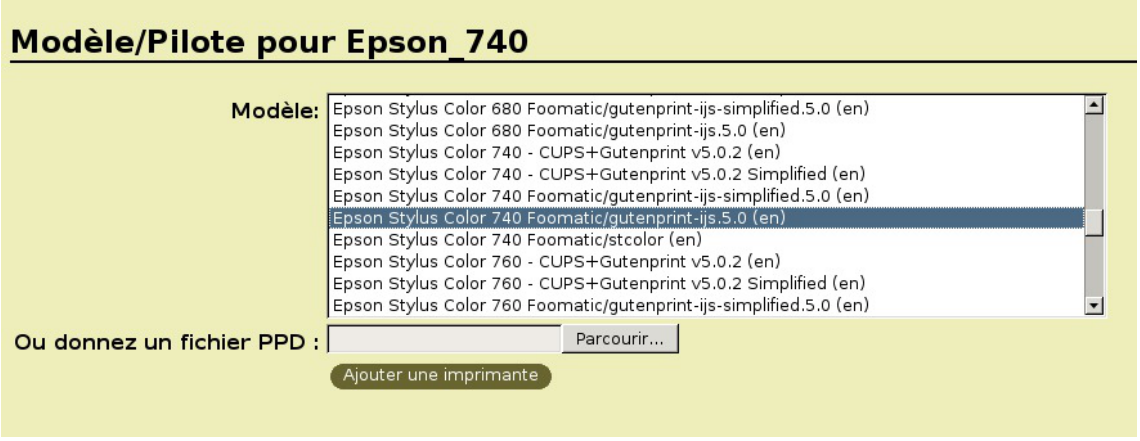
11.2.2.c. Utilisation des pilotes CUPS

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.

11.2.3. 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

11.3. Gestion des imprimantes sous Windows



Ceci ne concerne pas les postes Windows Millennium et inférieur et nécessite l'utilisation du logiciel ESU[p.889].

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.

11.4. Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvé une ou des réponses.



Accéder à l'interface de gestion de CUPS sur un module AmonEcole

Utiliser l'adresse IP du serveurs de fichiers.

Pour se connecter à l'interface de gestion de CUPS sur un module AmonEcole il faut utiliser l'adresse IP du serveur de fichiers renseignée dans l'interface de configuration du module.

Dans un navigateur web, sans passer par le proxy, il faut saisir l'adresse suivante :

```
https://<adresse IP du serveur de fichiers>:631
```

12. Les applications web sur le module AmonEcole

Le module AmonEcole est l'association du module Amon et du module Scribe. Ce module intègre donc l'ensemble des applications web proposées sur le module Scribe. La plupart sont le résultat de la mutualisation inter-académique Envole.

Elles sont adaptées pour fonctionner avec un serveur d'authentification unique. Grâce à cette méthode d'authentification unique, les utilisateurs du module Scribe 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.

Parmi les services web qu'il est possible de proposer on trouve des cahiers de texte numériques, des gestionnaires de fichiers, des CMS[p.885] mais aussi un portail.

Le portail Envole permet de centraliser les différentes applications web et offre bien d'autres services : widgets, réseaux sociaux, délégation de droits ...

Le paramétrage du module Amon permet de rendre ces services web accessibles depuis l'extérieur de

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'établissement.

Application par défaut

Si le portail Envole n'est pas installé, l'application web par défaut est Rouncube et l'adresse `http://<adresse serveur>/` pointe vers `http://<adresse serveur>/roundcube/`

Il est possible de modifier ce comportement dans l'interface de configuration du module, dans l'onglet Applications Web → Application Web par défaut (redirection).

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.

12.1. L'authentification unique avec EoleSSO

L'authentification unique

EOLE propose un mécanisme d'authentification unique par l'intermédiaire d'un serveur SSO[p.902].

Ce serveur est compatible CAS[p.885], SAML[p.901] et OpenID[p.896].

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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

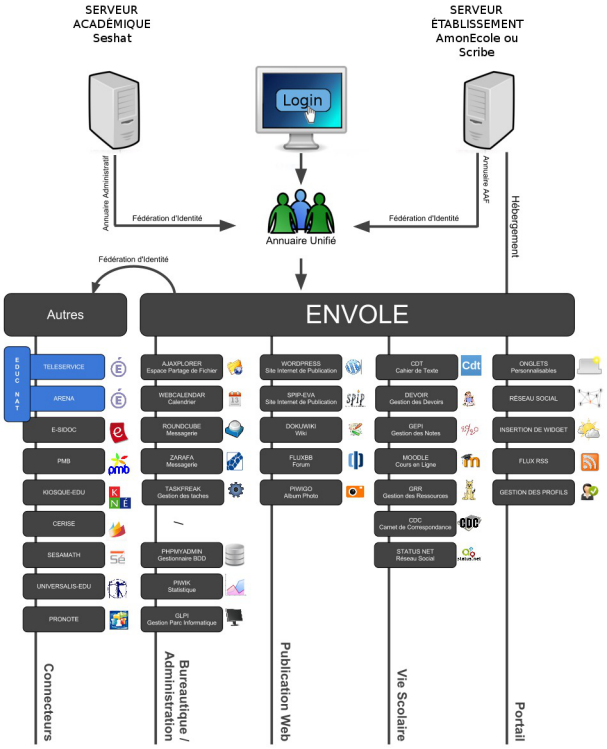
Le navigateur doit être configuré pour **accepter les cookies**.

12.2. Espace Numérique Personnel pour l'Éducation avec Envole

Envole est un Espace Numérique Personnel[p.889] pour l'Éducation.

Il propose une interface de type portail Web 2.0[p.904] 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 ...

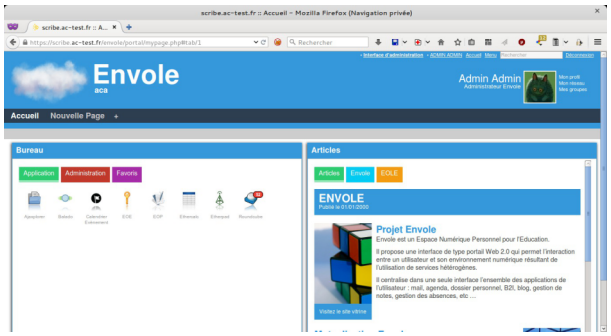


Panorama d'Envole

Envole est adapté pour mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Établissement (PIE) ou un Espace Numérique de Travail (ENT).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Envole est personnalisable par l'administrateur (changer le thème, imposer des onglets et des widgets, concevoir des widgets) et par l'utilisateur (ajouter des onglets et des boutons, gérer ses marque-pages, utiliser des widgets).



Portail et Bureau d'accès rapide aux applications

Le site de la mutualisation interacadémique : http://envole.ac-dijon.fr

Le site de l'ENT Envole : http://www.ent-envole.com

Historique du projet

- Envole 1 a été créé par l'académie de Créteil pour construire sa solution ENT : Cartable en ligne.

  À la demande du Ministère de l'Éducation nationale, les différentes évolutions ont permis la sortie d'une version 1.5 permettant l'utilisation d'Envole dans d'autres académies. Envole 1.5 est monolithique (modularité réduite) et n'évoluera plus (produit non porté sur EOLE 2.3).
- Envole 2.0 (pour web 2.0) est un projet mutualisé entre les académies de Créteil et de Dijon. Cette version est modulaire et propose de nouvelles applications web.
- Envole 3 correspond à la version d'Envole diffusée avec EOLE 2.3. Cette version propose de nouvelles applications web. Elle est le résultat de la mutualisation entre les académies d'Aix-Marseille, de Besançon, de Créteil, de Dijon, de La Réunion, d'Orléans-Tours, de Poitiers et de Reims.
- Envole 4 correspond à la version d'Envole diffusée avec EOLE 2.4 (à partir de la version 2.4.2). Cette version propose de nouvelles applications web. Elle est le résultat de la mutualisation entre les académies d'Aix-Marseille, de Besançon, de Créteil, de Dijon, de La Réunion, d'Orléans-Tours, de Poitiers, de Caen, de Grenoble, de Nice et de Reims.
- Envole 5 correspond à la version d'Envole diffusée avec EOLE 2.5 (à partir de la version 2.5.2). Cette nouvelle version s'appuie sur une version plus récente de PHP nécessaire pour le fonctionnement des dernières versions des applications web proposées.
- Envole 6 correspond à la version d'Envole diffusée avec EOLE 2.6 (à partir de la version 2.6.1).
- Envole 7 correspond à la version d'Envole diffusée avec EOLE 2.7 (à partir de la version 2.7.1).

Le pôle EOLE est chargé de sa diffusion et participe à l'élaboration de la solution, en particulier sur les aspects annuaire LDAP et authentification SSO.

Principes de fonctionnement

L'authentification

Pour l'authentification des utilisateurs, Envole utilise un serveur SSO[p.902].

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 intégrées dans le

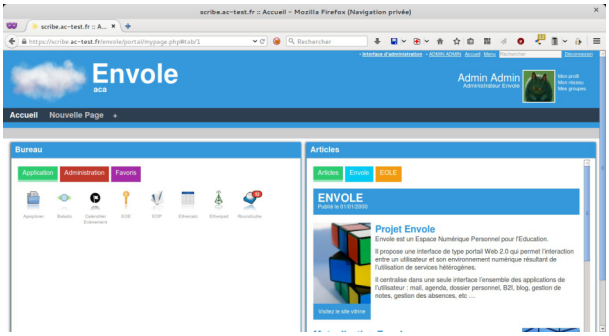
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

portail sans avoir à se ré-identifier sur chacune d'entre-elles. Les applications web pré-configurées disponibles sur le module Scribe utilisent ce serveur SSO pour l'authentification. Lors de la phase d'authentification celui-ci renvoie des informations sur l'utilisateur, ce qui permet, par le biais d'un système de profils, de personnaliser le portail.

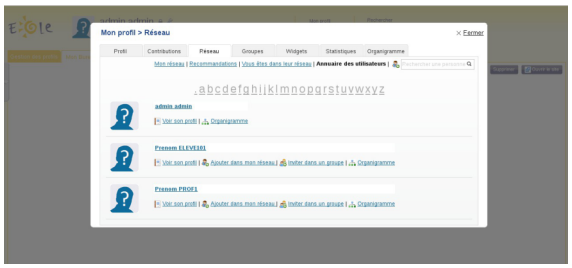
Le portail

Historiquement basé sur le logiciel POSH (http://sourceforge.net/projects/posh), le portail Envole propose :

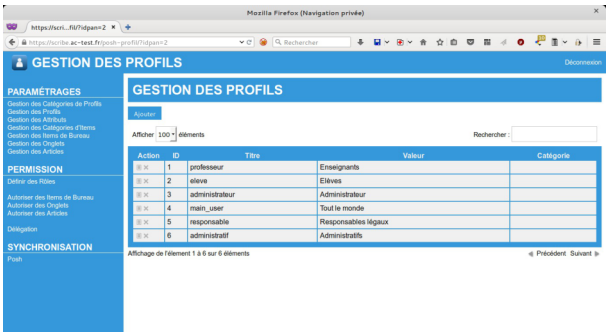
- un système d'onglet pour organiser ses applications ;
- un bureau d'accès rapides aux applications ;
- des widgets pour la gestion du flux d'informations ;
- un réseau social ;
- la gestion des profils (onglet, bureau) permettant de personnaliser l'environnement des utilisateurs ;
- un espace d'administration.



Portail et Bureau d'accès rapide aux applications

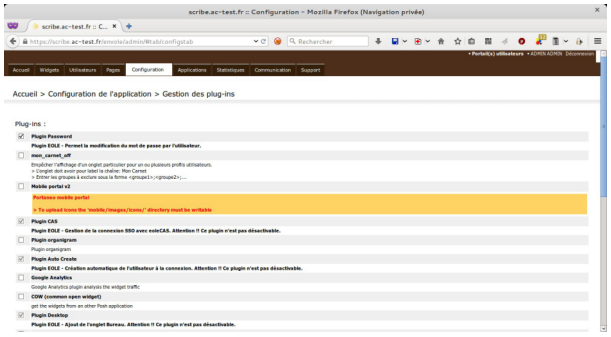


Réseau social du portail Envole



Gestion des profils

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Espace d'administration

12.2.1. Installation et paramétrage

La mise en place du portail Envole se décompose comme suit :

- installation du portail Envole ;
- activation du service SSO ;
- configuration de l'authentification CAS ;
- paramétrage du portail Envole ;
- sélection des applications web pré-configurées ;
- configuration pour un accès extérieur.

Ces différentes étapes se font à partir de l'interface de configuration du module.

Installation du portail Envole

Envole s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-posh
```

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
```

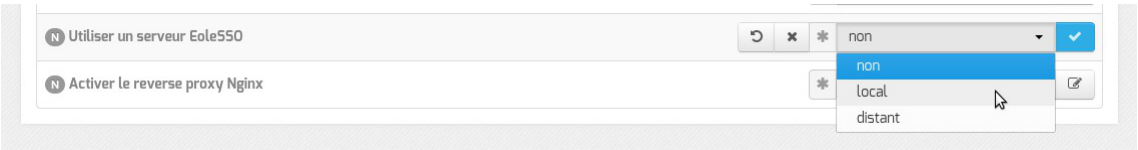
```
# service apache2 reload
```

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 `Applications web`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

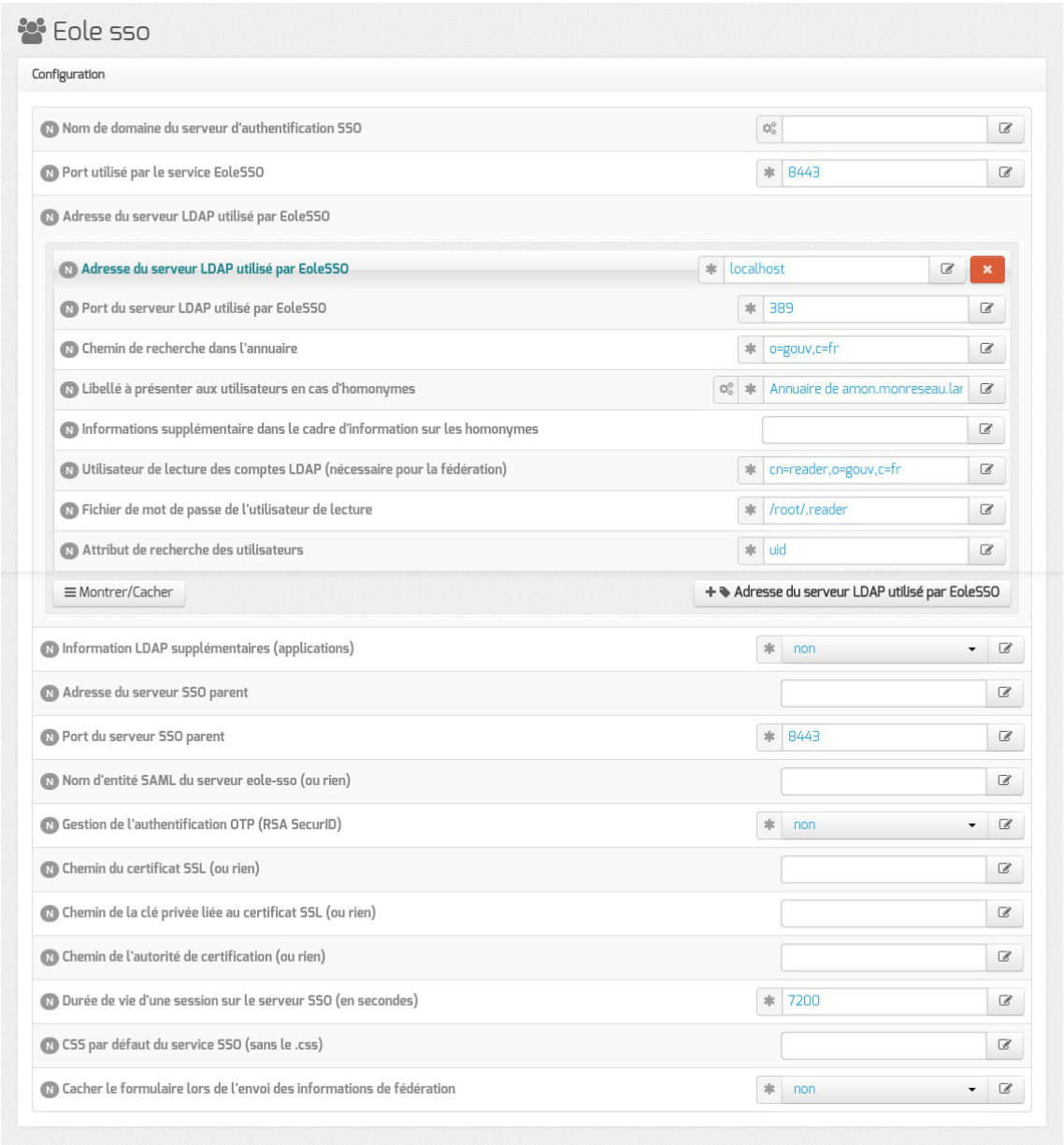
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Activation du serveur EoleSSO



Dans l'onglet `Services`,vérifier que `Utiliser un serveur EoleSSO` est bien configuré en `local` (ou en `distant` selon l'architecture cible envisagée).

Configuration de l'authentification CAS



Configuration d'un serveur EoleSSO local

Indiquer le chemin permettant aux applications web de rediriger les utilisateurs vers la mire en cas de connexion ou de déconnexion.

Dans l'onglet `Eole sso`, saisir le nom de domaine dans : `Nom de domaine du serveur`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

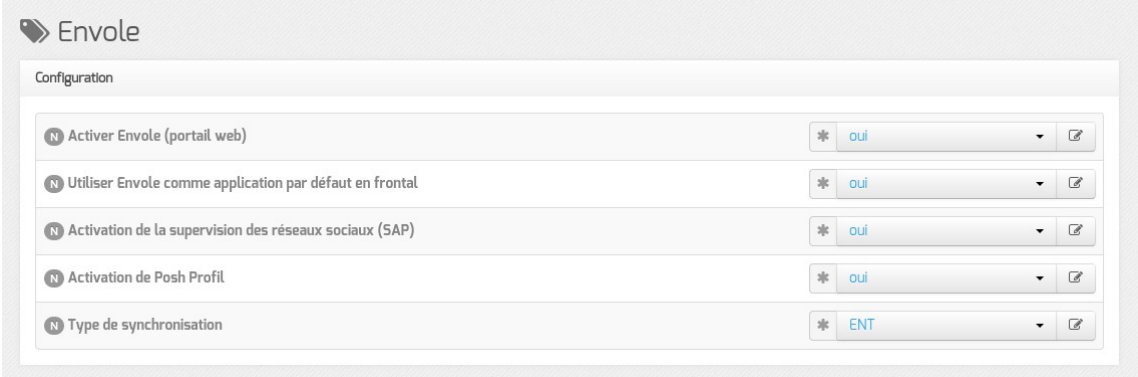
`d'authentification SSO`



Saisir une adresse IP est possible mais est incompatible avec un accès extérieur.

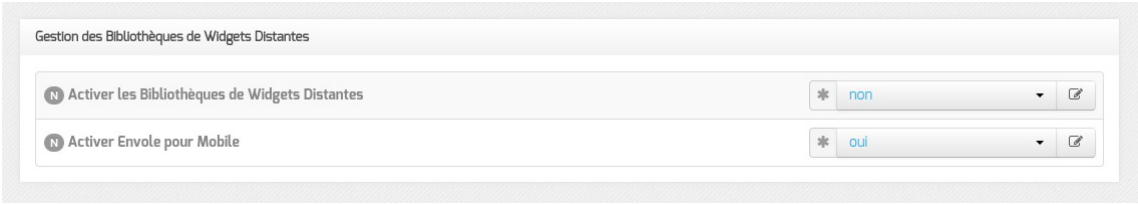
Paramétrage du portail Envole

Dans l'onglet `Envole`, vérifier que `Activer Envole (portail web)` est à `oui`.



D'autres options sont paramétrables dans cet onglet :

- Utiliser Envole ou une autre application web comme application par défaut lors de la connexion sur le port 80 ;
- Activer ou non la supervision du réseau social d'Envole (gestion des publications et des commentaires) ;
- Activer ou non la gestion des profils (Posh profil) ;
- Choisir le type de synchronisation `ENT` ou `Annuaire` ;



- Activer ou non la bibliothèque de widgets distants ;
- Activer ou non la prise en compte des périphériques mobiles (tablettes et téléphones).



Le paramétrage de l'application web par défaut dépend de l'activation du portail Envole :

- Si le portail Envole n'est pas activé ou que la variable de l'onglet `Envole` : `Utiliser Envole comme application par défaut en frontal` est à `non`, l'application web par défaut sera celle renseignée dans la variable de l'onglet `Applications web` : `Application web par défaut (redirection)`. Exemple : Si la variable `Application web par défaut` vaut `/webmail`, alors l'adresse `http://<adresse serveur>/` pointera vers `http://<adresse serveur>/webmail/` (SquirrelMail).
- Si le portail Envole est activé et que la variable de l'onglet `Envole` : `Utiliser Envole comme application par défaut en frontal` est à `oui`, l'adresse

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `http://<adresse serveur>/` renverra vers le portail.
>
> Toute modification nécessitera une reconfiguration du serveur avec la commande `reconfigure`.

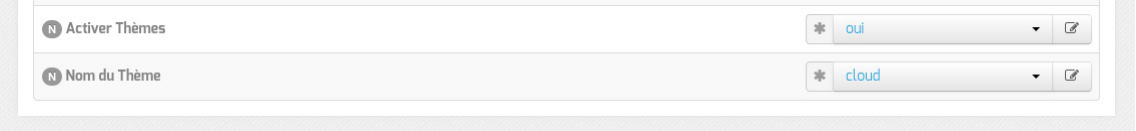
Configuration du serveur web



Dans l'onglet `Application web` :

- `Nom de domaine des applications web (sans http://)` renseigner le nom de domaine avec lequel vous souhaitez accéder à votre portail ;

  Saisir une adresse IP est possible mais est incompatible avec un accès extérieur.
- l'application web par défaut n'est disponible que si la variable `Utiliser Envole comme application par défaut en frontal` est à non dans l'onglet `Envole` ;
- préciser si le serveur web est derrière un proxy inverse et saisir son adresse IP (généralement l'adresse IP du module Amon sur la zone), cela permet d'obtenir les adresses IP sources dans les journaux au lieu de l'adresse IP du proxy inverse, cela permet également de mettre en place correctement certaines restrictions sur les applications web. En contrepartie la déclaration du proxy inverse ajoute une entête qui contient une adresse IP qui peut être falsifiée depuis la machine source ;
- pour gérer les bases de données via l'application web phpMyAdmin passer `Activer phpMyAdmin` à `oui`.

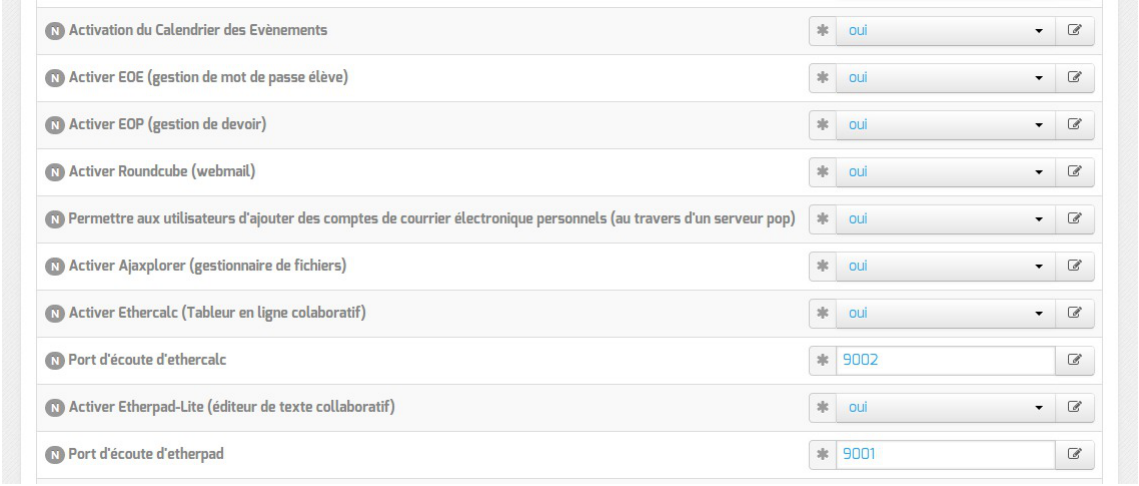


Envole thème est installé par défaut avec Envole et gère les thèmes de certaines applications web, de l'EAD et de la mire SSO. Il est possible de choisir parmi une liste de thèmes ou de désactiver Envole thème.

Sélection des applications web

Toujours dans l'onglet `Applications web`, choisir les applications à activer en les passant à `oui`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'onglet "Applications web"

Chaque application est documentée séparément, référez-vous à chacune d'entre-elles pour plus d'informations (installation, accessibilité, rôles des utilisateurs, etc).

Certaines applications, comme les gestionnaires de fichiers en ligne, nécessitent l'activation de l'accès FTP.

Depuis l'interface de configuration du module, dans l'onglet `Services` vérifier que `Activer l'accès FTP` est à `oui`.

12.2.2. Accès au portail

Une fois installé, si Envole est configuré pour être en frontal il est accessible à l'adresse `http://<adresse_serveur>/` sinon à l'adresse `http://<adresse_serveur>/envole/`

Accès interne

Pour un accès interne, vous pouvez accéder au portail :

- par le nom de machine ;
- par l'adresse IP ;
- par le nom de domaine si l'accès extérieur est configuré.

Accès externe

Pour un accès externe, vous pouvez accéder au portail :

- par le nom de domaine.

Le serveur Amon doit être configuré pour permettre l'accès depuis l'extérieur.

Rôles des utilisateurs

Les comptes d'accès à Envole sont ceux de l'annuaire défini dans l'interface de configuration du module.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Seul l'utilisateur `admin` est l'administrateur du portail.

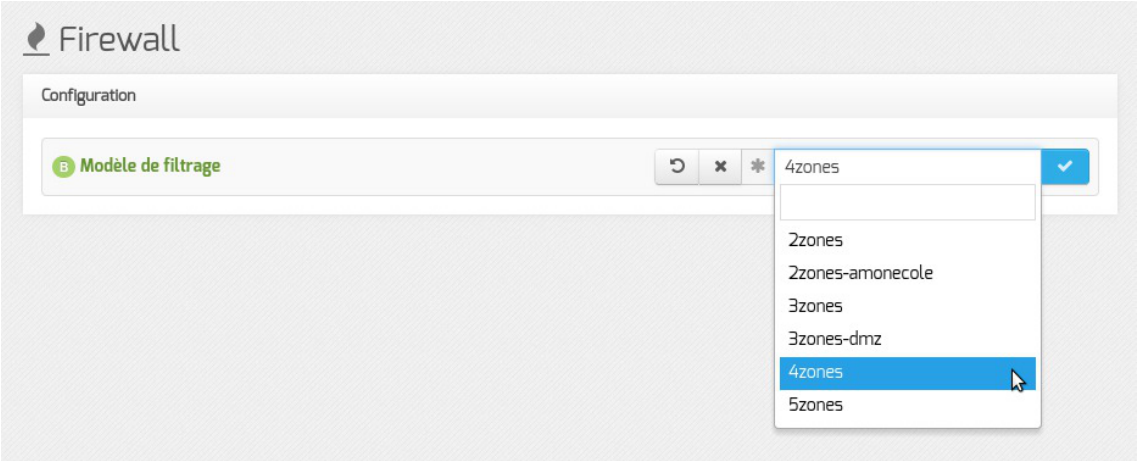
Il est possible de déléguer ce rôle dans l'interface d'`administration du portail / utilisateurs / gestion des utilisateurs`, cliquer sur le compte utilisateur choisi et passer champ `Type d'utilisateur` à `administrateur`.

12.2.2.a. Configurer le module Amon pour Envole

Configurer le pare-feu

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet `Firewall`, choisir un `Modèle de filtrage` compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.



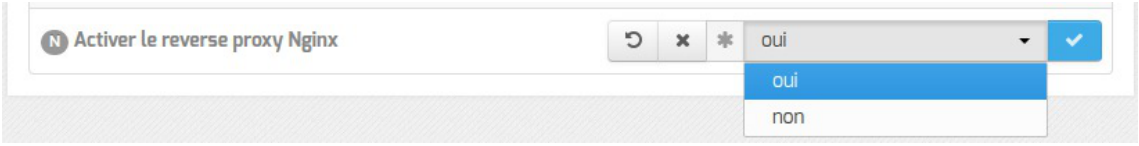
Le modèle de zone proposés correspondent à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Configuration du proxy inverse

Pour activer le proxy inverse, dans `Services`, passer `Activer le reverse proxy Nginx` à `oui`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

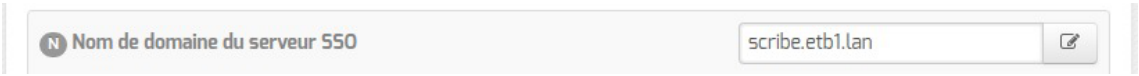


L'activation du service fait apparaître un nouvel onglet nommé `Reverse proxy`.



Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

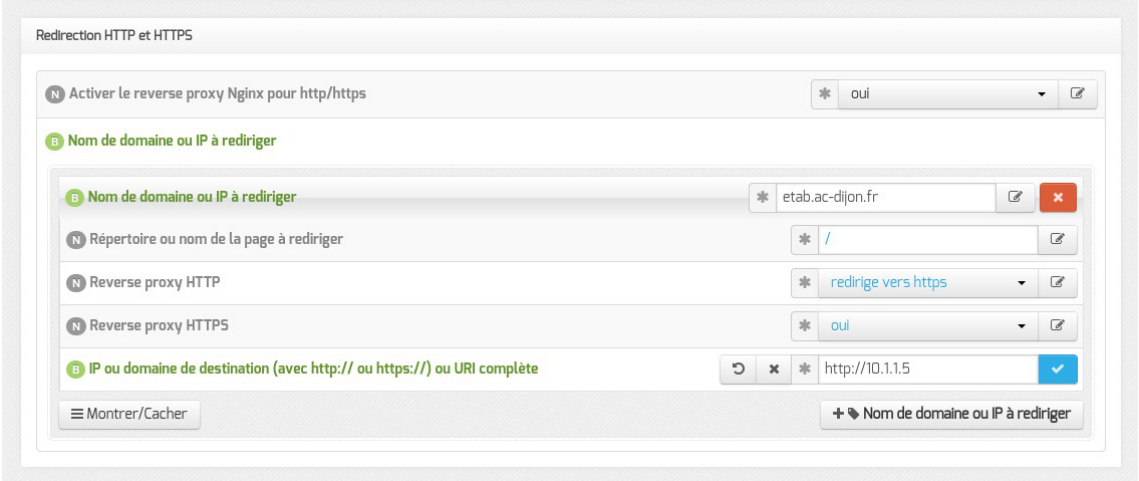


Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.



Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

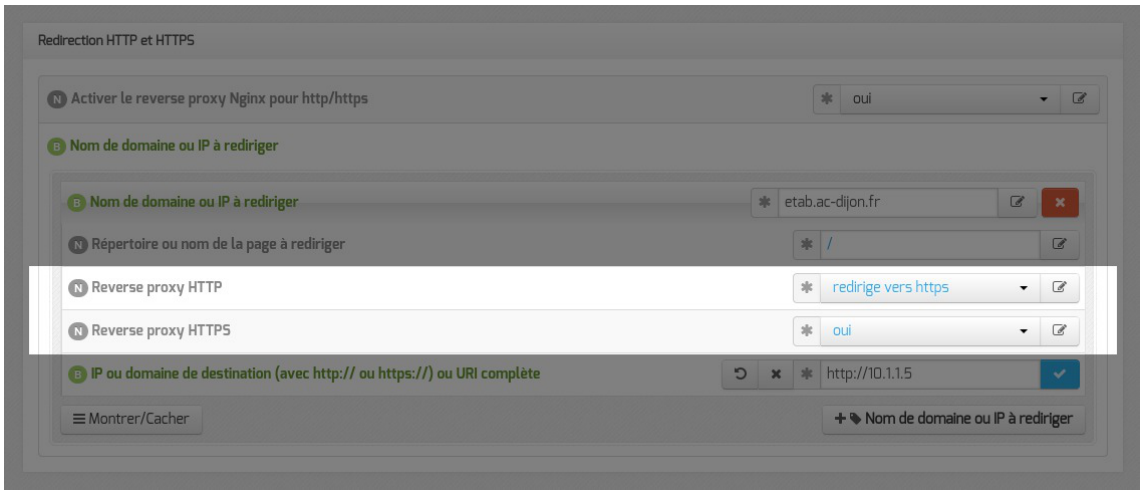
Redirection HTTP et HTTPS



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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est `/` ;
- l'`IP ou domaine de destination (avec http:// ou https://) ou URI complète` permet de saisir l'adresse IP (exemple : `http://192.168.10.1`), le nom de domaine (exemple : `http://scribe.monetab.fr`) ou l'URI[p.904] (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`.

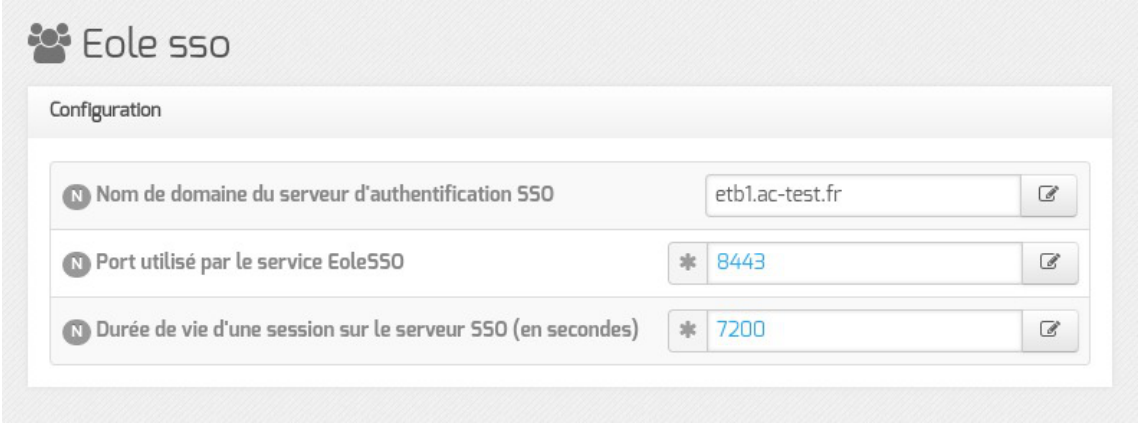
Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `Nom de domaine ou IP à rediriger`.

> Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.898], `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).

Activation de l'authentification unique

Si vous voulez activer le service EoleSSO sur le module Amon, `Utiliser un serveur EoleSSO à distant` dans l'onglet `Services`, dans l'onglet `Eole sso`, 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Configuration d'un serveur EoleSSO distant

L'option `Nom de domaine du serveur d'authentification SSO` doit être configurée avec le nom de domaine public utilisé dans Envole (typiquement : *monetab.ac-monacad.fr*).

Dans ce cas l'utilisateur `admin` du module Scribe sera administrateur du module Amon.

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.

Nom de domaine et récapitulatif de la configuration

Le nom de domaine doit être renseigner à de multiples endroits de la configuration.

- onglet `Général` : choisir le modèle de filtrage ;
- onglet `Services` :
  - Activer le proxy inverse Nginx : `oui` ;
- onglet `Eole sso` :
  - Nom de domaine du serveur d'authentification SSO : `etab.ac-acad.fr` ;
- onglet `Applications web` si module AmonEcole :
  - Nom de domaine des applications web (sans http://) : `etab.ac-acad.fr` ;
- onglet `Reverse proxy` :
  - Nom de domaine par défaut : `etab.ac-acad.fr` ;
  - Nom de domaine du serveur SSO : `etab.ac-acad.fr` ;
  - Activer la configuration automatique pour les applications locales à `oui`.
- onglet `Certificats ssl` uniquement en mode expert :
  - Nom DNS/IP alternatif du serveur : `etab.ac-acad.fr` *(ré-générer les certificats si nécessaire)*.

Voir aussi...

Onglet Firewall

Onglet Reverse proxy : Configuration du proxy inverse

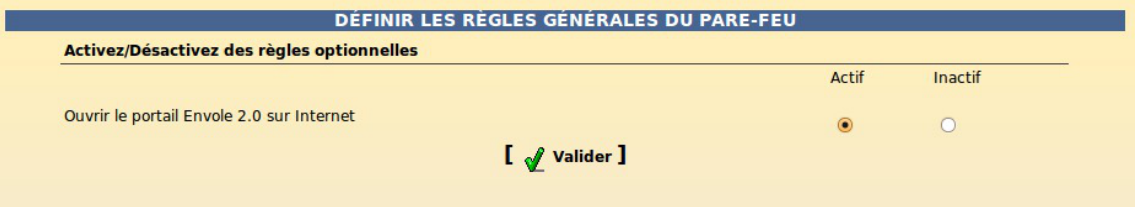
Onglet Eole sso : Configuration du service SSO pour l'authentification unique

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

ERA, éditeur de règles pour le module Amon

12.2.2.b. Activer le portail Envole dans l'EAD du module Amon

Pour activer la règle optionnelle permettant l'accès au portail depuis l'extérieur, il faut se rendre dans l'EAD du module Amon, dans `Configuration Générale` / `Règles du pare-feu`, et passer à Actif `Ouvrir le portail Envole 2.0 (Posh) sur internet` et valider.



Configuration EAD pour Envole

12.2.2.c. Configuration sans module Amon

L'onglet `EAD` du portail Envole pointe vers l'EAD du serveur Scribe sur le port 4203.

Envole est configuré par défaut pour fonctionner derrière un Amon.

Si vous souhaitez utiliser autre chose qu'un module Amon, la valeur du port est modifiable depuis l'interface de configuration du module :

En `Mode` / `Expert` onglet `Ead-web` passer `Utilisation d'un reverse proxy pour l'accès à l'EAD` à ***non*** .

12.2.3. Administration

12.2.3.a. Généralités sur la gestion des profils

Les profils

Le gestionnaire de profils permet, depuis les informations véhiculées par l'authentification SSO :

- d'imposer l'affichage d'onglets dans le portail d'un utilisateur donné ;
- de proposer des liens vers des applications depuis le `Bureau`.

Ces profils sont administrés depuis une interface de gestion de profils disponible pour l'administrateur sous la forme d'un onglet.

Les onglets

Lorsque l'utilisateur supprime un onglet qui lui est imposé depuis le gestionnaire de profil,cet onglet reviendra au rechargement de la page ou à la prochaine connexion.

Si l'onglet est retiré de son profil par l'administrateur, l'onglet restera tout de même dans son portail.

C'est l'utilisateur qui est à l'initiative de la suppression.

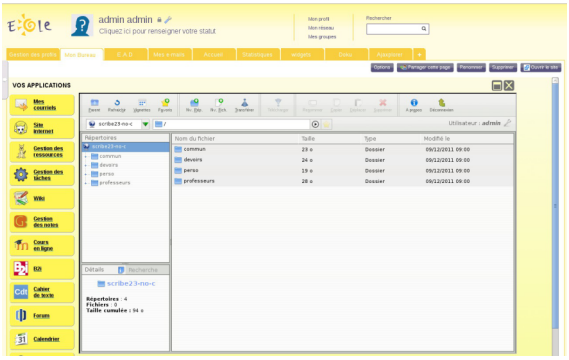
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le bureau

L'onglet `Mon Bureau` permet de configurer une liste de boutons d'accès rapides à des applications web.

Chaque bouton se définit par :

- Une icône (facultative) ;
- Une URL ;
- Un libellé.



Bureau d'accès rapide aux applications

`Mon Bureau` est un onglet, celui-ci doit donc être imposé à l'utilisateur par le biais de la gestion des profils.

La confusion est possible entre les profils du portail et ceux du gestionnaire de profil.

Des groupes de profil sont directement intégrés au portail et accessibles pour l'utilisateur `admin` depuis l'interface d'administration.

Ces groupes n'ont pas de lien avec la gestion des profils accessible depuis le portail de l'utilisateur `admin` par le biais de l'onglet `Gestion des profils`.

12.2.3.b. Gestion des profils

Le gestionnaire de profil

L'interface de gestion permet de :

- créer des éléments (items de bureau, onglets) ;
- ajouter des profils (professeur, élèves, élèves de BTS, ...) ;
- associer les profils aux éléments ;
- créer des attributs utilisateurs ;
- associer des utilisateurs à ces profils par le biais des attributs utilisateurs.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



L'interface de gestion des profils

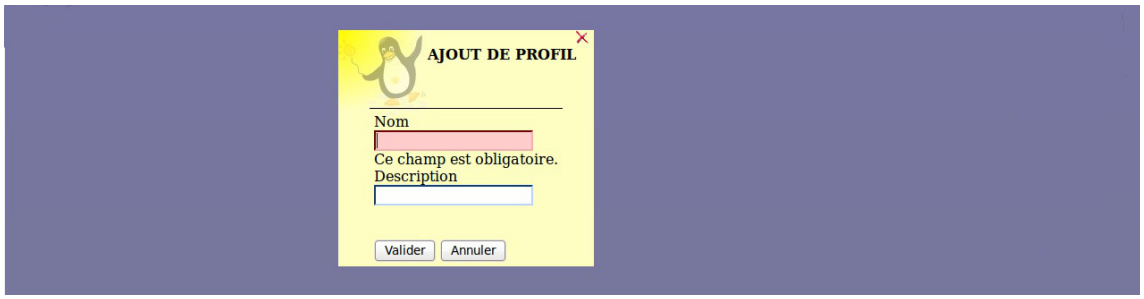
> Ajout d'un profil utilisateur

Pour ajouter un profil utilisateur :

- aller dans `Ajout de paramètres` / `Profil utilisateur` ;
- entrer le nom du profil et sa description ;
- valider.



Création d'un profil utilisateur



Ajout d'un profil utilisateur



Le nom du profil ne doit comprendre ni espace, ni caractères spéciaux.

En revanche il n'y aucune restriction pour la description.

> Créer un onglet vers des pages externes

Les onglets du portail peuvent être forcés via le gestionnaire de profils.

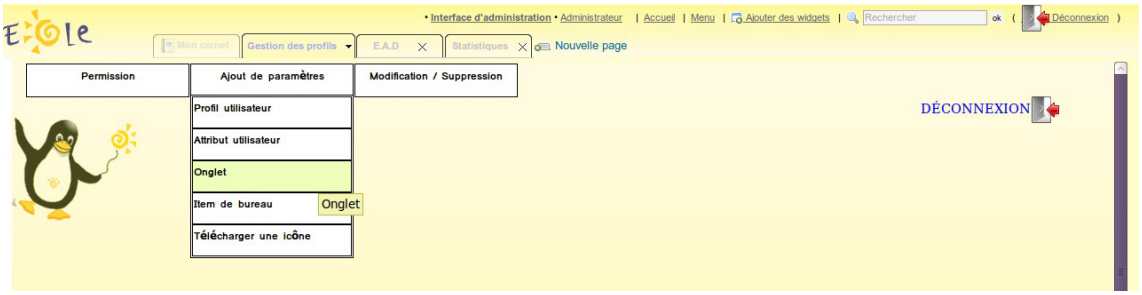
Pour ajouter un nouvel onglet :

- aller dans `Ajout de paramètres` / `Onglet` ;
- entrer un nom (unique) ;
- entrer un libellé (affiché dans le portail) ;

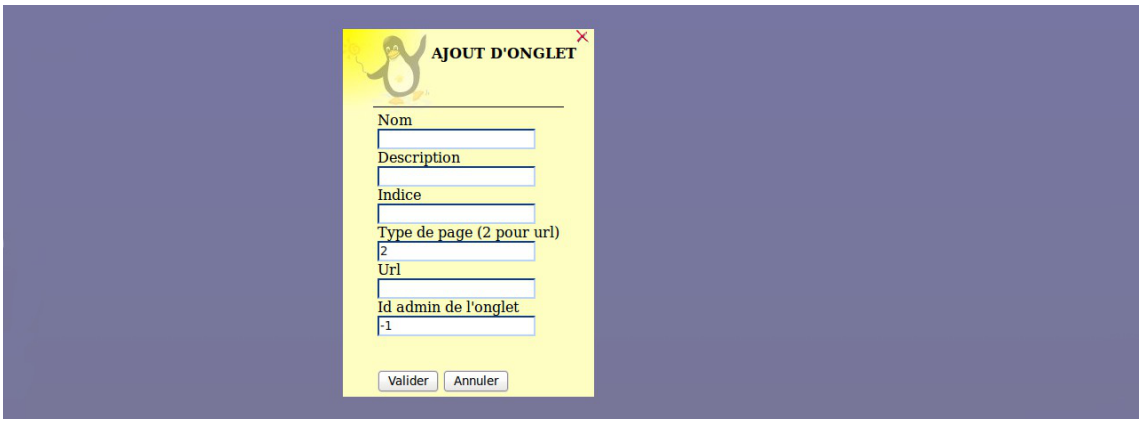
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- entrer la place de l'onglet (indice) : "1" signifie que l'onglet doit être en première place ;
- entrer le type posh de l'onglet : mettre "2" pour une URL ;
- entrer l'URL de l'application ;
- laisser le champ `Id admin de l'onglet` à "-1" ;
- valider.

L'onglet peut alors être associé à un profil.



Ajouter un onglet



Paramétrage du nouvel onglet

Les paramètres passés dans l'URL ne fonctionnent pas.

Ne pas mettre ni "? ", ni "&".

> Créer un item de bureau pour le greffon desktop du portail

Le gestionnaire de profil propose un accès rapide à des applications via un onglet nommé Mon Bureau .

Ce bureau est composé par des boutons chargeant des URL dans une fenêtre permettant un accès rapide aux applications les plus utilisées.

Pour créer un nouvel item de bureau :

- aller dans `Ajout de paramètres` / `Item de bureau` ;
- entrer un nom (unique) ;
- entrer un libellé ;
- entrer l'URL de l'application associée ;
- entrer l'URL d'une icône (facultatif) ;

L'item de bureau est alors disponible pour être associé à un profil.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Un onglet bureau doit être disponible pour l'utilisateur afin que l'on puisse lui associer des items.

Voir aussi...

Télécharger des icônes de bureau [p.667]

> Autoriser des éléments pour des profils

Les éléments (onglets , items de bureau), une fois créés, ne sont pas disponibles.

Il faut les autoriser en les associant à des profils.

Autoriser un onglet

- Aller dans Permission / Autoriser des onglets ;
- choisir le profil dans la liste déroulante ;
- choisir les onglets dans la liste de droite (garder Ctrl appuyé pour une sélection multiple) ;
- cliquer sur la flèche de transfert verte ;
- valider.

Les utilisateurs ayant le profil choisi disposeront du nouvel onglet lors du prochain affichage de leur portail (pas besoin de se reconnecter Ctrl + R suffit).

Pour enlever des onglets , la procédure est : choisir les onglets à gauche, les transférer avec la flèche rouge et valider.

Lorsque l'utilisateur supprime un onglet qui lui est imposé depuis le gestionnaire de profil,cet onglet reviendra au rechargement de la page ou à la prochaine connexion.

Si l'onglet est retiré de son profil par l'administrateur, l'onglet restera tout de même dans son portail.

C'est l'utilisateur qui est à l'initiative de la suppression.

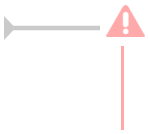
Autoriser un item de bureau

- Aller dans Permission / Autoriser des items de bureau
- choisir le profil dans la liste déroulante ;
- choisir les items de bureau dans la liste de droite (garder Ctrl appuyé pour une sélection multiple) ;
- cliquer sur la flèche de transfert verte ;
- valider.

Les utilisateurs ayant le profil choisi disposeront du nouvel item lors du prochain affichage de leur portail (pas besoin de se reconnecter Ctrl + R suffit).

Pour enlever des items de bureau, la procédure est : choisir les items à gauche, les transférer avec la flèche rouge et valider.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Un onglet `bureau` doit être disponible pour l'utilisateur afin que l'on puisse lui associer des items.

> Associer des utilisateurs à un profil

Un profil est lié à des permissions. Afin de donner accès à ces permissions pour un utilisateur donné, il faut lui associer le profil en question. L'association se fait via des attributs utilisateur.

Les attributs d'un utilisateur sont véhiculés par le portail depuis le serveur d'authentification SSO et permettent à l'utilisateur d'être finement identifié :

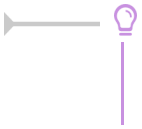
- Je suis Monsieur Dupond
- Mon typeadmin est 2 (je suis professeur)
- Le RNE de mon établissement est le 211234
- ...

Étape 1

Créer une entrée pour l'attribut utilisateur à considérer :

- aller dans `Ajout de paramètres` / `Attribut utilisateur ;`
- entrer le nom de l'attribut (typiquement une clé de l'annuaire ldap, éventuellement autre chose si vous avez configuré votre SSO pour que ces informations soient véhiculées) ex : typeadmin ;
- entrer la valeur de cet attribut, ex : "2" ;
- valider ;

Cet "attribut utilisateur" est alors disponible pour être associé à un profil.



La valeur *None* signifie "valeur quelconque". Seule la présence de la clé compte dans ce cas là.

Étape 2

Associer l'attribut utilisateur à un profil :

- aller dans `Permission` / `Définir des rôles ;`
- choisir l'attribut utilisateur ;
- choisir les profils dans la liste de droite pour les associer à cet attribut (garder `Ctrl` appuyé pour une sélection multiple) ;
- cliquer sur la flèche de transfert verte ;
- valider.

Les utilisateurs ayant l'attribut considéré (typeadmin de valeur 2 dans notre cas) auront le profil choisi (ex : professeur),

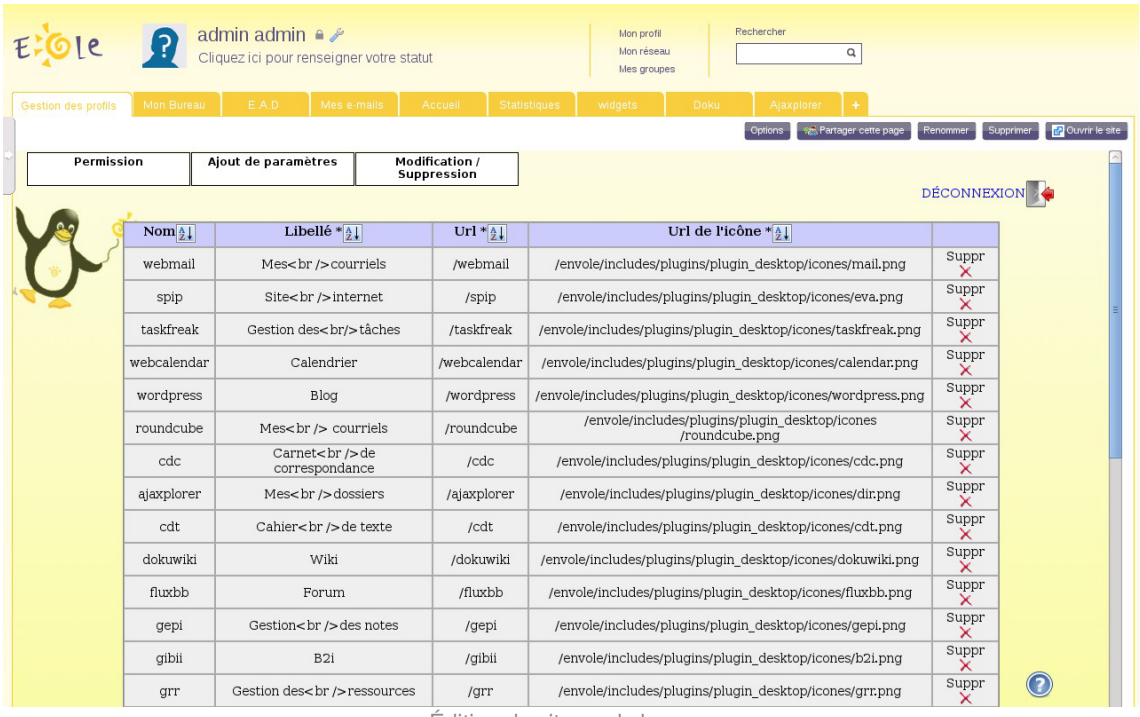
ainsi que toutes les autorisations qui vont avec (onglets et items de bureau).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour enlever un lien entre un profil et un attribut utilisateur, procédure inverse (choisir le profil dans la liste de gauche, transferer avec la flèche rouge et valider).

> Visualiser / supprimer des éléments

Il est possible de visualiser et de supprimer des éléments référencés (profil, item de bureau, onglet, attribut utilisateur).



Nom	Libellé *	Url *	Url de l'icône *	
webmail	Mes courriels	/webmail	/envole/includes/plugins/plugin_desktop/icones/mail.png	Suppr
spip	Site internet	/spip	/envole/includes/plugins/plugin_desktop/icones/eva.png	Suppr
taskfreak	Gestion des tâches	/taskfreak	/envole/includes/plugins/plugin_desktop/icones/taskfreak.png	Suppr
webcalendar	Calendrier	/webcalendar	/envole/includes/plugins/plugin_desktop/icones/calendar.png	Suppr
wordpress	Blog	/wordpress	/envole/includes/plugins/plugin_desktop/icones/wordpress.png	Suppr
roundcube	Mes courriels	/roundcube	/envole/includes/plugins/plugin_desktop/icones /roundcube.png	Suppr
cdc	Carnet de correspondance	/cdc	/envole/includes/plugins/plugin_desktop/icones/cdc.png	Suppr
ajaxplorer	Mes dossiers	/ajaxplorer	/envole/includes/plugins/plugin_desktop/icones/dir.png	Suppr
cdt	Cahier de texte	/cdt	/envole/includes/plugins/plugin_desktop/icones/cdt.png	Suppr
dokuwiki	Wiki	/dokuwiki	/envole/includes/plugins/plugin_desktop/icones/dokuwiki.png	Suppr
fluxbb	Forum	/fluxbb	/envole/includes/plugins/plugin_desktop/icones/fluxbb.png	Suppr
gepi	Gestion des notes	/gepi	/envole/includes/plugins/plugin_desktop/icones/gepi.png	Suppr
gibii	B2i	/gibii	/envole/includes/plugins/plugin_desktop/icones/b2i.png	Suppr
grr	Gestion des ressources	/grr	/envole/includes/plugins/plugin_desktop/icones/grr.png	Suppr

Édition des items de bureau

Depuis le menu `Modification/Suppression :`

- choisir le type d'élément ;
- un tableau liste les éléments de ce type, il est possible de les supprimer grâce à la croix.

> Télécharger des icônes de bureau

Il est possible d'ajouter des icônes pour illustrer vos items de bureau.

Ces icônes sont chargées sur le serveur et sont ensuite disponibles en accès web.

- aller dans `Ajout de paramètres` / `Télécharger une icône ;`
- sélectionner votre fichier à télécharger ;
- rentrer un éventuel nouveau nom ;
- télécharger ;
- l'icône se trouve désormais dans la liste et a été redimensionnée au format 32x32.



Si vous renommez votre fichier image, vous devez impérativement lui mettre une extension faisant partie des types connus (.jpg ,*.png ,*.ico ,*.gif, ...).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Copiez l'URL de l'image et collez-là dans la configuration de votre item de bureau.

Pour supprimer une icône :

- aller dans `Ajout de paramètres` / `Télécharger une icône` ;
- cliquer sur le bouton de suppression correspondant.

12.2.3.j. Nouvelle gestion des profils

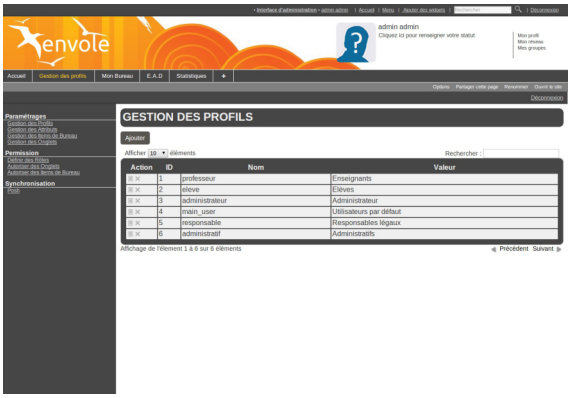
La nouvelle gestion des profils propose une nouvelle interface plus souple, plus ergonomique et plus esthétique. Elle n'utilise plus les services `posh-profil` et `admin-posh-profile`.

La nouvelles gestion des profils permet une synchronisation des comptes utilisateurs, celle-ci permet de ne plus attendre la première connexion de l'utilisateur pour voir apparaître son compte dans une application donnée.

Cette synchronisation permet également :

- de bénéficier des possibilités de partage de page par groupe utilisateur dans le portail ;
- d'avoir l'intégralité des utilisateurs déjà créés dans le portail ;
- de purger les groupes / utilisateurs obsolètes.

Une synchronisation dans WordPress permet également de déterminer à l'avance qui sera lié à une instance de blog et avec quel permission.



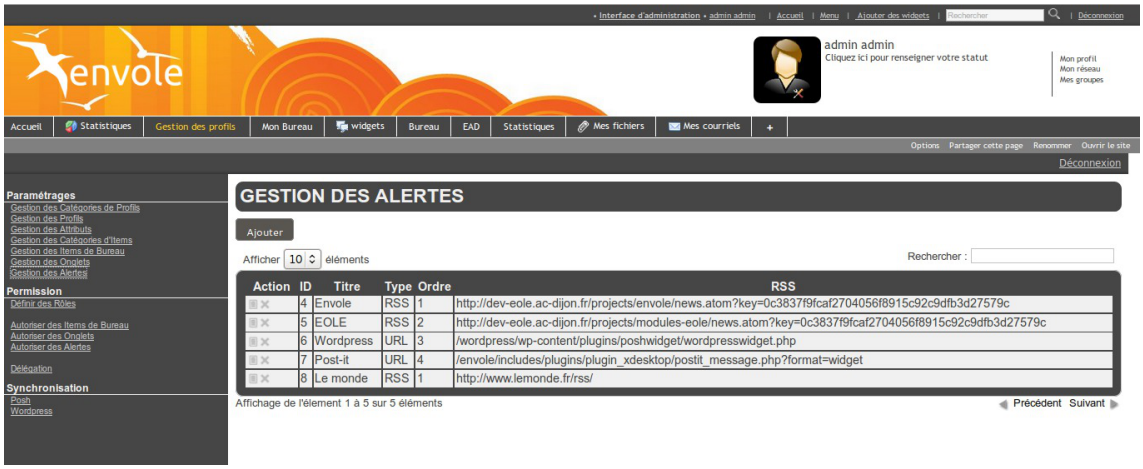
L'interface de gestion des profils

Dans la gestion des profiles il est possible de visualiser et de supprimer des éléments référencés (profil, item de bureau, onglet, attribut utilisateur, alerte).

Pour visualiser les éléments référencés, il faut se rendre dans la rubrique `Paramétrages` et choisir l'élément voulu :

- `Gestion des Profils` ;
- `Gestion des Onglets` ;
- `Gestion des Alertes` ;
- etc.

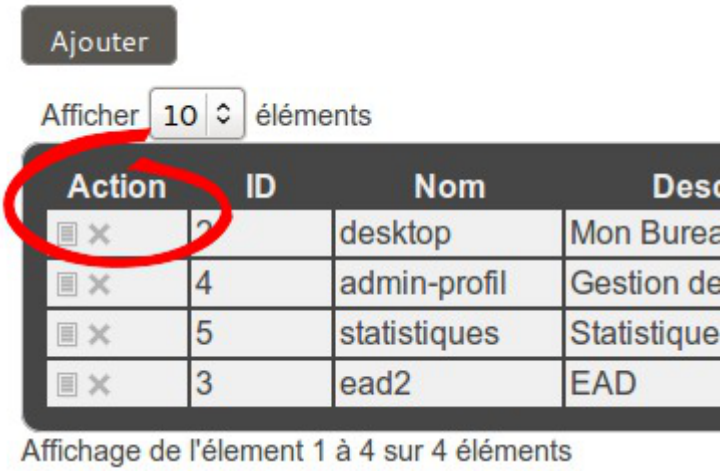
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Gestion des Alertes

Caractéristiques de l'interface :

- les champs obligatoires sont signalés par une `*` ;
- chaque liste d'élément propose des actions (modifier, supprimer) qui peuvent être différentes selon le contexte.

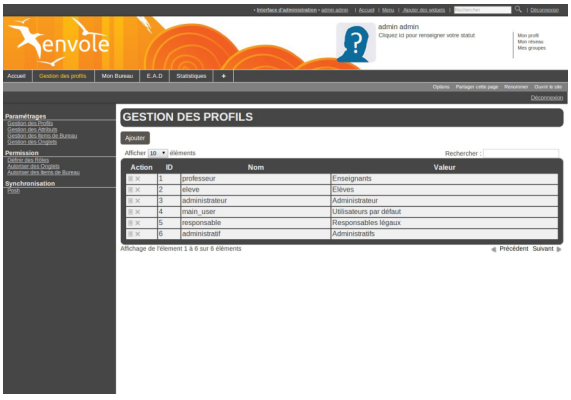


Actions modifier et supprimer

> Ajout d'un profil utilisateur

Pour ajouter un profil utilisateur :

- aller dans `Paramétrage` / `Gestion des Profil`

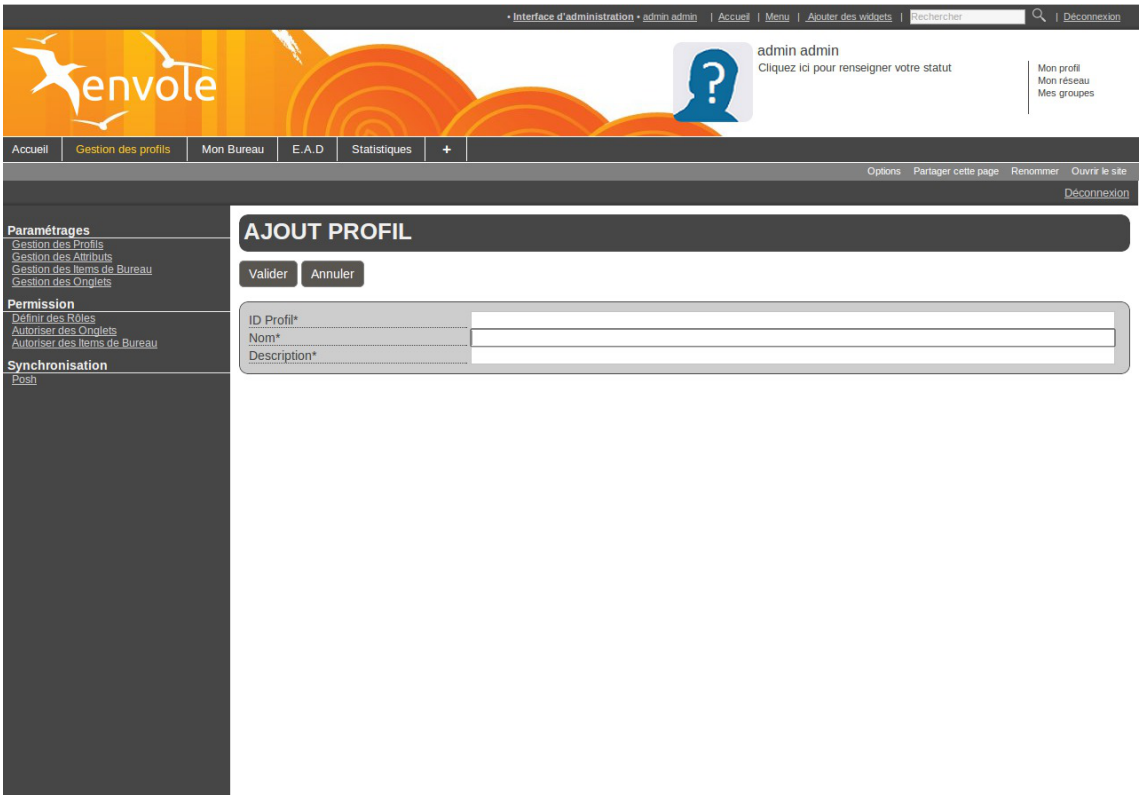


L'interface de gestion des profils

- puis cliquer sur `Ajouter` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

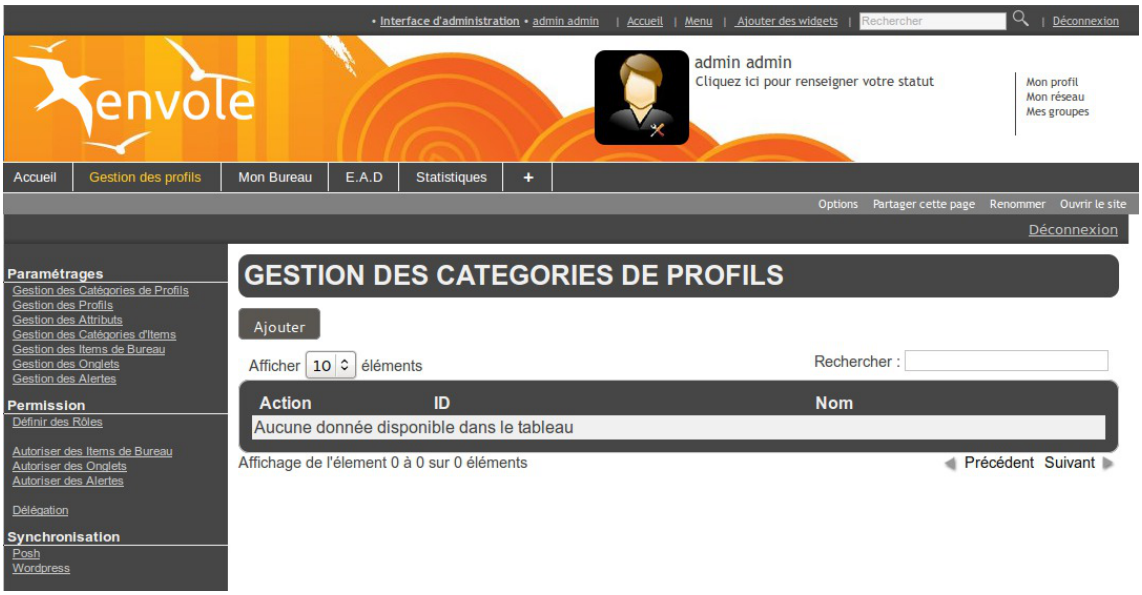
- entrer le nom du profil, sa description et choisissez une catégorie existante ;
- cliquer sur Valider.



Création d'un profil utilisateur

Le nom du profil et la description ne doivent pas comprendre d'apostrophe.

Pour ajouter, modifier, supprimer une nouvelle catégorie il faut se rendre dans Paramétrage / Gestion des Catégories de Profils.



Gestion des catégories de profils

> Associer des utilisateurs à un profil

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Un profil est lié à un rôle lui même lié à des permissions. Afin d'affecter un rôle à une utilisateur donnée il faut associer un profil à un attribut de l'annuaire LDAP. L'association se fait via la valeur que renvoie l'attribut d'un utilisateur donné.

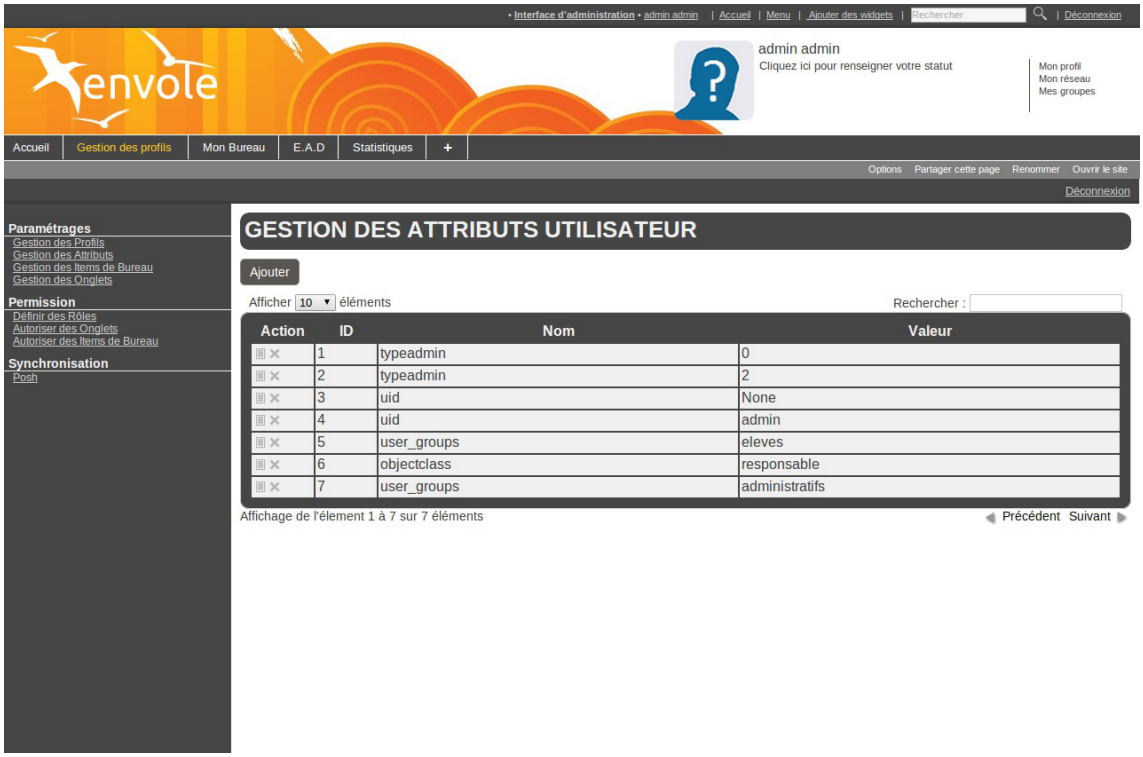
Les attributs d'un utilisateur sont véhiculés par le portail depuis le serveur d'authentification SSO et permettent à l'utilisateur d'être finement identifié :

- Je suis Monsieur Dupond
- Mon typeadmin est 2 (je suis professeur)
- Le RNE[p.900] de mon établissement est le 211234
- ...

Création d'un attribut

Créer une entrée pour l'attribut utilisateur à considérer :

- aller dans `Paramètrages` / `Gestion des attributs` ;



Gestion des Attributs

- cliquer sur `Ajouter` ;
- saisir le nom de l'attribut (typiquement une clé de l'annuaire LDAP, éventuellement autre chose si vous avez configuré votre serveur SSO pour que ces informations soient véhiculées) ;
- saisir la valeur de cet attribut ;
- cliquer sur `Valider` ;

Cet attribut utilisateur est alors disponible pour être associé à un profil.

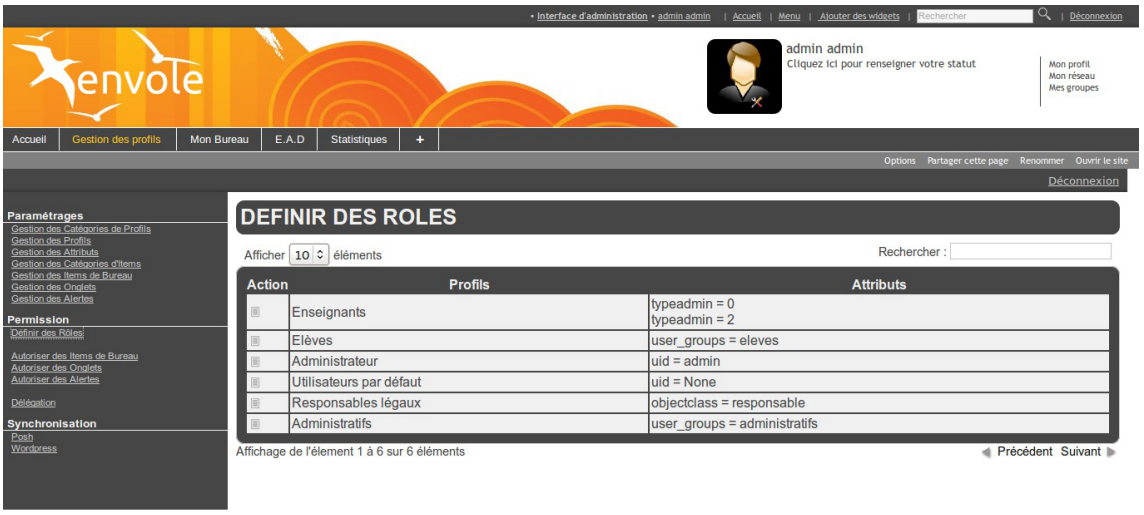
Nom : `typeadmin` ;

Valeur : `2` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La valeur `None` peut être utilisée et signifie que seule la présence de la clé validera validera l'identification et ce sans tenir compte de la valeur de l'attribut.

Définir des rôles



Définir des rôles

Associer l'attribut utilisateur à un profil :

- aller dans `Permission` / `Définir des rôles` ;
- choisir le profil et cliquer sur l'icône modifier de la colonne `Action` ;



Un nouvel écran présente les propriétés du profil sélectionné et une liste d'attributs. Il est possible d'ajouter et de supprimer des attributs. La suppression d'attribut se fait en cliquant sur le bouton supprimer dans la colonne action. Pour ajouter un ou des attributs.

- cliquer sur le bouton `Ajouter` dans `Liste des Attributs` ;
- dans le nouvel écran il faut cliquer sur le bouton ajouter de la colonne action correspondant à la ligne de l'attribut sélectionner ;
- de retour sur l'écran précédent il ne faut pas oublier de cliquer sur le bouton `Valider` en haut de page.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les utilisateurs ayant l'attribut considéré (typeadmin de valeur 2 dans notre cas) auront le profil choisi (ex : professeur), ainsi que toutes les autorisations qui vont avec (onglets et items de bureau).

Si un profil est lié à plusieurs attributs, un opérateur OU est appliqué.

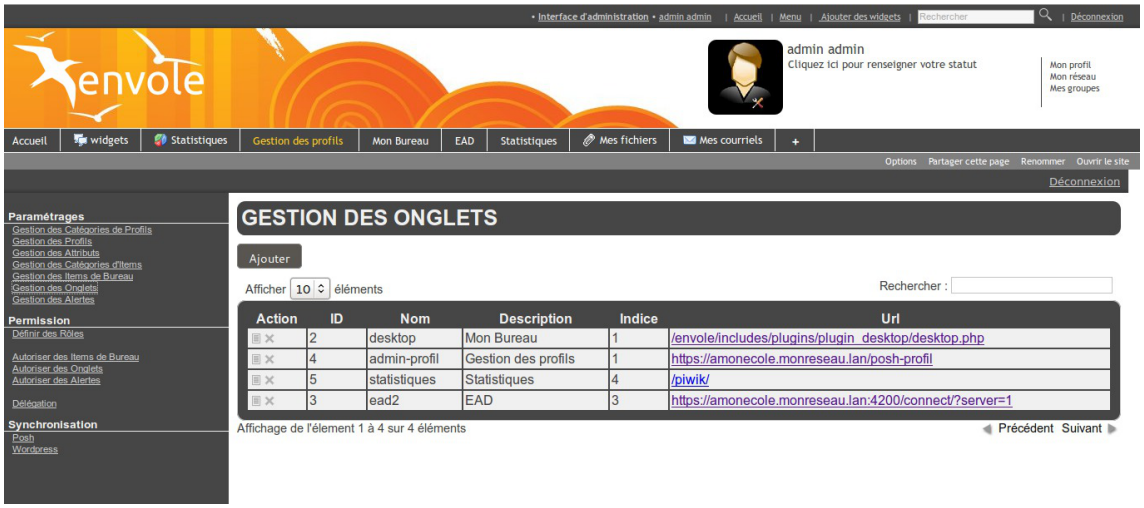
Par exemple un enseignant dans la copie d'écran ci-dessous aura un attribut `typeadmin = 0` OU `typeadmin = 2`

> Créer un onglet vers des pages externes

Les onglets du portail peuvent être forcés via le gestionnaire de profils.

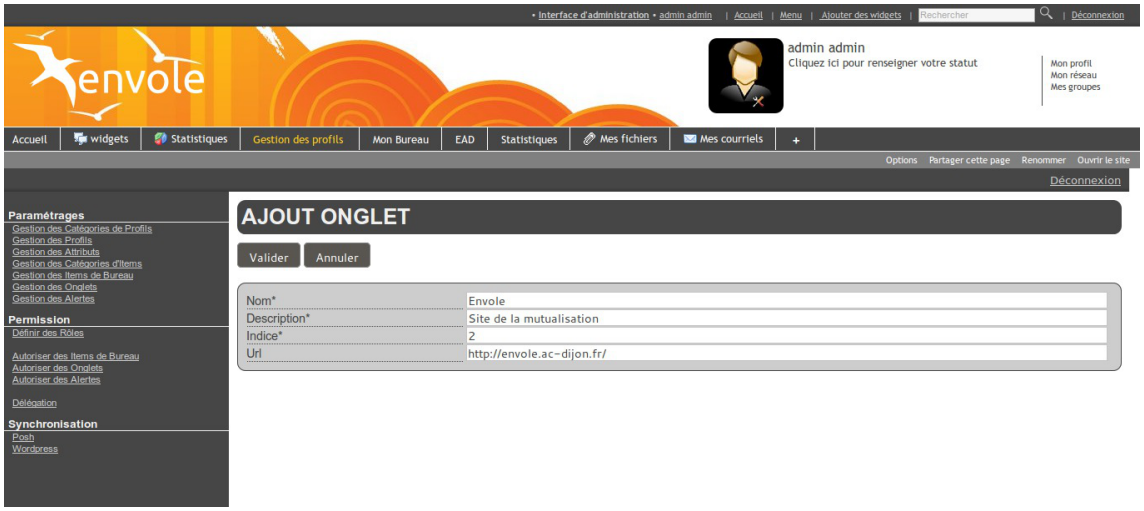
Pour ajouter un nouvel onglet :

- aller dans `Paramétrages` / `Gestion des Onglets` ;



Gestion des Onglets

- cliquer sur `Ajouter` ;



Ajouter un onglet

- entrer un `Nom` ;
- entrer une `Description` (affiché dans le portail) ;
- entrer l'`Indice` (la place de l'onglet) : la valeur `1` signifie que l'onglet doit être en première place ;
- entrer l'`URL` de l'application ;
- cliquer sur `Valider`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'onglet peut maintenant être associé à un profil.

Pour associer un onglet à un profil il faut se rendre dans la partie `Permission` / `Autoriser des Onglets`.



Il faut alors cliquer sur l'action modifier du profil choisi.



Cliquer sur le bouton `Ajouter` dans la partie `Liste des Onglets` pour voir s'afficher la liste des onglets disponibles.

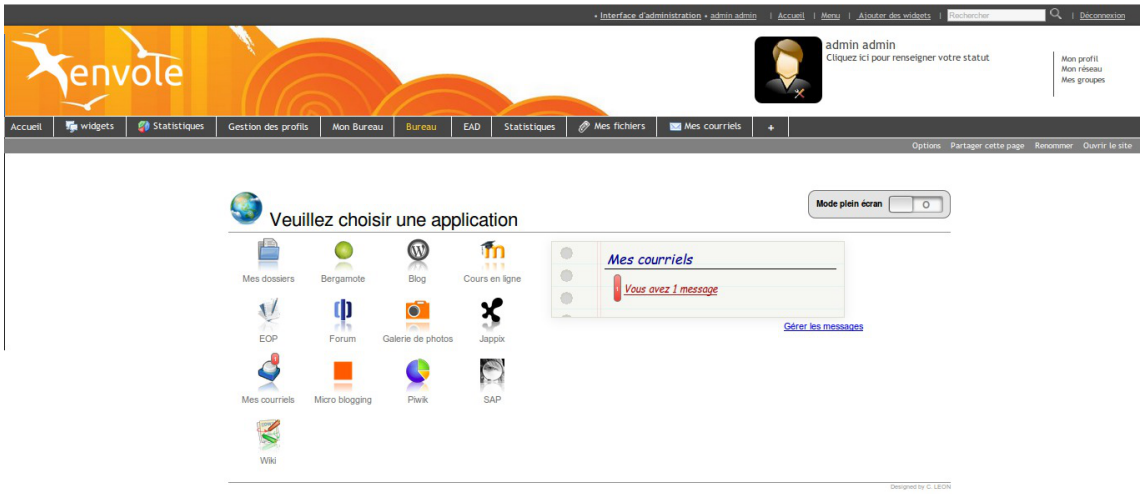
Il suffit de cliquer sur l'action `+` pour ajouter les onglets et de valider en cliquant sur le bouton `Fermer`.

> Créer un item de bureau pour le greffon Xdesktop du portail

Le gestionnaire de profil propose un accès rapide à des applications via un onglet nommé Mon Bureau .

Ce bureau est composé par des boutons chargeant des URL dans une fenêtre permettant un accès rapide aux applications les plus utilisées.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

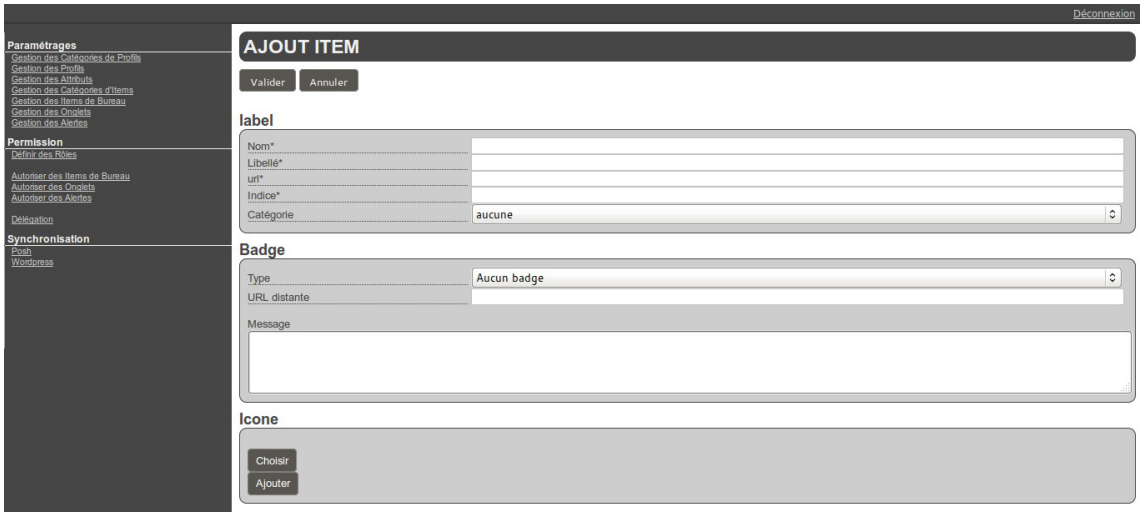


Vue du greffon xDesktop

Un certain nombre d'items sont pré-paramétrés pour les applications disponibles dans Envole.

La création d'un nouvel item de bureau se fait dans la `Gestion des Profils` :

- aller dans `Paramétrages` / `Gestion des Items de Bureau` ;
- cliquer sur le bouton `Ajouter` ;



Ajouter un item

Dans la section `Label` :

- saisir un `Nom` ;
- saisir un `Libellé` ;
- saisir l'URL de l'application à associer ;
- choisir l'`Indice` de l'item (détermine la place de l'icône sur le Bureau) ;
- choisir une `Catégorie` dans la liste déroulante (facultatif) ;

Le choix d'un badge est facultatif, cela permet de gérer (comme Roundcube par exemple), une remontée d'information en surimpression sur l'icône du bureau. Cette méthode permet également de mettre en avant une nouvelle icône en choisissant le type de badge `Nouveau`.

Dans la section `Badge` :

- choisir le `Type` de badge ;
- saisir l'URL distante ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- saisir le `Message` (texte apparaissant dans l'infobulle lorsque le pointeur reste sur l'icône) ;

Dans la section `Icône` :

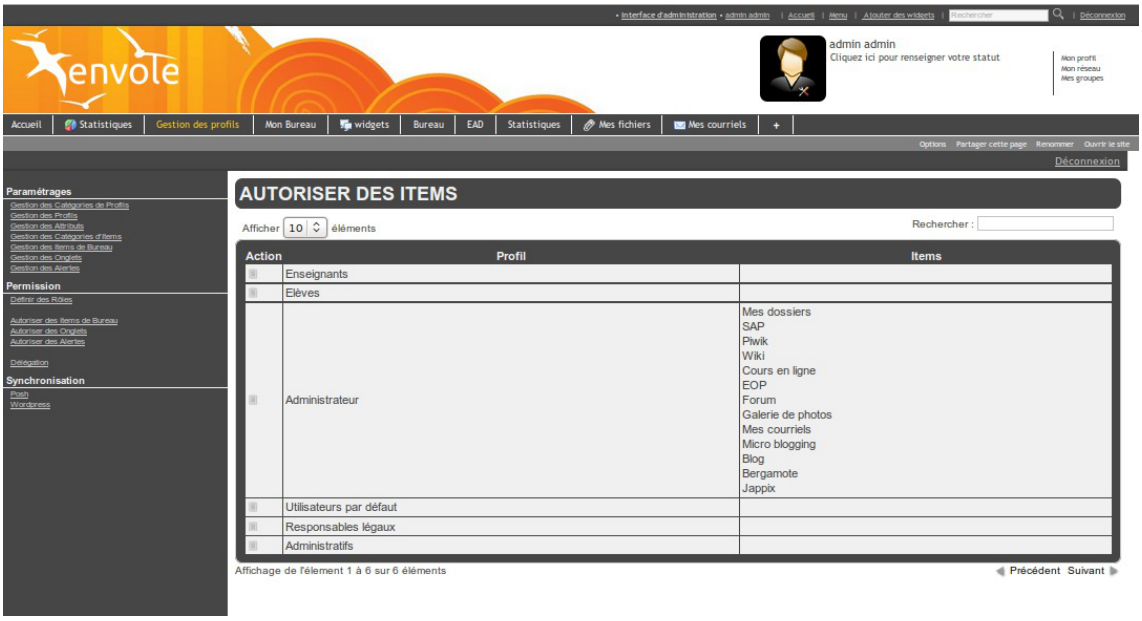
- cliquer sur `Choisir` (pour utiliser une icône existante) ou sur `Ajouter` (pour télécharger une icône ou une image depuis votre système, l'application propose la sélection d'une partie de l'image) ;

Enfin il faut valider l'ajout d'un item :

- cliquer sur le bouton `Valider` en haut de page.

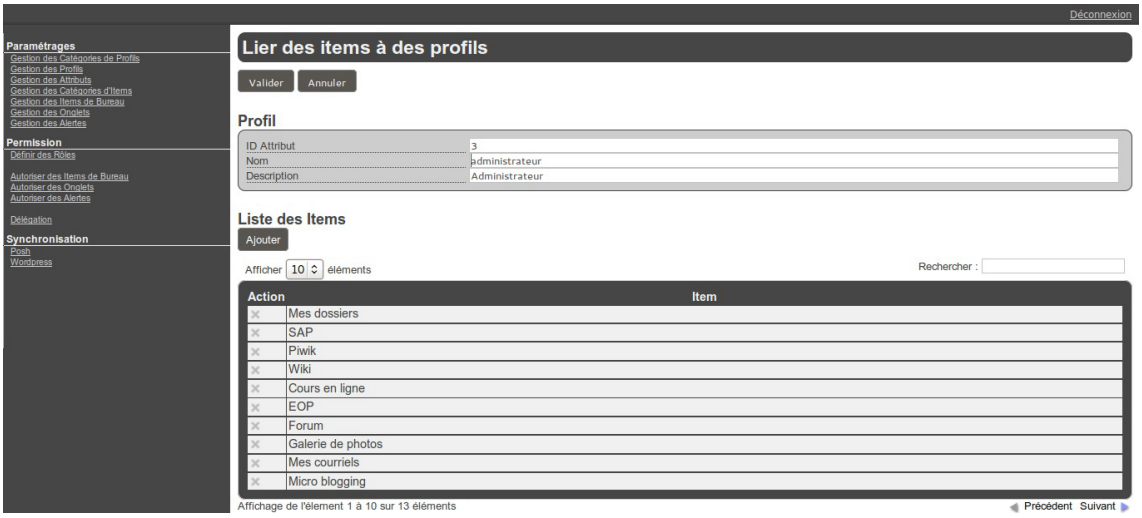
L'item de bureau est alors disponible pour être associé à un profil.

Pour associer un item de bureau à un profil il faut se rendre dans la partie `Permission` / `Autoriser des Items de Bureau`.



Autoriser des items

Il faut alors cliquer sur l'action modifier du profil choisi.



Liste des items

Cliquer sur le bouton `Ajouter` dans la partie `Liste des Items` pour voir s'afficher la liste des items disponibles.

Il suffit de cliquer sur l'action `+` pour ajouter les onglets et de valider en cliquant sur le bouton `Fermer`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

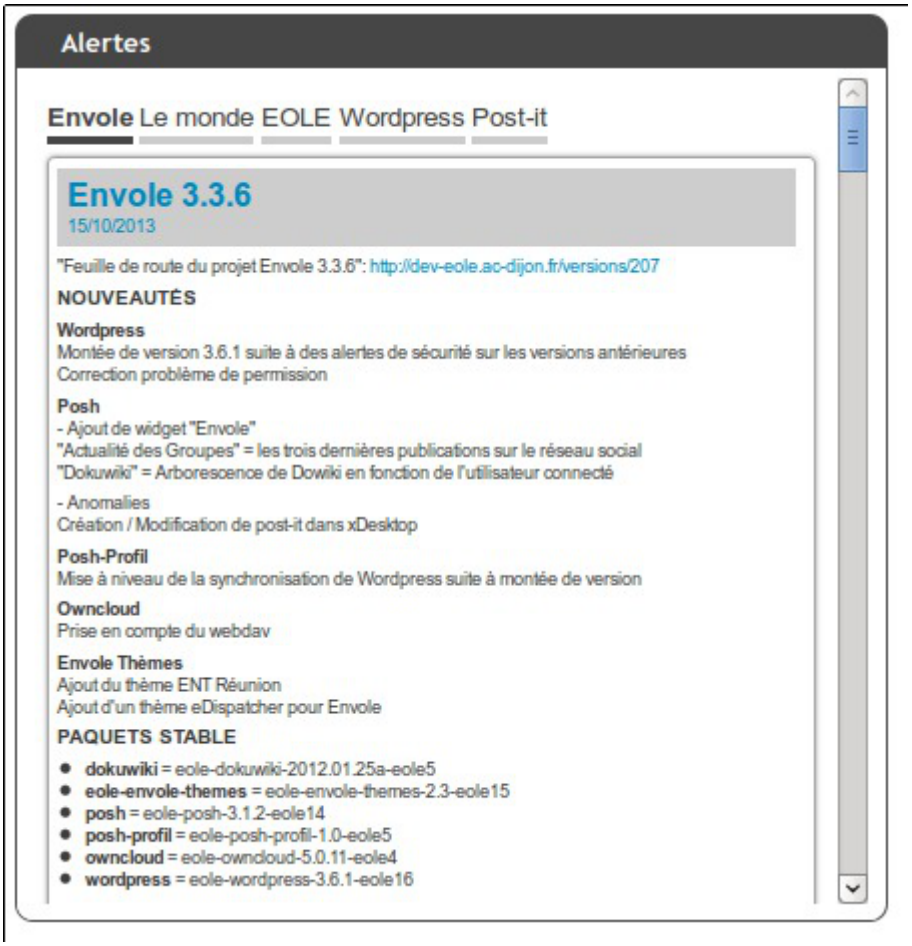
Voir aussi...

Télécharger des icônes de bureau [p.684]

> Créer une alerte pour le widget Alertes

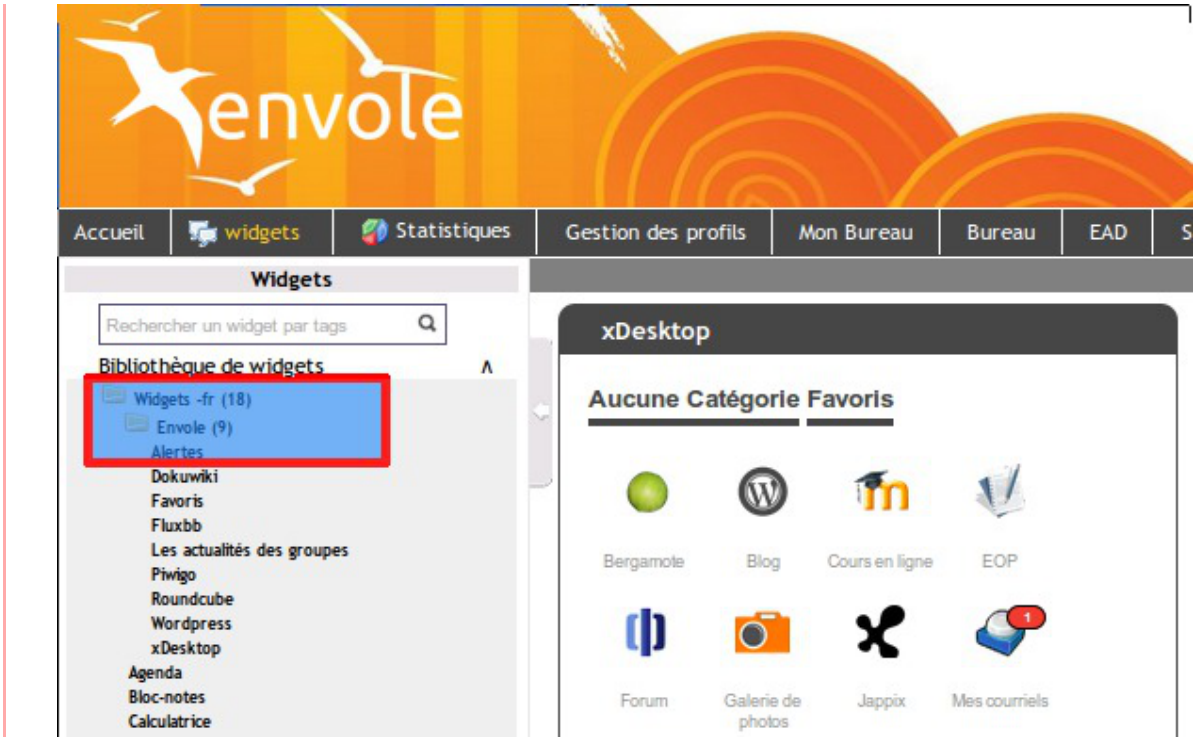
La nouvelle gestion des profils permet de gérer directement des alertes de plusieurs natures (URL, flux RSS et articles) qui seront affichées dans le widget Alertes.

Par défaut le widget Alertes affiche déjà les nouvelles provenant de Wordpress et de Post-it.



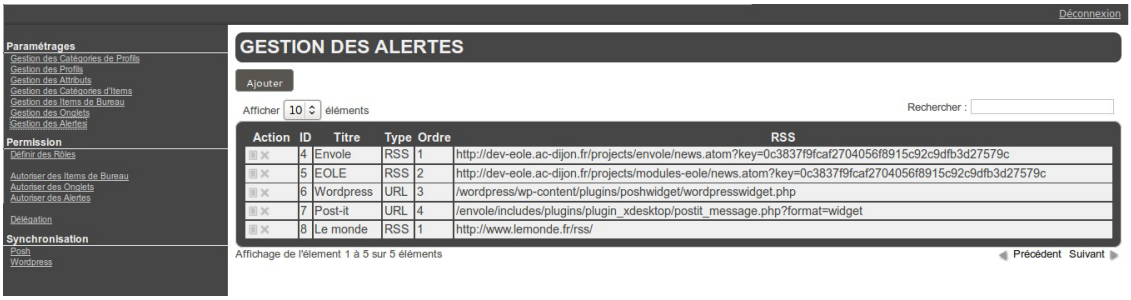
Il ne faut pas confondre le widget Alertes avec le widget du même nom présent par défaut dans le portail et qui affiche les alertes du réseau social. Pour afficher le widget Alertes dans un onglet servant à accueillir les widgets, il se rendre sur l'onglet et activer le panneau de gestion des widgets puis cliquer sur → Bibliothèque de widgets → Widget-fr → Envole → Alertes.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Ajouter une nouvelle alerte

Dans la gestion des profiles il faut se rendre dans la section `Paramétrages` et cliquer sur `Gestion des Alertes`.



Selon les fonctionnalités que vous avez activées dans le portail, le flux RSS de WordPress et le flux des Post-it peuvent déjà être configurés.

Pour ajouter une nouvelle alerte il faut cliquer sur le bouton `Ajouter`.



Une nouvelle vue permet :

- donner un `Titre` à nos alertes, celui-ci apparaîtra dans le haut du widget ;

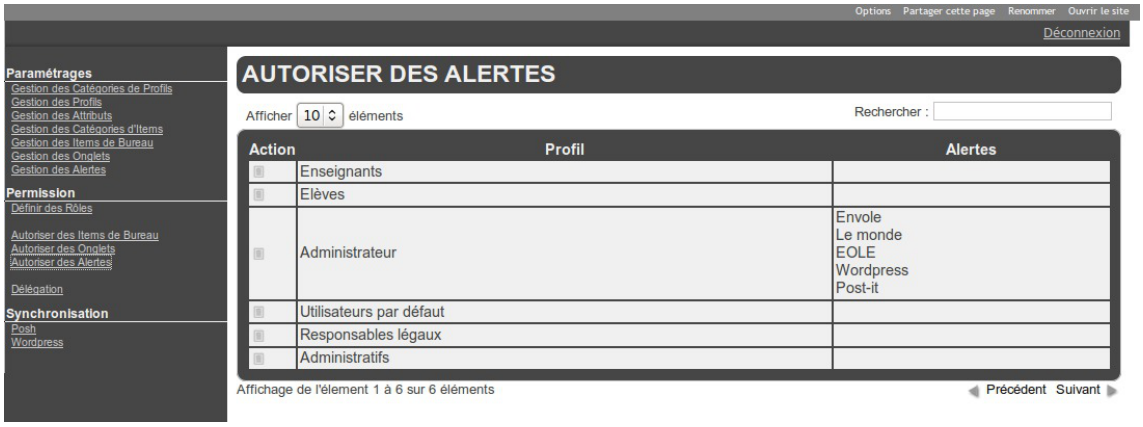
création : Mai 2015 Version : révision : Avril 2018
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- choisir son type : RSS, Articles ou URL ;
- saisir l'`URL` dans le cas d'un flux RSS ou d'une URL ;
- saisir l'`Ordre`, pondération permettant de gérer l'ordre dans le menu haut du widger ;
- saisir le `Nombre d'alertes affichées`.

Il ne faut pas oublier d'enregistrer l'ajout en cliquant sur le bouton `Valider`.

Autoriser des alertes selon le profil

Une fois une nouvelle alerte configurée, il faut en autoriser l'affichage dans le widget et ce en fonction du profil.
Pour se faire, il faut se rendre dans la catégorie `Permission` du menu et cliquer sur `Autoriser des Alertes`.



Il faut choisir le profil pour lequel on veut modifier les autorisations d'alertes puis cliquer sur le bouton modifier du profil choisi dans la colonne `Action`. Dans cette nouvelle vue la section `Profil` rappelle les détails du profil choisi tandis que la section `Liste des Alertes` affiche les alertes déjà autorisées pour le profil donné.



Pour autoriser une alerte il faut cliquer sur le bouton `Ajouter`, dans la nouvelle vue qui liste les alertes disponibles il faut ajouter les alertes avec le bouton `+` de la colonne `Action`. Il faut renouveler l'opération pour chaque alerte à ajouter. Pour finir il ne faut pas oublier d'enregistrer les changements en cliquant sur le bouton `Valider`.

> Synchronisation des comptes

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La synchronisation permet de déterminer une politique de synchronisation des comptes pour plusieurs des applications présentes dans Envole. Chacun des utilisateurs se verra attribuer des droits et des interdictions.

L'utilisateur `admin` ou le compte à qui la délégation de la nouvelle gestion des profils a été confié, a la possibilité d'activer ou de désactiver tout ou une partie de la synchronisation.

La synchronisation peut être lancée à la main mais elle est déjà paramétré pour se lancer tous les jours avec eole-schedule.

Les journaux de la synchronisation peuvent être consultés dans le fichier `/var/log/posh-profil/posh-profil.log`, celui-ci se trouve sur la maître en mode non conteneur et dans le conteneur web en mode conteneur.

>> Synchronisation de POSH

L'objectif est :

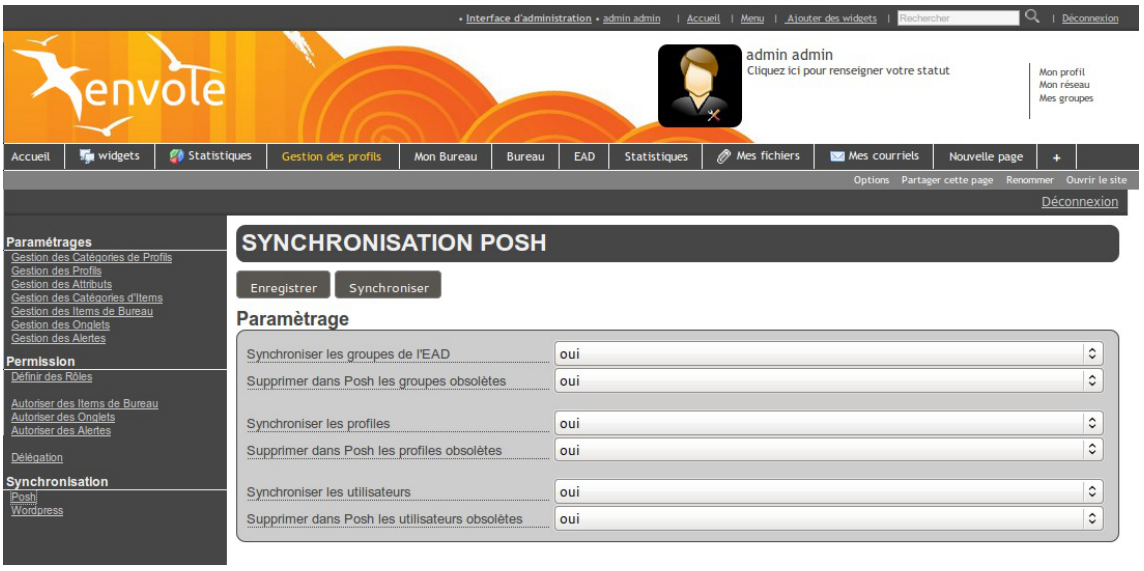
- de bénéficier des possibilités de partage de page par groupe d'utilisateur POSH ;
- d'avoir l'intégralité des utilisateurs déjà créés dans POSH ;
- de purger les groupes / utilisateurs obsolètes.

Il existe deux notions de groupes dans POSH :

- les groupes du réseau social ;
- les groupes créer par l'administrateur pour gérer une catégorie d'utilisateurs.

L'utilisateur peut, par exemple, choisir d'activer la synchronisation des groupes de l'EAD mais de ne pas supprimer les groupes obsolètes dans POSH.

Pour effectuer une synchronisation il faut se rendre dans le menu `Synchronisation` et cliquer sur `POSH`.



Vue dans d'ensemble de la synchronisation POSH

Il faut effectuer les réglages de la synchronisation souhaitée.

Synchro Groupe = Annuaire géré par le module scribe et donc associé à une population scolaire : élèves, parents, professeurs, classes, etc.

Synchro Profil = Plutôt lié à un annuaire académique dont la structure nous est inconnu. Avec la notion

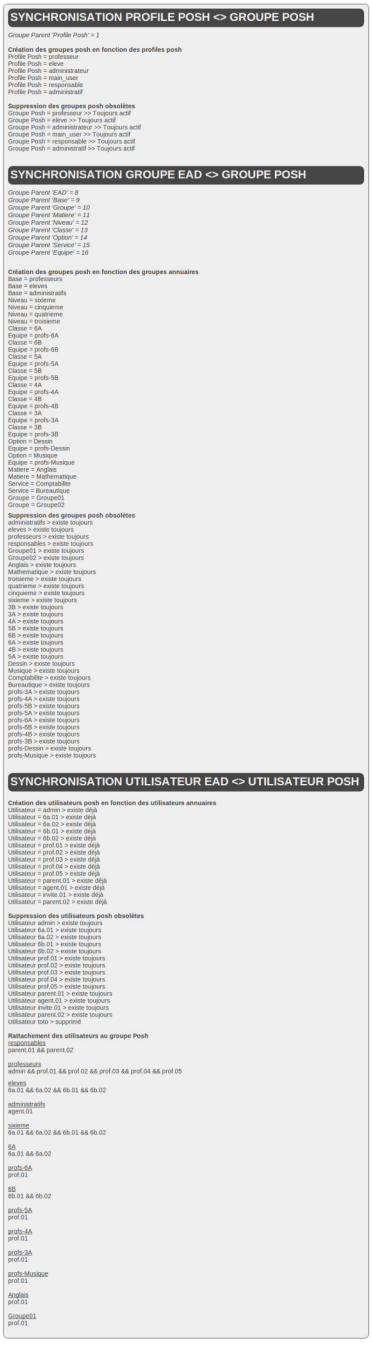
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

de profil il est possible à l'administrateur d'ajouter des attributs propres à son annuaire LDAP. Il lui est même possible de créer des attributs calculés. C'est donc uniquement à la création du ticket SSO que nous sommes capable de déterminer quels profils sont liés à l'utilisateur.

Pour lancer la synchronisation il faut cliquer sur le bouton `Synchroniser`.

> Le rattachement des utilisateurs ne se fait que sur les groupes EAD et non sur les Profils renseigné dans POSH.
>
> Le rattachement d'une personne à un groupe POSH en fonction de son profil ne pourra se faire que lors de sa connexion.

Un rapport de la synchronisation s'affiche en dessous du paramétrage.



SYNCHRONISATION PROFILE POSH <> GROUPE POSH

Groupe Parent 'Profile Posh' = 1

Création des groupes posh en fonction des profiles posh
Profile Posh = professeur
Profile Posh = eleve
Profile Posh = administrateur
Profile Posh = main_user
Profile Posh = responsable
Profile Posh = administratif

Suppression des groupes posh obsolètes
Groupe Posh = professeur >> Toujours actif
Groupe Posh = eleve >> Toujours actif
Groupe Posh = administrateur >> Toujours actif
Groupe Posh = main_user >> Toujours actif
Groupe Posh = responsable >> Toujours actif
Groupe Posh = administratif >> Toujours actif

SYNCHRONISATION GROUPE EAD <> GROUPE POSH

Groupe Parent 'EAD' = 8
Groupe Parent 'Base' = 9
Groupe Parent 'Groupe' = 10
Groupe Parent 'Matiere' = 11
Groupe Parent 'Niveau' = 12
Groupe Parent 'Classe' = 13
Groupe Parent 'Option' = 14
Groupe Parent 'Service' = 15
Groupe Parent 'Equipe' = 16

Création des groupes posh en fonction des groupes annuaires
Base = professeurs
Base = eleves
Base = administratifs
Niveau = sixieme
Niveau = cinquieme
Niveau = quatrieme
Niveau = troisieme
Classe = 6A
Equipe = profs-6A
Classe = 6B
Equipe = profs-6B
Classe = 5A
Equipe = profs-5A
Classe = 5B
Equipe = profs-5B
Classe = 4A
Equipe = profs-4A
Classe = 4B
Equipe = profs-4B
Classe = 3A
Equipe = profs-3A
Classe = 3B
Equipe = profs-3B
Option = Dessin
Equipe = profs-Dessin
Option = Musique
Equipe = profs-Musique
Matiere = Anglais
Matiere = Mathematique
Service = Comptabilite
Service = Bureautique
Groupe = Groupe01
Groupe = Groupe02

Suppression des groupes posh obsolètes
administratifs > existe toujours
eleves > existe toujours
professeurs > existe toujours
responsables > existe toujours
Groupe01 > existe toujours
Groupe02 > existe toujours
Anglais > existe toujours
Mathematique > existe toujours
troisieme > existe toujours
quatrieme > existe toujours
cinquieme > existe toujours
sixieme > existe toujours
3B > existe toujours
3A > existe toujours
4A > existe toujours
5B > existe toujours
6B > existe toujours
6A > existe toujours
4B > existe toujours
5A > existe toujours
Dessin > existe toujours
Musique > existe toujours
Comptabilite > existe toujours
Bureautique > existe toujours
profs-3A > existe toujours
profs-4A > existe toujours
profs-5B > existe toujours
profs-5A > existe toujours
profs-6A > existe toujours
profs-6B > existe toujours
profs-4B > existe toujours
profs-3B > existe toujours
profs-Dessin > existe toujours
profs-Musique > existe toujours

SYNCHRONISATION UTILISATEUR EAD <> UTILISATEUR POSH

Création des utilisateurs posh en fonction des utilisateurs annuaires
Utilisateur = admin > existe déjà
Utilisateur = 6a.01 > existe déjà
Utilisateur = 6a.02 > existe déjà
Utilisateur = 6b.01 > existe déjà
Utilisateur = 6b.02 > existe déjà
Utilisateur = prof.01 > existe déjà
Utilisateur = prof.02 > existe déjà
Utilisateur = prof.03 > existe déjà
Utilisateur = prof.04 > existe déjà
Utilisateur = prof.05 > existe déjà
Utilisateur = parent.01 > existe déjà
Utilisateur = agent.01 > existe déjà
Utilisateur = invite.01 > existe déjà
Utilisateur = parent.02 > existe déjà

Suppression des utilisateurs posh obsolètes
Utilisateur admin > existe toujours
Utilisateur 6a.01 > existe toujours
Utilisateur 6a.02 > existe toujours
Utilisateur 6b.01 > existe toujours
Utilisateur 6b.02 > existe toujours
Utilisateur prof.01 > existe toujours
Utilisateur prof.02 > existe toujours
Utilisateur prof.03 > existe toujours
Utilisateur prof.04 > existe toujours
Utilisateur prof.05 > existe toujours
Utilisateur parent.01 > existe toujours
Utilisateur agent.01 > existe toujours
Utilisateur invite.01 > existe toujours
Utilisateur parent.02 > existe toujours
Utilisateur toto > supprimé

Rattachement des utilisateurs au groupe Posh
responsables
parent.01 && parent.02

professeurs
admin && prof.01 && prof.02 && prof.03 && prof.04 && prof.05

eleves
6a.01 && 6a.02 && 6b.01 && 6b.02

administratifs
agent.01

sixieme
6a.01 && 6a.02 && 6b.01 && 6b.02

6A
6a.01 && 6a.02

profs-6A
prof.01

6B
6b.01 && 6b.02

profs-5A
prof.01

profs-4A
prof.01

profs-3A
prof.01

profs-Musique
prof.01

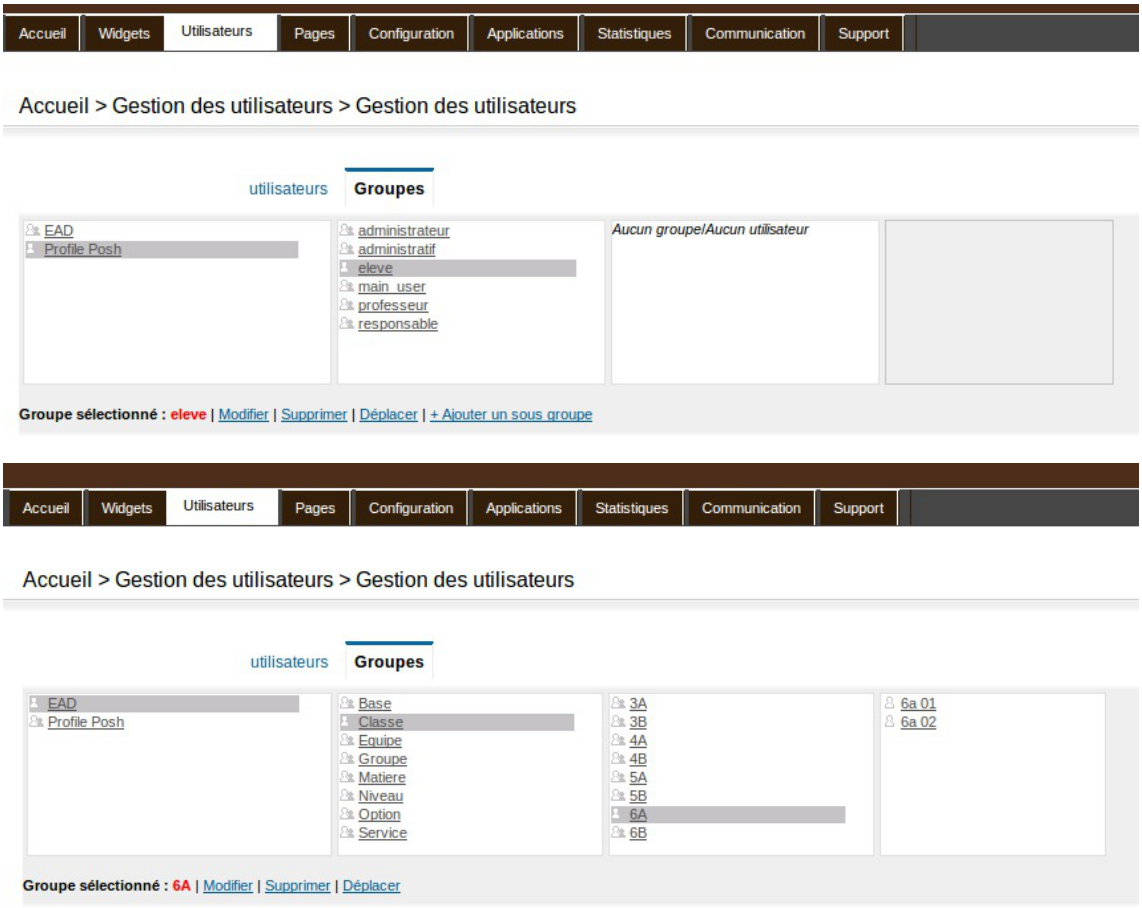
Anglais
prof.01

Groupe01
prof.01

Après synchronisation, il sera possible d'observer les groupes dans l'interface d'administration de POSH.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Deux grandes familles de groupe sont EAD et Posh Profil.



Le groupe EAD sera à jour alors celui de Posh Profil ne se remplira que au fur et à mesure des connexions des utilisateurs.

>> Synchronisation de WordPress

La synchronisation permet de déterminer une politique de synchronisation pour chacun des sites présent sur l'application WordPress d'Envole.

Pour par exemple la synchronisation permet de déterminer que les comptes du Site1 seront synchroniser avec l'ensemble des utilisateurs d'un établissement et que les comptes du Site2 seront uniquement synchroniser avec les élèves de la classe 6èmeA.

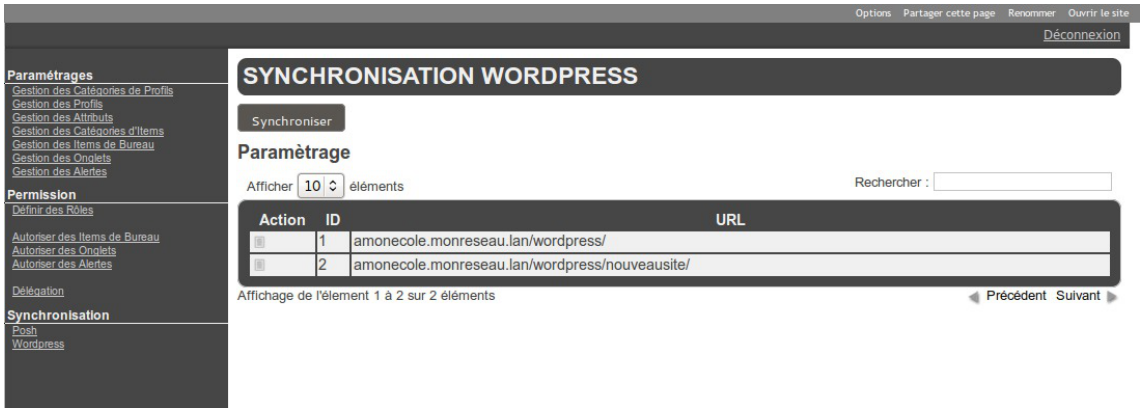
Quoi qu'il arrive cela restera à l'administrateur de créer les nouvelles instances de site.

Gestion de plusieurs instances de WordPress

WordPress (cf. WordPress : système de gestion de contenu) [p.780]

A l'initialisation seule le site principale sera synchronisé. Il sera nécessaire à l'administrateur de venir activer ou non la synchronisation sur les différentes instances de WordPress.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

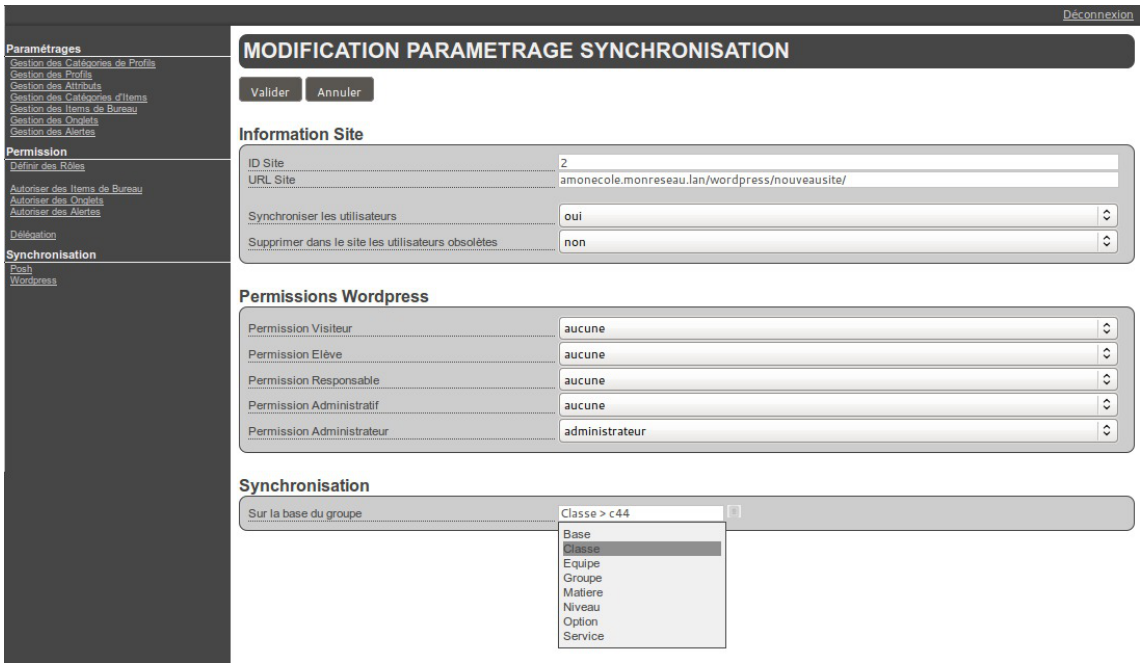


Chaque instance peut être paramétrée en cliquant sur le bouton Action de la ligne correspondante à l'instance choisie.

Les paramètres sont les suivants :

- activation ou non de la synchronisation ;
- purge ou non des utilisateurs obsolètes ;
- concordances entre les rôles et les permissions dans l'instance choisie ;
- choix du groupe de l'EAD servant à la synchronisation.

L'enregistrement des paramètres de synchronisation de fait en cliquant sur le bouton Valider de la vue.



Il ne sera pas possible d'indiquer un rôle WordPress autre qu'administrateur aux utilisateurs administrateur de l'EAD.

L'instance principale de WordPress sera forcement synchroniser avec l'ensemble de l'annuaire.

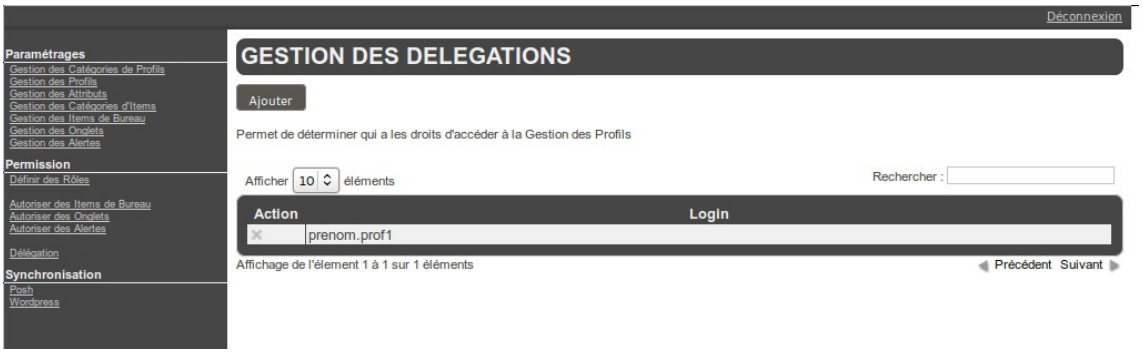
Pour lancer la synchronisation manuelle il faut cliquer sur le bouton Synchroniser de la vue principale.

> Délégation de la gestion des profils

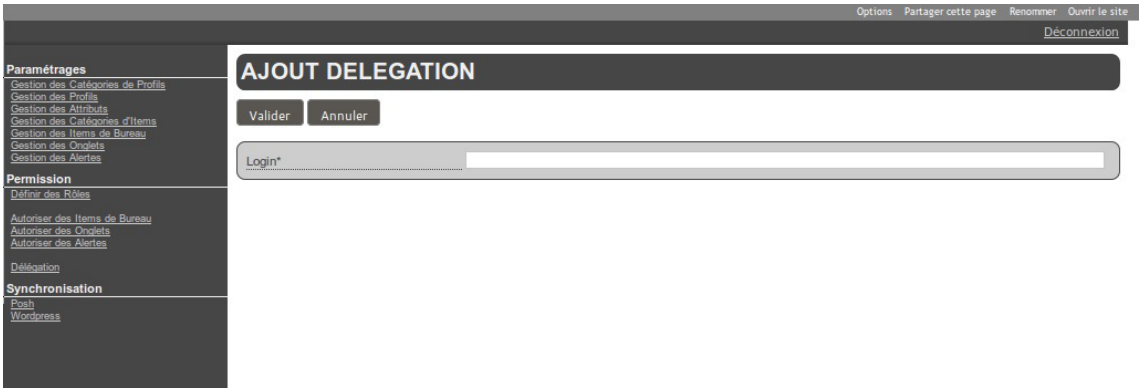
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La nouvelle gestion des profils permet de déléguer la gestion à un utilisateur de l'annuaire LDAP.

Pour se faire il faut se rendre dans la rubrique `Permission` et cliquer sur `Délégation`.



Pour ajouter une délégation il faut cliquer sur le bouton `Ajouter` et saisir le nom du compte de l'utilisateur.





Il n'y a pas de mécanisme qui teste l'existence réelle du compte dans l'annuaire.

Il faut ensuite cliquer sur le bouton `Valider` pour que le changement soit pris en compte.

Pour supprimer une délégation il faut cliquer sur le bouton supprimer de la colonne `Action` correspondant au compte sélectionné. Il faut alors confirmer la suppression sur le bouton du même nom.

> Télécharger des icônes de bureau

Il est possible d'ajouter des icônes pour illustrer vos items de bureau.

Ces icônes sont chargées sur le serveur et sont ensuite disponibles en accès web.

- aller dans `Ajout de paramètres` / `Télécharger une icône ;`
- sélectionner votre fichier à télécharger ;
- rentrer un éventuel nouveau nom ;
- télécharger ;
- l'icône se trouve désormais dans la liste et a été redimensionnée au format 32x32.



Si vous renommez votre fichier image, vous devez impérativement lui mettre une extension faisant partie des types connus (.jpg ,*.png ,*.ico ,*.gif, ...).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Copiez l'URL de l'image et collez-là dans la configuration de votre item de bureau.

Pour supprimer une icône :

- aller dans `Ajout de paramètres` / `Télécharger une icône` ;
- cliquer sur le bouton de suppression correspondant.

12.2.3.u. Widgets

Validation d'un widget

Un widget développé par un utilisateur ou importé depuis un portail externe (google, netvibes) n'est disponible qu'après validation par l'administrateur.

Profil

L'accès à certains widgets peut être restreint à certains groupes de 'profil'.

Voir aussi...

Widget Ressource [p.688]

12.2.3.v. Réseau Social

Le réseau social du portail permet notamment la gestion de groupe, le suivi d'activité et le partage d'information par le biais d'un carnet de bord.

Synchronisation des comptes

Pour synchroniser les groupes de l'annuaire avec le réseau social du portail, il suffit d'aller dans le menu `Envole/Synchronisation` et de choisir les groupes à synchroniser.

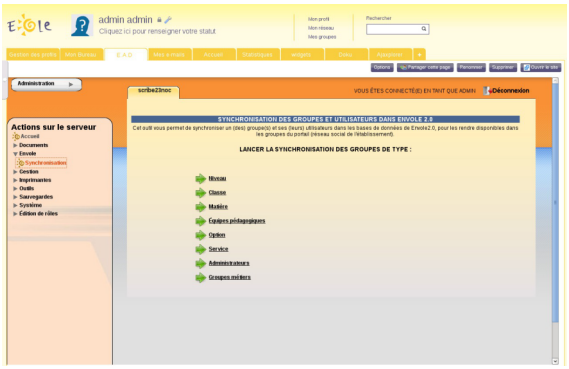
La synchronisation des groupes crée aussi les comptes associés.

Choisir le type de groupe à synchroniser parmi :

- Niveau
- Classe
- Matière
- Équipes pédagogiques
- Option
- Service
- Administrateurs
- Groupes métiers (élèves, professeurs, administratifs)

Cocher les cases correspondantes aux groupes à synchroniser, puis cliquer sur `Valider`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Synchronisation des groupes dans l'EAD

Désactiver le réseau social

Pour simplifier l'utilisation du portail, il est possible de désactiver le réseau social.

- Se connecter en tant qu'utilisateut admin au portail Envole ;
- Aller dans `Interface d'administration` / `Configuration` / `Configuration générale de l'application` ;
- Tout en bas de la page cliquer sur `Options avancées` ;
- Mettre le champ `useNetwork` à `false` ;
- Mettre le champ `useSharing` à `false` ;
- Mettre le champ `useNotebook` à `false` ;
- Mettre le champ `useGroup` à `false` ;
- Vider le champ `homeDivs` ;
- Cliquer sur `Enregistrer les modifications`.

Les fonctionnalités de réseau social et l'usage des groupes qui leur est associé est désormais désactivé.

Lors de la connexion de l'utilisateur, celui-ci se trouvera directement sur le premier onglet de son profil.

La désactivation du réseau social est incompatible avec l'utilisation du greffon charte d'utilisation du portail.

12.2.3.w. Synchronisation

Il est possible de synchroniser les données de l'annuaire (utilisateurs, groupes) avec le portail.

Les données synchronisées sont ensuite visibles depuis l'interface d'administration dans l'onglet `Utilisateurs`.

Les groupes de type 'profil'

La synchronisation est effectuée de manière hebdomadaire et se fait selon une structure prédéfinie :

- `élèves` / `niveaux` / `classes` ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- professeurs / disciplines / équipes pedagogiques classes ;
- responsables ;
- personnels / administration / éducation .

Il est possible de lancer cette tâche manuellement en tapant la commande suivante depuis une console :
`/usr/share/envole/scripts/2.0/synchronize_profile.py`

Les comptes des utilisateurs de l'annuaire du module Scribe sont alors créés dans le portail.

Une fois synchronisé, il est possible d'associer des onglets spécifiques aux groupes choisis.



L'usage de la synchronisation est limité aux portails s'authentifiant sur l'annuaire local du moduler Scribe.

Pour les portails s'authentifiant sur un annuaire ou un serveur d'authentification distant, ces fonctionnalités ne sont pas disponibles.

12.2.3.x. Greffons

Dans la partie administration du portail il est possible de gérer les greffons.

1. aller dans l'interface d'administration du portail avec le compte `admin` ;
2. aller dans Configuration / Gestion des plug-ins ;
3. cocher (Activer) ou décocher (Désactiver) les plugins ;
4. cliquer sur Enregistrer les modifications.



Certains greffons ne sont pas désactivable.

> Charte d'utilisation

Un greffon permet d'ajouter une charte d'utilisation lors de la connexion au portail. Ce greffon est désactivé par défaut.

La charte peut être masquée par l'utilisateur, mais tant qu'il ne l'a pas validée, elle sera affichée sur sa page d'accueil.

Mode ligne de commande

Il est possible d'activer le greffon directement en ligne de commande :

- placer un fichier contenant du code html sur le serveur (par exemple /root/macharte.html) ;
- lancer la commande /usr/share/envole/scripts/2.0/install_charte.sh /root/macharte.html.

La charte d'utilisation est alors activée.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Depuis l'interface

Depuis l'interface d'administration, il est possible de télécharger une charte d'utilisation ou bien d'en rédiger une en ligne :

- aller dans l'interface d'administration du portail avec le compte `admin` ;
- aller dans `Configuration / Gestion des plug-ins` ;
- activer le greffon `plugin CHARTE` ;
- cliquer `Valider`.

A ce stade le greffon de charte d'utilisation est activé et un onglet d'administration est apparu.

- aller dans `Charte d'utilisation` ;
- télécharger un fichier au format html ;

ou

- rédiger votre charte en ligne ;
- cliquer sur `Valider`.

La charte est par défaut en mode "Brouillon".
Afin de l'activer, cliquer sur `Activer`.

Désactiver le greffon

Dans l'interface d'administration :

- aller dans l'interface d'administration du portail avec le compte `admin` ;
- aller dans `Configuration / Gestion des plug-ins` ;
- désactiver le greffon `plugin CHARTE` ;
- cliquer `Valider`.

> Widget Ressource

Le greffon widget ressource permet de créer des widgets de façon simplifiée, à partir d'une URL.
Ce greffon est désactivé par défaut.

Activation du greffon

1. aller dans l'interface d'administration du portail avec le compte `admin` ;
2. aller dans `Configuration / Gestion des plug-ins` ;
3. activer le greffon `Widget Ressource` ;
4. cliquer `Valider`.

Création de widgets de type ressource

Il est alors possible pour les administrateurs de créer des widgets de type ressource :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- aller dans `Widgets / Créer un widget / Créer un widget ressource` ;
- entrer un titre, une description (libellé dans l'interface), une URL ;
- choisir une icône parmi celle proposées ou proposer une URL pour en utiliser une autre ;
- cliquer sur `Activer` ;
- Suivre les instructions pour procéder à la validation du widget (processus standard de création des widgets).

Les utilisateurs peuvent alors facilement ajouter cette ressource dans leur portail.

> Les icônes proposées lors de la création du widget sont celles qui se trouvent dans le dossier `ressources` disponible dans le répertoire personnel de l'utilisateur admin.
> Pour accéder à ce dossier depuis Pydio ou un client FTP, il faut dans l'onglet `Ftp` de l'outil de configuration du module, en mode expert, passer la variable `Activer l'accès au dossier des ressources web` à `oui`.

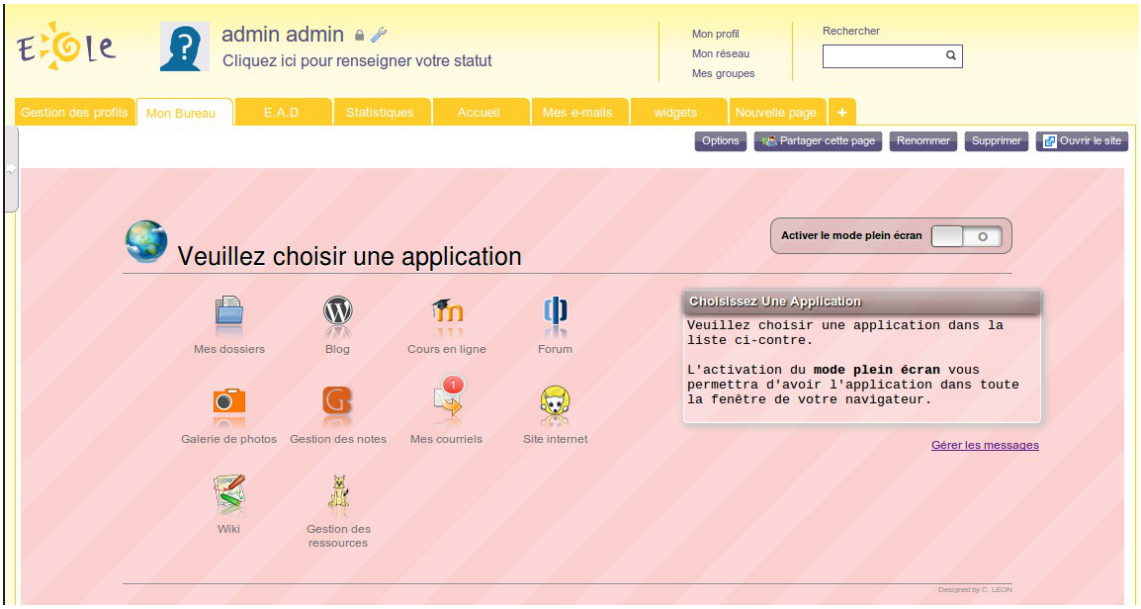
Désactivation du greffon

1. aller dans l'interface d'administration du portail en tant qu'utilisateur `admin` ;
2. aller dans `Configuration / Gestion des plug-ins` ;
3. désactiver le greffon `Widget Ressource` ;
4. cliquer `Valider`.

> Greffon Xdesktop

Présentation

Le greffon Xdesktop est une sur-couche du greffon Desktop, le bureau d'accès rapide aux applications.
Il est dépendant du greffon Desktop.

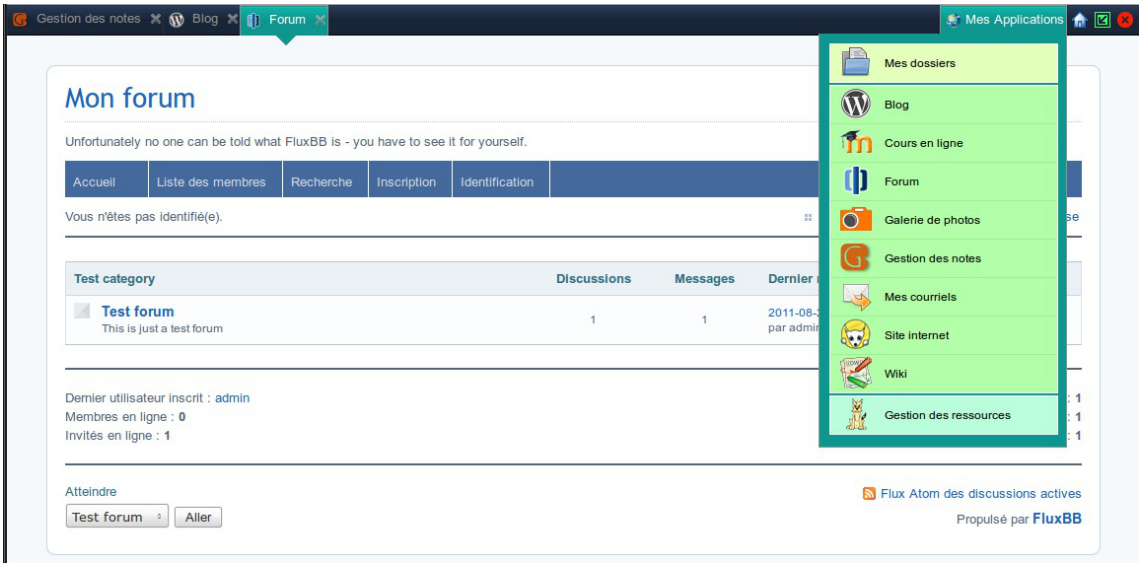


Plus convivial, il permet une navigation plein écran, une catégorisation des applications et une gestion de

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

l'affichage de mémos par profils.

Il permet également une remontée des statistiques dans l'application Piwik d'un module centralisé.



Ce greffon n'est pas activé par défaut.

Le bureau Xdesktop (cf. Le bureau Xdesktop)

Activation du greffon

1. aller dans l'interface d'administration du portail avec le compte `admin` ;
2. aller dans Configuration / Gestion des plug-ins ;
3. activer le greffon `plugin Xdesktop` ;
4. cliquer sur : Enregistrer les modifications .

Création d'un onglet unique pour tester

Côté portail utilisateur :

- créer un nouvel onglet, cliquer sur `Nouvelle page`, à droite des onglets existants ;
- définir un titre pour l'onglet dans le champ `Définissez le titre de la page ;`
- choisir `Ajouter une page internet` dont l'URL est /envole/includes/plugins/plugin_xdesktop/xdesktop.php (ne pas oublier le / au début de l'URL).



Si vous avez changé le chemin vers l'ENT Envole lors de la configuration du serveur, pensez à mettre le contenu de la variable "alias_envole" dans les chemins.

Par défaut sa valeur est ***`/envole`*** et elle est éditable par l'outil `gen_config` dans l'onglet `Application web` en ◉ mode expert .

Substituer l'ancien bureau par le nouveau

Pour réaliser la substitution, il faut utiliser le Gestionnaire de profil du portail en tant qu'`admin` :

1. se rendre dans la Gestion des profils , Modification / Suppression , Onglet

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

2. remplacer le champ `Url` /envole/includes/plugins/plugin_desktop/desktop.php par /envole/includes/plugins/plugin_xdesktop/xdesktop.php



Création d'un onglet pour un profil donné

Il est possible de proposer le nouveau bureau à un profil donné et pas à un autre.

Pour créer un nouvel onglet, il faut utiliser le Gestionnaire de profil du portail en tant qu'`admin` :

1. créer un nouvel onglet pour le nouveau bureau , `Gestion des profils` , `Ajout de paramètres` , `Onglet` , et en remplissant les champs suivants :

   `Nom` = "Mon nouveau bureau" ;

   `description` = "Bureau à la mode Xdesktop" ;

   `Indice` = "1" ;

   `Type de page` = "2" ;

   `Url` = "/envole/portal/xdesktop.php" ;

   `Id admin de l'onglet` ="-1".

2. autoriser l'onglet pour les profils souhaités : `Gestion des profils` , `Permission` , `Autoriser des onglets` .
3. suppression optionnelle de l'ancien onglet.

En cas de suppression de l'onglet de l'ancien bureau :

- les utilisateurs qui ne se sont jamais connectés au portail auront directement le nouveau bureau sans avoir l'ancien.
- les utilisateurs qui se sont déjà connectés au portail devront se connecter, supprimer l'onglet de l'ancien bureau manuellement (clic sur la croix de l'onglet) pour ne plus l'avoir lors de leurs prochaines connexions.



Les deux bureaux peuvent cohabiter dans deux onglets différents, il n'est pas obligatoire de supprimer l'onglet ou d'en interdire l'accès.

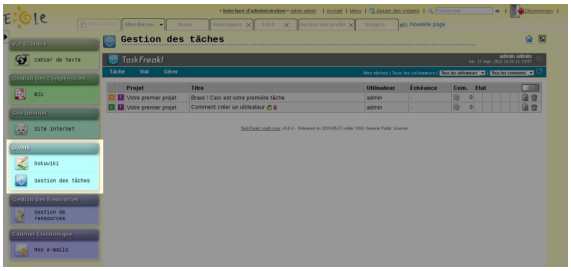
Lorsque l'on clique sur une application depuis la première page du bureau, on obtient la liste des applications dans la colonne de gauche et l'ouverture de l'application à droite.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Regroupement des applications par catégorie

La colonne de gauche liste les applications disponibles.



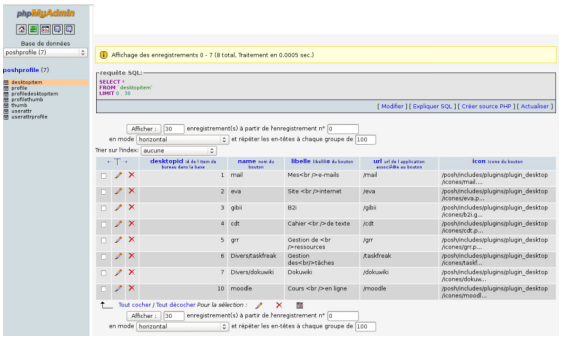
Groupement des applications par catégorie

Lors de leur ajout, on peut regrouper les applications par catégorie en utilisant, dans le nom des items de bureau, le format "catégorie/nom_de_l'application" :

`Gestion des profils`, `Ajout de paramètres`, `Item de bureau`, `Nom` : "nom_de_votre_catégorie/nom_de_l'application_apparaissant_colonne_de_gauche".

Pour les existants il faut supprimer l'item et le recréer, car le nom n'est pas éditable.

Toutefois il est possible de modifier en passant par la base de donnée `poshprofile`, table `desktopitem`, champ `name`.



Édition des données de la table desktoitem par phpMyAdmin

Si la catégorie n'est pas explicitée dans le nom, l'item se retrouve par défaut dans la catégorie "Aucune Catégorie".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour la prise en compte des modifications il est nécessaire :

- de relancer le gestionnaire de profil :

  `# service posh-profile restart`

- de se déconnecter ou de vider le cache du portail

Pour faire la mise en place, il peut être plus pratique d'accéder directement à la page Xdesktop à l'adresse : `http://<adresse_serveur>/envole/includes/plugins/plugin_xdesktop/xd`

Statistiques d'utilisation des applications

Par défaut les accès aux applications par Xdesktop vont alimenter l'application Piwik du module Scribe hébergeant le portail.

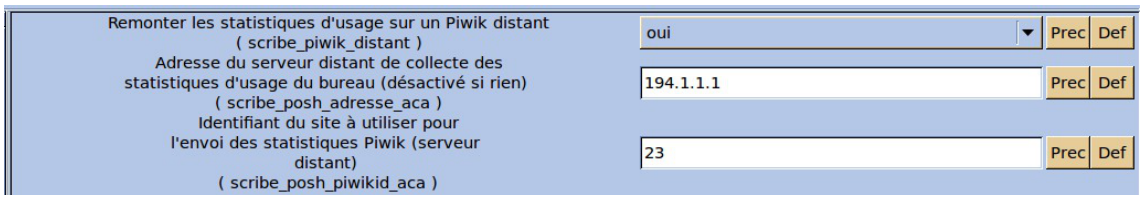
Il est possible de configurer l'application différemment pour avoir des remontées sur un module EOLE centralisé ou un autre serveur hébergeant l'application Piwik, nous nommerons ce serveur : serveur central.

Pour ce faire il faut passer :

- modifier la configuration du module.
- modifier le serveur central.

Pour modifier la configuration du module il faut :

- lancer l'outil de configuration du module ;
- passer en ◉ mode expert ;
- dans l'onglet Ent mettre `Remonter les statistiques d'usage sur un Piwik distant` à `oui` ;
- saisir l'adresse du serveur EOLE hébergeant l'application Piwik centralisée, exemple pour un module Seshat centralisé : `https://<adresse serveur>/piwik2` ;
- saisir l'identifiant du site concerné fourni par l'application Piwik centralisée ;
- enregistrer la configuration et lancer une reconfiguration du serveur avec la commande reconfigure.

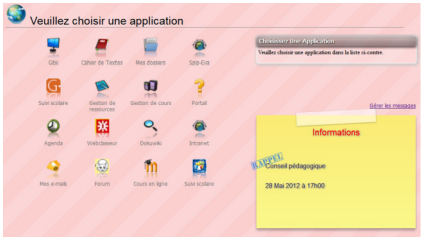


Sur le serveur central il faut renommer le fichier piwik.js en piwik_global.js et l'éditer pour renommer l'objet `Piwik` en `PiwikGlobal`.

Par exemple sur une module Seshat il faudra renommer le fichier /var/www/html/piwik/piwik.js en /var/www/html/piwik/piwik_global.js et l'éditer.

Gestion des mémos

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Les personnes pouvant gérer les mémos doivent faire partie du groupe `admin postit` sinon, seul le compte `admin` y a accès.

Dans l'EAD, se rendre dans `Gestion / Groupes / Création de groupe`, créer le groupe `admin postit`.

Pour affecter des rédacteurs de mémo au groupe `admin postit`, toujours dans l'EAD, se rendre dans `Gestion / Édition groupée` et choisir le ou les utilisateurs avec les critères suivants :

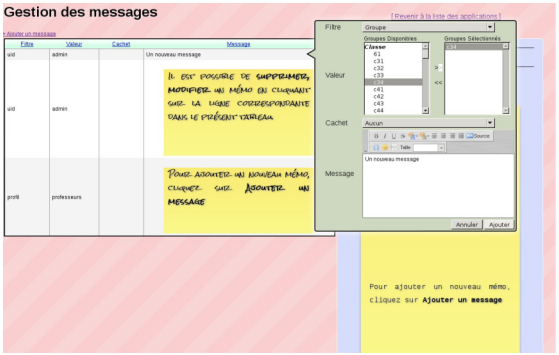
- `Première lettre du login` ;
- `Type d'utilisateur` ;
- `Membre du groupe` ;
- `Partie du nom de famille`.

Valider en cliquant sur `Lister`.

Cocher le ou les futurs rédacteurs, puis cliquer sur `Inscrire ces utilisateurs à d'autres groupes`

Dans la liste `Inscrire les utilisateurs sélectionnés au groupe` : , choisir le groupe `admin postit` et cliquer sur `Valider`.

Pour accéder à la gestion des mémos, il faut cliquer sur `Gérer les messages`.



Désactivation du greffon

Dans l'interface d'administration :

- aller dans l'interface d'administration du portail avec le compte `admin` ;
- aller dans `Configuration / Gestion des plug-ins` ;
- désactiver le greffon `plugin Xdesktop` ;
- cliquer `Valider`.

> Greffon Password

Introduction

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Un greffon permet aux utilisateurs de modifier leur mot de passe directement depuis le portail. Ce greffon est activé par défaut sur une nouvelle installation mais pas sur un module déjà en production avant la mise à jour.

L'outil de modification de mot de passe est disponible dans les paramètres du compte.

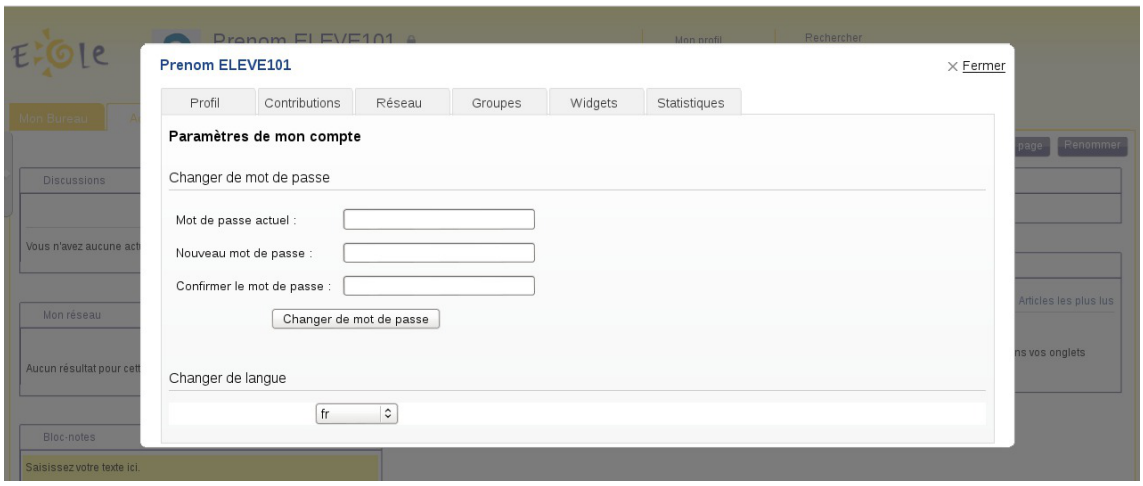
Pour accéder aux paramètres du compte il faut cliquer sur l'identifiant affiché en haut du portail.



Puis il faut cliquer sur `Paramètres de mon compte` en haut à droite du calque affiché.



Pour changer le mot de passe il faut saisir le mot de passe actuel.



Activation du greffon

- aller dans l'interface d'administration du portail avec le compte `admin` ;
- aller dans `Configuration` / `Gestion des plug-ins` ;
- activer le greffon `Plugin Password` ;
- cliquer sur `Enregistrer les modifications` .

Le greffon est alors disponible.

Le mot de passe est modifié pour la connexion au portail, pour la connexion aux applications

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> web ainsi que pour la connexion au domaine.
>
> Le nombre de caractères pour le mot de passe est par défaut fixé à 5. Il est possible de modifier cette valeur dans l'onglet `Mot de passe` de l'interface de configuration du module en mode normal.

Voir aussi...

> Onglet Mots de passe : Politique de mot de passe pour les utilisateurs [p.64]

> Greffon Thumb

Le greffon Thumb permet la création des onglets en fonction des profils de l'utilisateur connecté.

Ce greffon apporte des évolutions :

- permet que la suppression d'un onglet dans posh-profil soit bien reportée dans le portail ;
- permet que la modification du label, de l'url ou de l'indice dans posh-profil soit bien reportée dans le portail ;
- rend impossible à l'utilisateur la modification d'un onglet associé à un de ses profiles ;
- rend impossible à l'utilisateur d'ajouter, de supprimer ou de modifier les widgets partagés par un onglet de type `widget` associé à un de ses profils ;
- rend opérationnel l'altèration par l'administrateur de la page widget servant de template à un onglet associé à un profil, les modifications sont apportées aux pages des utilisateurs ;
- l'utilisateur sera rattaché aux groupes qui correspondent à son profil lors de la synchronisation de POSH.

Installation du greffon

Le greffon est pré-installé par défaut.

Désactiver le greffon

Le greffon n'est pas désactivable dans l'interface d'administration du portail.

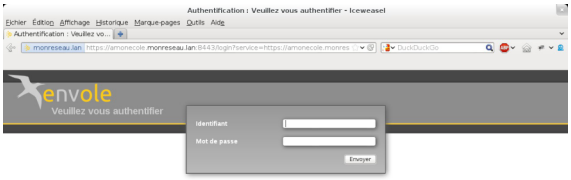
12.2.4. Personnalisations visuelles

12.2.4.a. Personnalisation avec Envole Thèmes

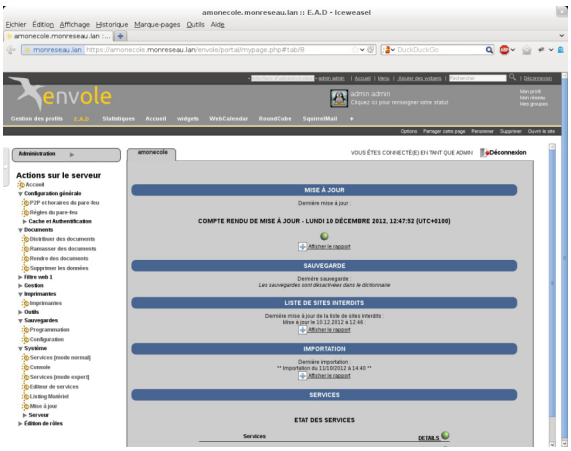
Présentation

Envole Thèmes permet de récupérer des thèmes pour les différents éléments visuels propre à Envole : mire SSO, EAD, portail Envole, les diverses applications supportées par la mutualisation, ...

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de la mire SSO avec le thème Envole



Vue du portail avec le thème Envole

Installation d'Envole Thèmes

Installation du paquet eole-envole-themes

Envole Thèmes s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-envole-themes
```

Pour choisir le thème parmi la liste proposée il faut se rendre dans l'interface de configuration du module dans l'onglet `Applications web` et choisir le thème dans `Nom du Thèmes`.

Envole Thèmes n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.



Cette solution n'est pas compatible avec certaines des personnalisations manuelles de la mire SSO.

12.2.4.b. Changer la page d'accueil

Envole démarre par défaut sur la page intitulé Mon carnet qui est l'accueil du réseau social.

Plusieurs configurations sont disponibles.

Depuis l'interface d'administration :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Dans l'onglet `Configuration / Configuration générale de l'application` ;
- Dans `A chaque connexion, charger par défaut` ;
- - Choisissez parmi :
  - `Le premier onglet` : ouvrira le premier onglet de l'utilisateur (pas Mon carnet) ;
  - `La page ouverte à la dernière fermeture` : ouvre le dernier onglet ouvert par l'utilisateur ou le premier onglet ;
  - `L'accueil (si applicable)` : ouvrira la page Mon carnet si le réseau social est activé.

12.2.4.c. 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

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`/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).

12.2.4.d. Le portail

Style par défaut

Une feuille de style par défaut est fournie par l'application :
`/var/www/html/posh/styles/main.css`

Création d'un thème personnalisé

La personnalisation se fait par le biais de thèmes (fichiers `*.thm`).
Les fichiers thm doivent être placés dans :
`/var/www/html/posh/styles/themes/`
Ils peuvent également être téléchargés au travers de l'interface d'administration.

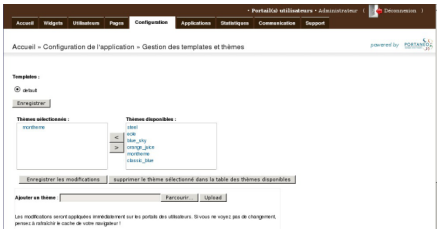
Pour vous y retrouver dans la structure css, regardez le fichier main.css, ou inspirez-vous de la version EOLE de main1.css (installée par défaut).

Droits sur les fichiers thm

L'utilisateur `www-data` doit avoir les droits de lecture sur les fichiers thm, les droits peuvent être modifiés de la façon suivante :

- `chown www-data:root /var/www/html/posh/styles/themes/montheme.thm`
- `chmod 600 /var/www/html/posh/styles/themes/montheme.thm`

Utilisation du thème personnalisé



Gestion des thèmes du portail

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- se connecter en tant qu'administrateur (compte 'admin') ;
- aller dans `Interface d'administration,` puis dans l'onglet `Configuration` et `Gestion des templates et thèmes` ;
- faire passer `montheme` de la liste de droite vers celle de gauche, enlever le thème `eole` de la liste de droite et valider ;
- toujours dans l'interface d'administration, dans l'onglet `Accueil`, cliquer sur `Rafraichir le cache`.



Il est parfois nécessaire de recharger plusieurs fois la page avant de voir votre thème pris en compte.

12.2.4.e. Le bureau d'application du portail

Une feuille de style est utilisée pour la mise en forme du bureau :
`/var/www/html/posh/includes/plugins/plugin_desktop/theme/style/theme.css`
Pour la mise en forme inspirez-vous de la feuille de style d'origine :
`/var/www/html/posh/includes/plugins/plugin_desktop/styles/default.css`
Placez les images utilisées dans :
`/var/www/html/posh/includes/plugins/plugin_desktop/theme/image/`

12.3. Applications pré-installées

Il est possible d'ajouter au module utilisé (AmonEcole, Scribe) des applications web pré-installées et de les intégrer à Envole.

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.



Reconfiguration du module

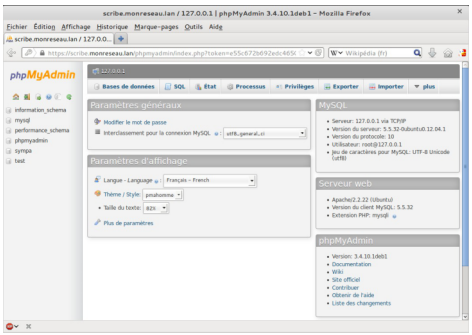
De nombreuses applications nécessitent d'être activées depuis l'interface de configuration du module et une reconfiguration du serveur est indispensable.

Cette procédure est relativement longue, il est donc possible d'activer plusieurs applications et de ne lancer qu'une fois la commande `reconfigure`.

12.3.1. phpMyAdmin : gestionnaire de base de données MySQL

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 `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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 :

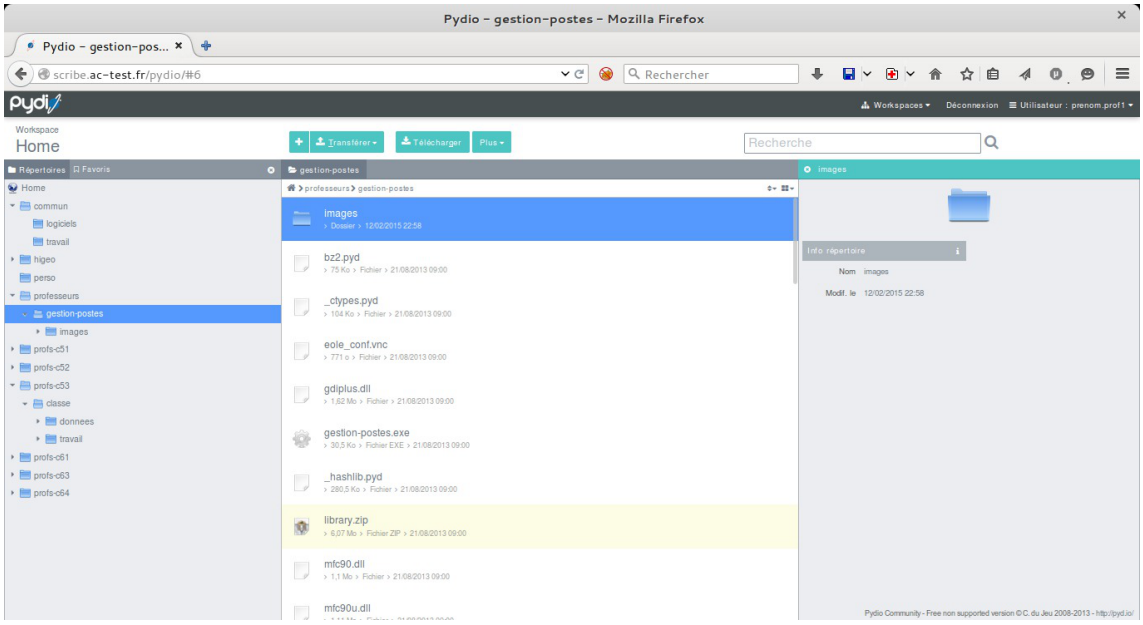
`mysql_pwd.py`

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.

12.3.2. Pydio : gestionnaire de fichiers

Présentation



Pydio, anciennement Ajaxplorer, est un gestionnaire de fichiers en ligne.

Ce gestionnaire permet de naviguer dans l'arborescence des fichiers utilisateurs. Il permet également l'édition de fichiers, l'écoute de fichiers audio, l'affichage d'images, ...

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

http://pyd.io/

Installation de Pydio

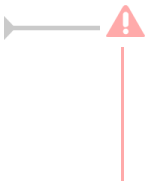
Piwigo s'installe manuellement, en saisissant les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-pydio
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



L'application nécessite l'activation de l'accès FTP.

Dans l'interface de configuration du module, dans l'onglet `Services`, passer la variable `Activer l'accès FTP` à `oui`.



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 `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 : `http://<adresse serveur>/pydio/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO[p.902], ce service doit donc être actif.

Rôles des utilisateurs

Par défaut les rôles des utilisateurs sont assignés comme suit :

- **Administrateur**

  Seul l'utilisateur `admin` est administrateur de l'application.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Il a un accès complet à l'application et à sa configuration.

Il peut déléguer ce rôle en donnant les droits administrateur à un utilisateur.

- **Utilisateur authentifié**

  Tout utilisateur ayant un répertoire personnel sur le module Scribe possède un accès à l'application.

Remarques

Les comptes sont créés dans Pydio lors de la première connexion à l'application (initialisation du compte et des préférences).

Mise à jour de la configuration suite à un changement d'adresse IP

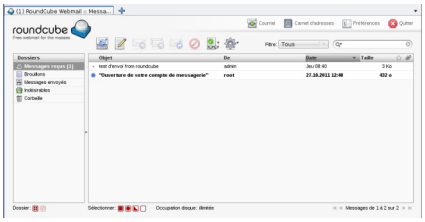
Si vous avez modifié l'adresse IP de votre serveur l'arborescence des répertoires est vide à la connexion à l'application. Il faut alors éditer la configuration de votre serveur.

Dans l'interface de configuration du module, en mode Expert, dans l'onglet Envole-expert :

- Mettre la nouvelle adresse IP de votre serveur dans `Adresse IP du client ftp`

12.3.3. Roundcube : interface pour le courrier électronique

Présentation



Consultation de messages avec Roundcube

Roundcube est une interface web pour consulter son courrier électronique (webmail).

Il supporte les protocoles IMAP et SMTP.

http://www.roundcube.net

Installation

Roundcube s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-roundcube
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .

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/`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 Applications web.

L'opération nécessite une reconfiguration du module avec la commande reconfigure.

Accéder à l'application

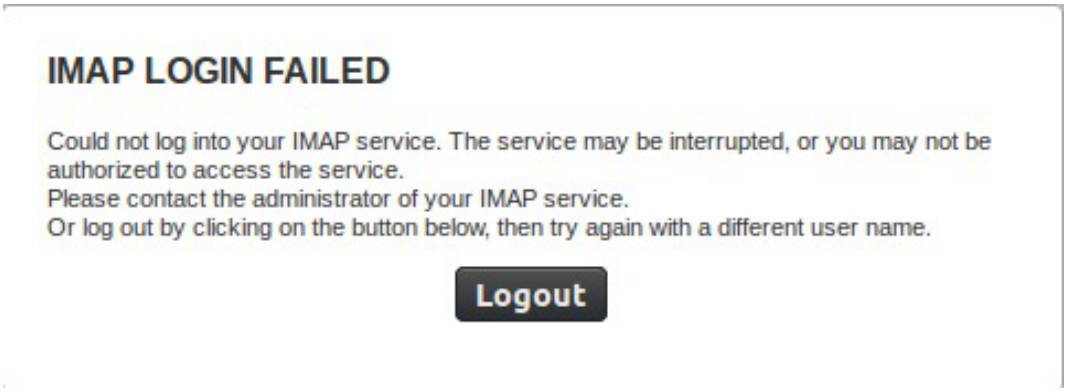
Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/roundcube/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire et ayant une boite de courrier électronique **locale** ont accès à l'application.

Un utilisateur sans boîte locale réussira à s'authentifier auprès du serveur SSO[p.902] mais sera rejeté par le serveur IMAP[p.891].

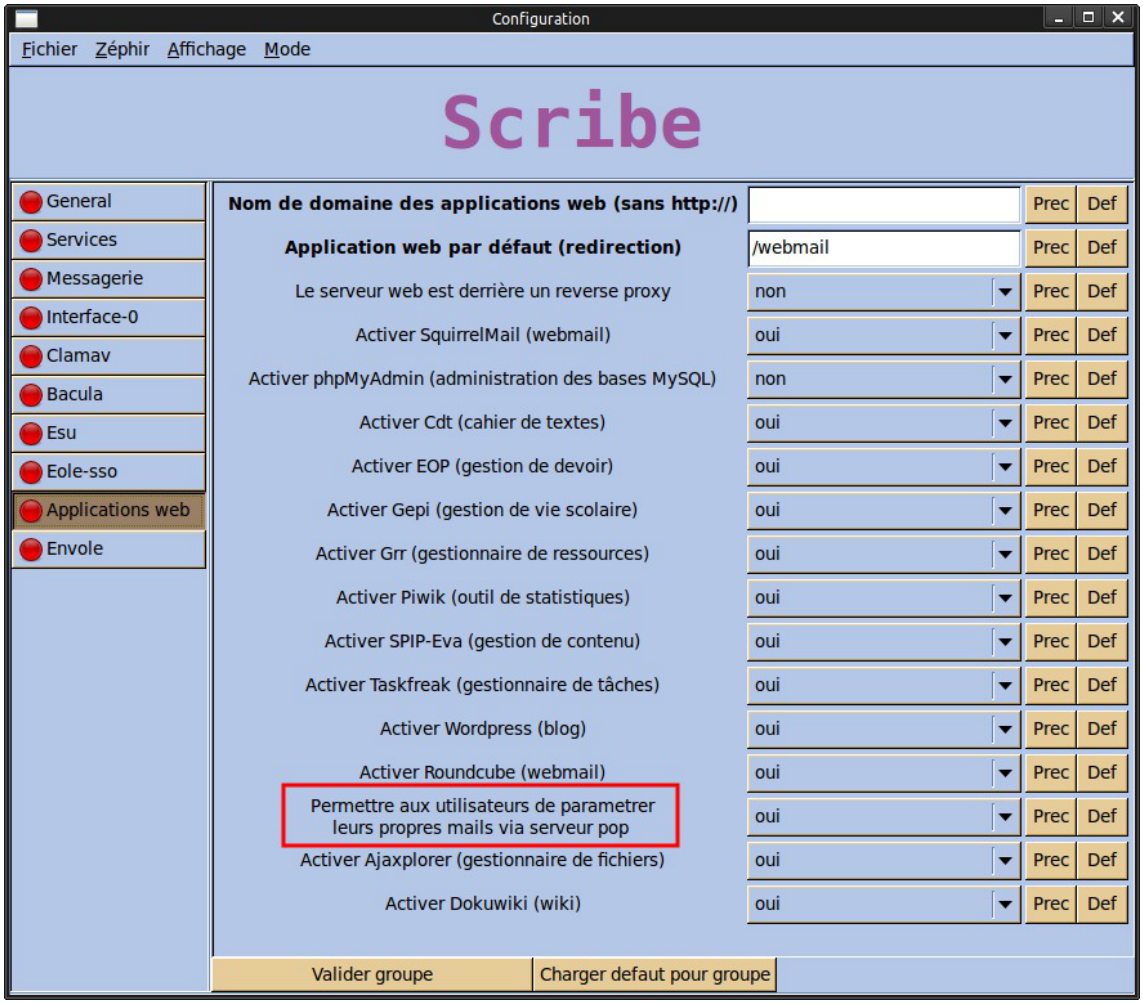


Comptes de messagerie secondaires

À partir de la version 0.9.1 le greffon **pop3fetcher** est intégré à Rouncube. Il est désormais possible pour les utilisateurs de paramétrer des comptes de messagerie secondaires. Ainsi ils peuvent consulter dans Roundcube leurs courriels d'une autre messagerie.

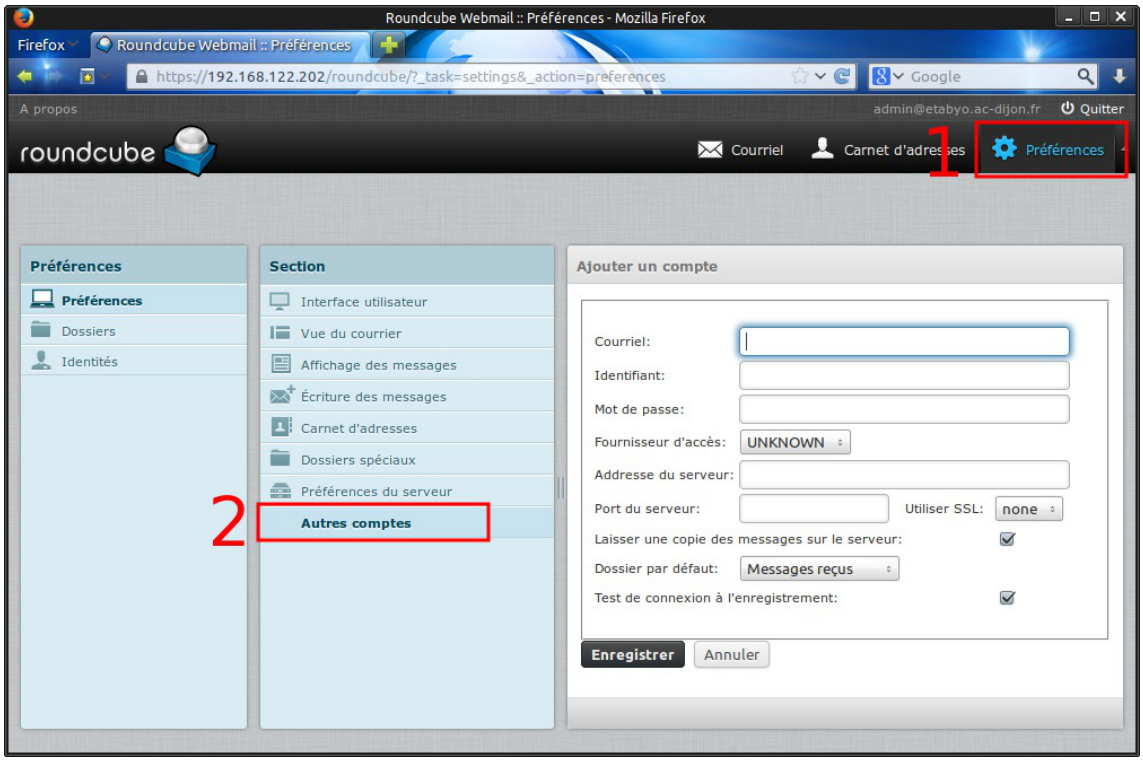
Cette option est par défaut à `oui` mais est désactivable dans l'onglet Applications web de l'interface de configuration du module.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Activation du greffon "pop3fetcher" dans l'interface de configuration du module

Dans Rouncube ce paramétrage se fait dans les préférences de l'utilisateur dans la section Autres comptes.



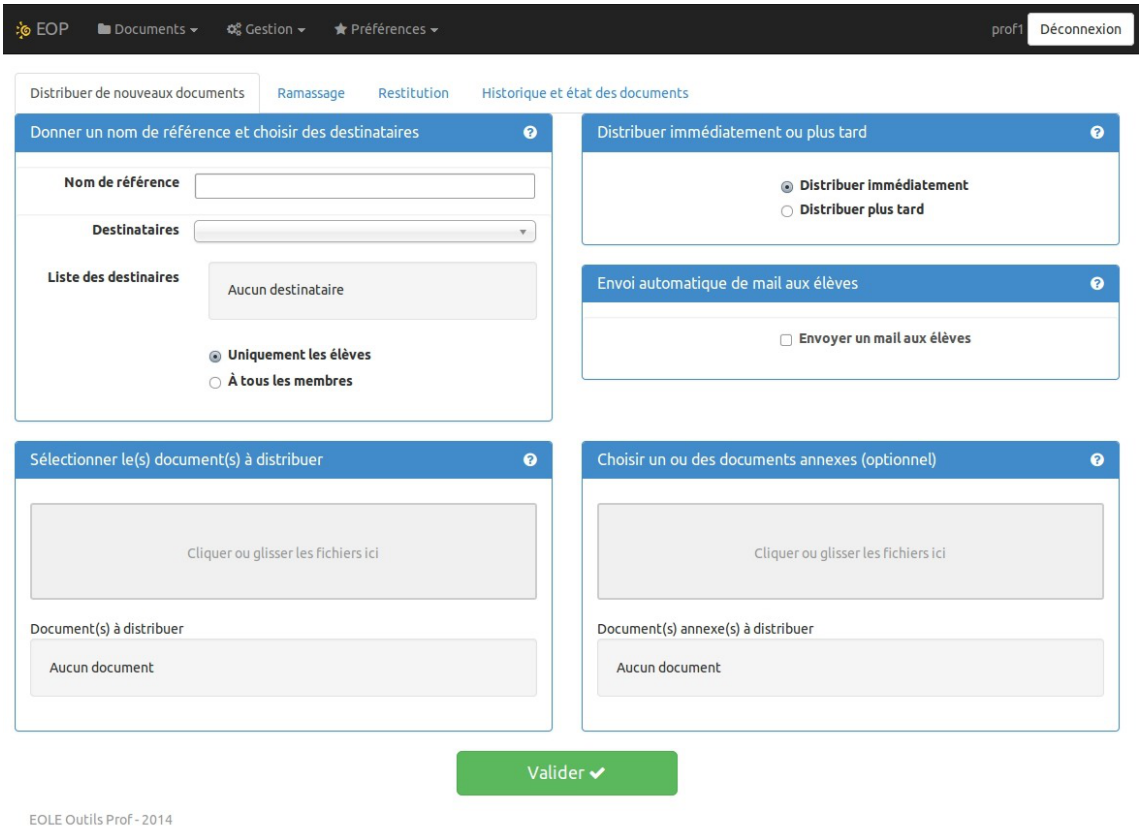
Déclaration de comptes de messagerie secondaire dans l'interface Roundcube

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

En mode conteneur, lorsqu'on active cette fonctionnalité, les ports 110 et 995 sont autorisés du conteneur web vers l'extérieur.

12.3.4. EOP : outils à destination des enseignants

Présentation



L'objectif de l'application web EOP (EOLE Outils Profs) est de proposer une interface simple contenant un ensemble d'outils à destination des enseignants. Cette nouvelle application, indépendante, ne traite pas uniquement de la gestion des documents et peut être intégrée dans un portail. Le développement est basé sur le framework python Flask[p.890].

http://dev-eole.ac-dijon.fr/projects/eop

Principales fonctionnalités

- gestion de documents (distribution simple, ou distribution et ramassage) ;
- observation et prise de contrôle des postes élèves ;
- possibilité de changer le mot de passe d'un élève ;
- possibilité de changer le mot de passe du compte enseignant.

Cette version d'EOP est compatible avec les navigateurs modernes ou avec une version d'Internet Explorer 9 et supérieure.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Installation

Cette application est pré-installée sur le module Scribe à partir de la version 2.4.2.

Pour désactiver l'application il faut se rendre dans l'interface de configuration du module en mode normal, dans l'onglet Applications web et passer `Activer EOP (gestion de devoir)` à `non`.
L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Accéder à l'application

Pour accéder à l'application il faut se rendre à l'adresse : `https://<adresse serveur>/eoleapps/eop/documents/`

Rôles des utilisateurs

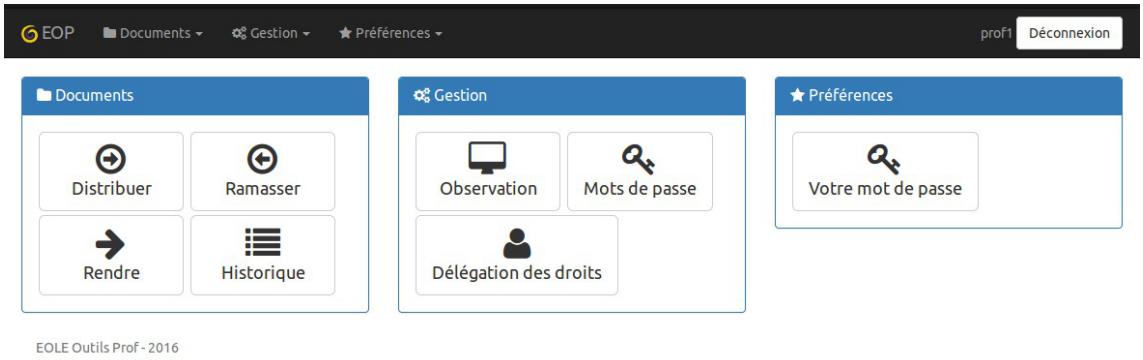
Seuls les enseignants et l'utilisateur `admin` (enseignant également) ont un accès à l'application.
Les professeurs principaux ont accès à quelques fonctionnalités supplémentaires.
Les élèves disposent des documents distribués dans leur répertoire personnel mais n'ont pas d'accès à l'application EOP.

Fonctionnalités

Le bandeau noir de l'interface permet un accès rapide aux différentes fonctionnalités.



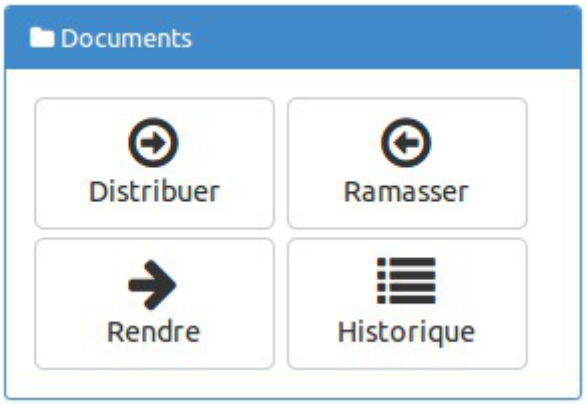
L'icône EOP permet d'afficher les différentes fonctionnalités sous forme de bouton.



À droite de l'interface apparaît l'identifiant utilisé et le bouton `Déconnexion`.

Menu Documents

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



- Distribuer : permet de gérer la distribution de documents ;
- Ramasser : permet de récupérer un document distribué et nécessitant la modification par les utilisateurs ;
- Rendre : permet d'annoter les documents ramassés et de les restituer ;
- Historique : permet de lister les différents documents et de connaître leur état.

Menu Gestion



- VNC : permet d'observer un ou plusieurs postes ou d'en prendre le contrôle à distance ;
- Mots de passe : visible uniquement avec le rôle de professeur principal, cette option permet de changer le mot de passe d'un ou de plusieurs utilisateurs.
- Délégation de droits : visible uniquement avec le rôle de professeur principal, elle permet de déléguer la gestion des mots de passe (dans EOP et EAD) et des comptes élève (dans l'EAD) pour une classe donnée.

Menu Préférences

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



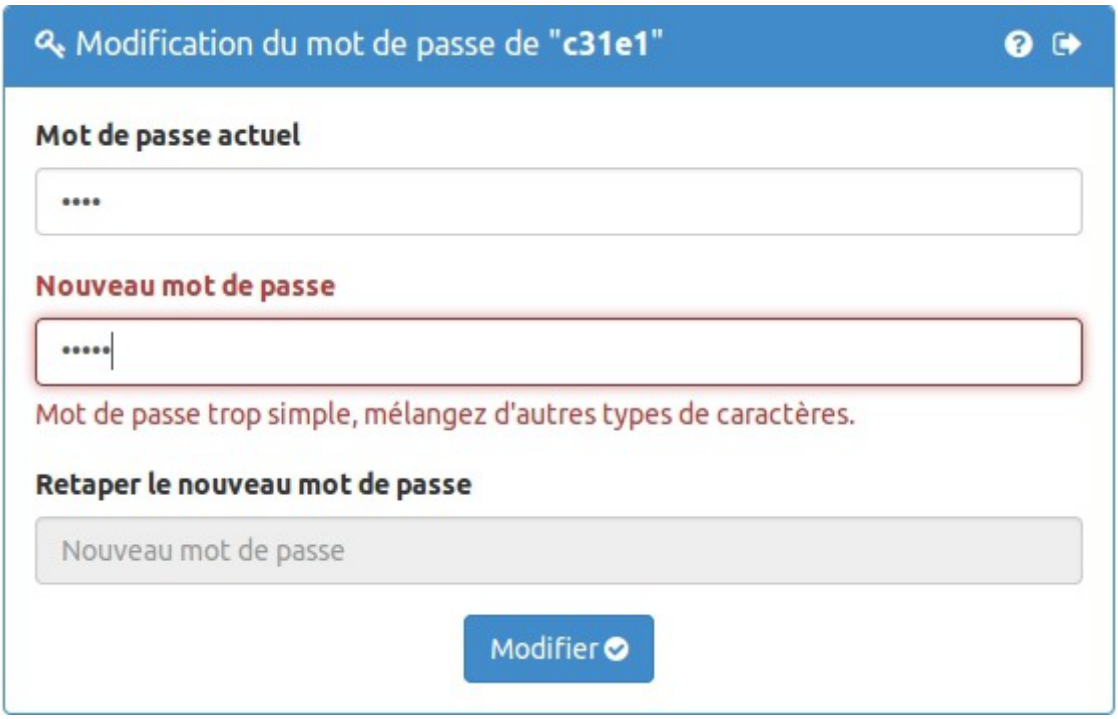
- Mots de passe : permet de modifier son propre mot de passe.

Voir aussi...

> EOP : application web à destination des enseignants [p.560]

12.3.5. EOE : outils à destination des élèves

Présentation



L'objectif de l'application web EOE (EOLE Outils Élèves) est de proposer une interface simple contenant un ensemble d'outils à destination des élèves. Cette nouvelle application permet, pour le moment, à l'élève de changer son mot de passe et peut être intégrée dans un portail. Le développement est basé sur le framework python Flask[p.890].

http://dev-eole.ac-dijon.fr/projects/eoe

Principale fonctionnalité

- possibilité de changer le mot de passe du compte élève.

Installation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette application est pré-installée sur le module Scribe à partir de la version 2.4.2.

Sur une version antérieure EOE n'est pas disponible.

Pour désactiver l'application il faut se rendre dans l'interface de configuration du module en mode normal, dans l'onglet Applications web et passer `Activer EOE (gestion de mot de passe élève)` à `non`.
L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Accéder à l'application

Pour accéder à l'application il faut se rendre à l'adresse : `https://<adresse serveur>/eoleapps/eleves/passperso`

Rôles des utilisateurs

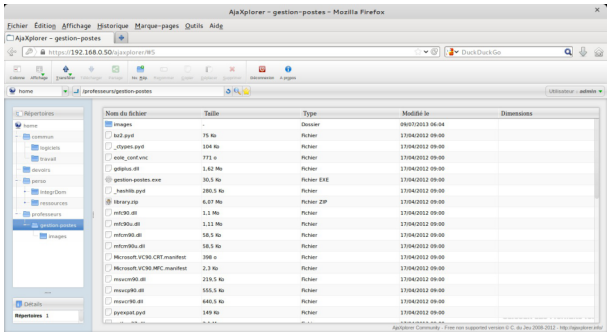
Les enseignants, les élèves ainsi que l'utilisateur `admin` (enseignants également) ont un accès à l'application.

12.4. Applications pré-packagées

Il est possible d'ajouter au module utilisé (AmonEcole, Scribe) des applications web pré-packagées dont l'installation est laissée à votre initiative.
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'entre elles pour plus d'informations.

12.4.1. Ajaxplorer : gestionnaire de fichiers

Présentation



Exploration de fichiers avec Ajaxplorer

Ajaxplorer est un gestionnaire de fichiers en ligne.
Ce gestionnaire permet de naviguer dans l'arborescence des fichiers utilisateurs. Il permet également l'édition de fichiers, l'écoute de fichiers audio, l'affichage d'images, ...
http://www.ajaxplorer.info

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Installation

Cette application est pré-installée sur les modules Scribe, AmonEcole.



L'application nécessite l'activation de l'accès FTP et l'utilisation d'un serveur EoleSSO local ou distant.

Dans l'interface de configuration du module, vérifier dans l'onglet Services, que la variable Activer l'accès FTP est à `oui` et que la variable Utiliser un serveur EoleSSO est à `local` ou à `distant`. Le paramétrage de EoleSSO s'effectue dans l'onglet Eole sso tandis que le paramétrage du serveur FTP se fait dans l'onglet Proftpd en mode expert.



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 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 : `http://<adresse serveur>/ajaxplorer/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO[p.902], ce service doit donc être actif.

Rôles des utilisateurs

Par défaut les rôles des utilisateurs sont assignés comme suit :

- **Administrateur**

  Seul l'utilisateur `admin` est administrateur de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer ce rôle en donnant les droits administrateur à un utilisateur.

- **Utilisateur authentifié**

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

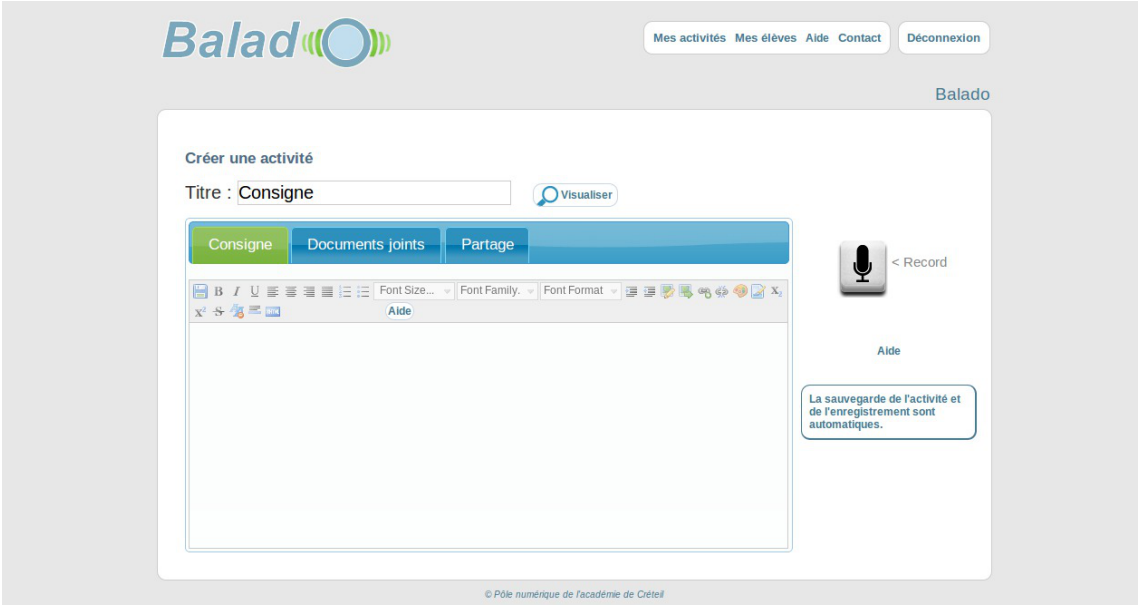
Tout utilisateur ayant un répertoire personnel sur le module Scribe possède un accès à l'application.

Remarques

Les comptes sont créés dans Ajaxplorer lors de la première connexion à l'application (initialisation du compte et des préférences).

Il est possible d'activer l'accès pour les enseignants aux dossiers personnels des élèves. L'option `Activer l'accès aux dossiers personnels des élèves pour les professeurs` se trouve dans le paramétrage du serveur FTP dans l'onglet `Proftpd` en mode expert, elle diminue légèrement la sécurité du serveur.

12.4.2. Balad((O)) : partager ses enregistrements



Dans le domaine éducatif, l'espace Balad((O)) de l'académie de Créteil permet de s'enregistrer directement en ligne et de partager ses enregistrements. Mais il offre plus que cela. D'abord, grâce aux flux RSS, c'est également un site de podcasting. Ensuite, la possibilité d'associer aux fichiers audio des images, des textes et des vidéos lui donne une véritable dimension pédagogique. L'espace Balad((O)) peut être utilisé comme un « labo de langues » asynchrone en ligne pour mettre en place des activités de classe, hors de la classe, c'est-à-dire des activités distantes et différées.

http://dev-eole.ac-dijon.fr/projects/balado

Installation de Balad((O))

Balad((o)) s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-balado
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 Applications web.

L'opération nécessite une reconfiguration du module avec la commande reconfigure.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/balado/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

- **professeur** : l'enseignant dispose d'un espace privé dans lequel il retrouve virtuellement ses élèves et ses groupes de classe. Après identification, il crée en ligne des activités qu'il diffusera à ses classes. Pour cela, il dispose d'un couple éditeur de texte / lecteur-enregistreur qui autorise une grande souplesse pour la préparation du travail.
- **élève** : chaque élève possède un accès personnalisé à l'espace Balad((O)). Une fois connecté, il accède aux activités préparées par ses professeurs avec tous leurs éléments : texte enrichi, enregistrement audio et pièces jointes qu'il télécharge d'un simple clic. Il écoute en ligne le fichier audio, mais il peut également le sauvegarder en local pour l'écouter ultérieurement, indépendamment de tout accès à Internet, et le transférer éventuellement sur son baladeur.

Remarques

Présentation vidéo

http://balado.crdp-creteil.fr/presentation

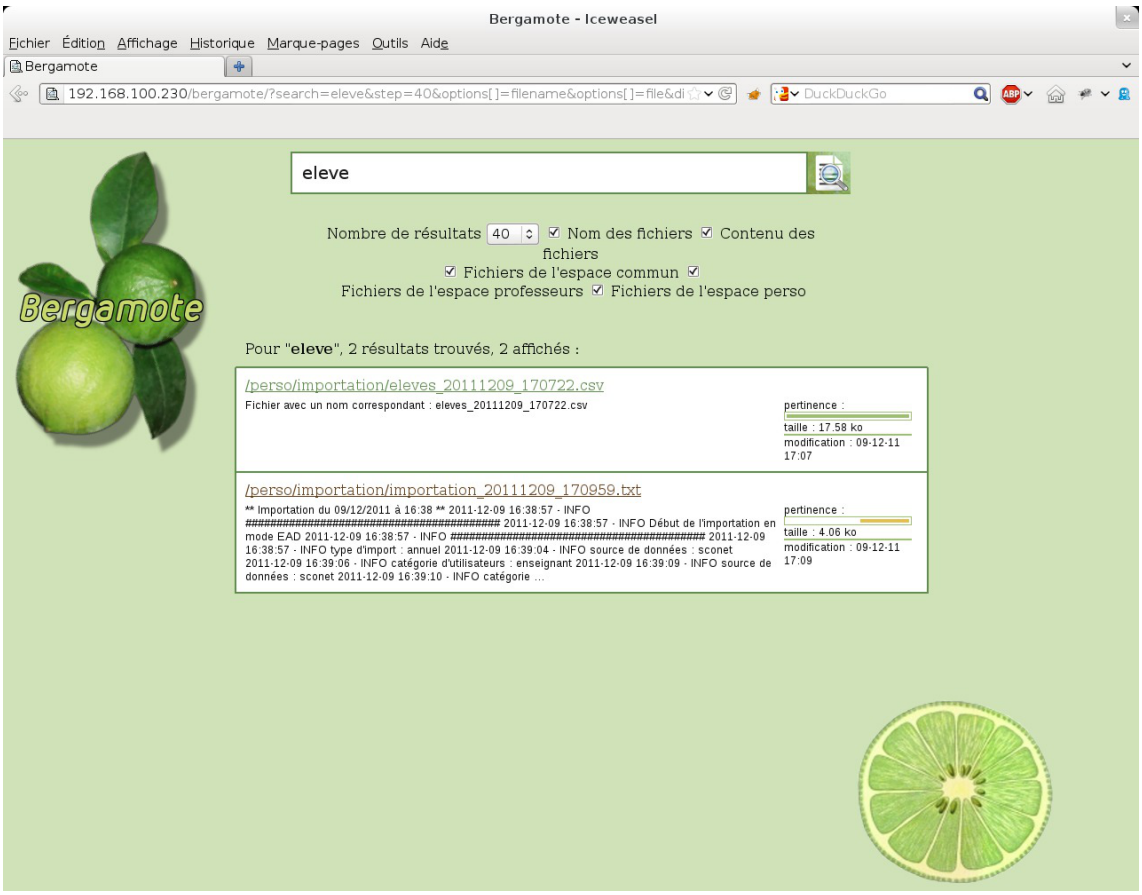
Fiches techniques

http://mediafiches.ac-creteil.fr/spip.php?article145&id_mot=3

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.4.3. Bergamote : indexation et recherche de fichier

Présentation



Bergamote est un outil qui permet l'indexation et la recherche des fichiers hébergés sur le serveur de fichiers Samba du module Scribe.

Cette application est basée sur le moteur de recherche Xapian et le logiciel de composition typographique multilingue Omega.

http://gitlab.com/bergamote/bergamote

Installation de Bergamote

Bergamote s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-bergamote
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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 `Applications web`.
>
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/bergamote/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

L'indexation des fichiers recherche dans les répertoires personnels et dans répertoires liés aux groupes de l'utilisateur. Pour le moment si l'utilisateur est dans un groupe mais qu'il n'a pas les droits suffisants le document apparaît dans le recherche mais il ne peut pas y accéder.

Remarques

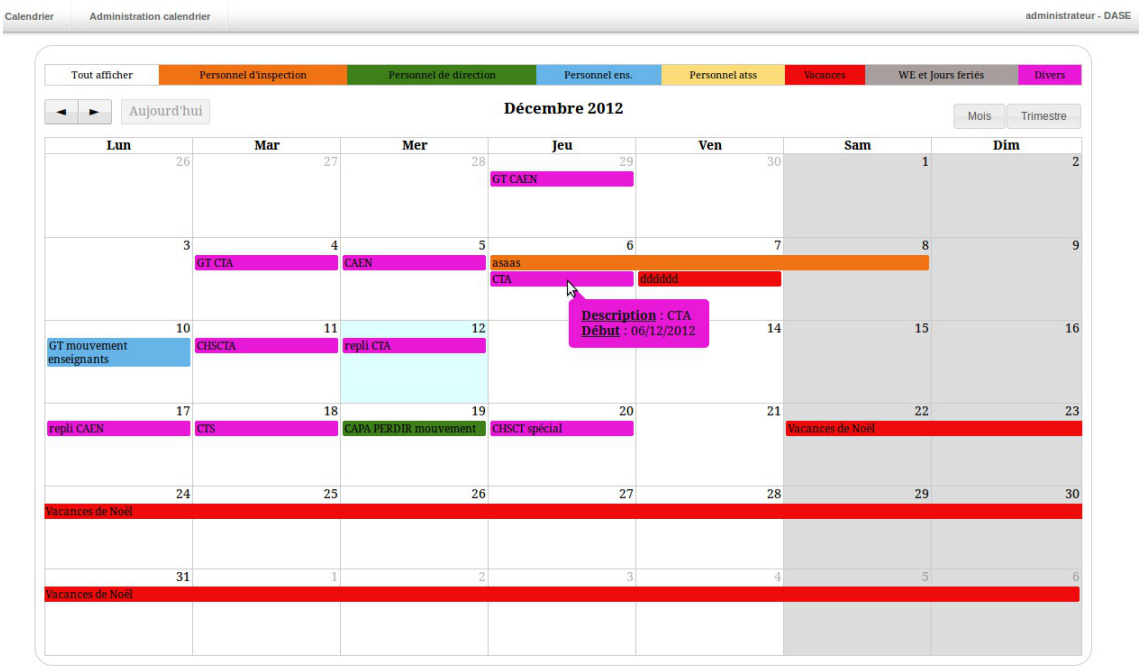
L'indexation des fichiers se fait par le biais d'une tâche `cron` lancée toutes les heures.

Le fichier se trouve dans `/etc/cron.hourly/`.

12.4.4. Calendrier : gestion des événements

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Consultation du calendrier dans le portail Envole

Le calendrier de gestion des événements est une application développée en PHP/MySQL et utilisant jQuery.

Elle permet la gestion d'événements sur un calendrier en vue mensuelle et trimestrielle.

http://dev-eole.ac-dijon.fr/projects/calendrier

Installation de Calendrier

Calendrier s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-calendrier
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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`.

Accès à l'application

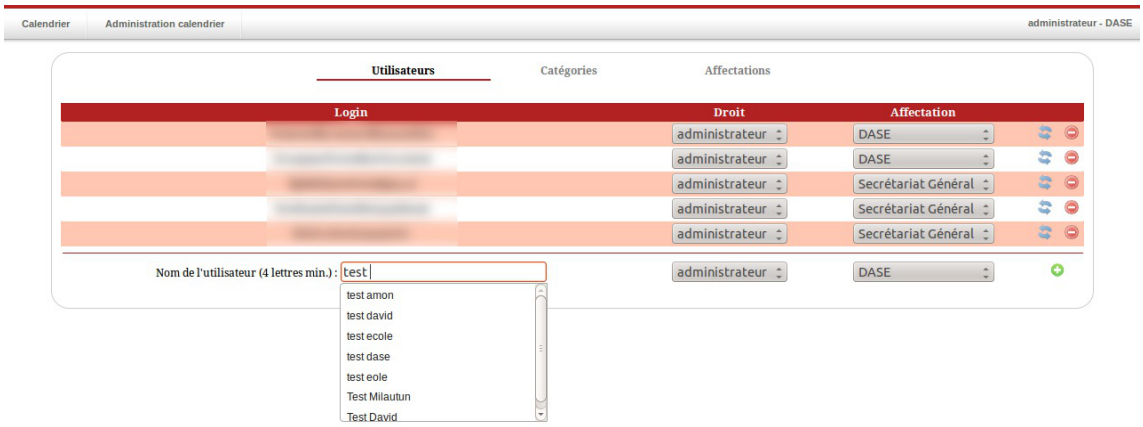
Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/calendrier/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Sur la page d'administration, il est possible de définir les utilisateurs ayant des droits spécifiques (administrateurs et éditeurs).

Un administrateur possédera tous les droits, alors qu'un éditeur pourra seulement créer des événements, et modifier ceux de son affectation.



Consultation du calendrier dans le portail Envole

Un utilisateur non connu dans de la base n'aura accès au calendrier qu'en lecture seule.

Remarques

Une documentation plus complète est disponible sur le site dédié à Envole : https://envole.ac-dijon.fr/wordpress/2012/12/12/610

12.4.5. CDC : carnet de correspondance

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Fenêtre de saisie d'un mot dans le carnet

CDC est une application qui reproduit le fonctionnement d'un carnet de correspondance : échange entre responsables et administratifs, affichage et validation du règlement intérieur.

Les notes et les absences sont des fonctionnalités qui ne sont pas disponibles dans CDC.

http://dev-eole.ac-dijon.fr/projects/cdc

Installation de CDC

CDC s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-cdc
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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 `Applications web`.
>
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/cdc/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

L'accès à l'interface d'administration se fait dans l'application une fois connecté en tant que `admin`.

Rôles des utilisateurs

Seul l'utilisateur `admin` est "administrateur" de l'application.

Il a un accès complet à l'application et à sa configuration.

Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.

Les rôles présents dans l'annuaire OpenLDAP (enseignants, élèves, ...) sont reportés dans l'application.

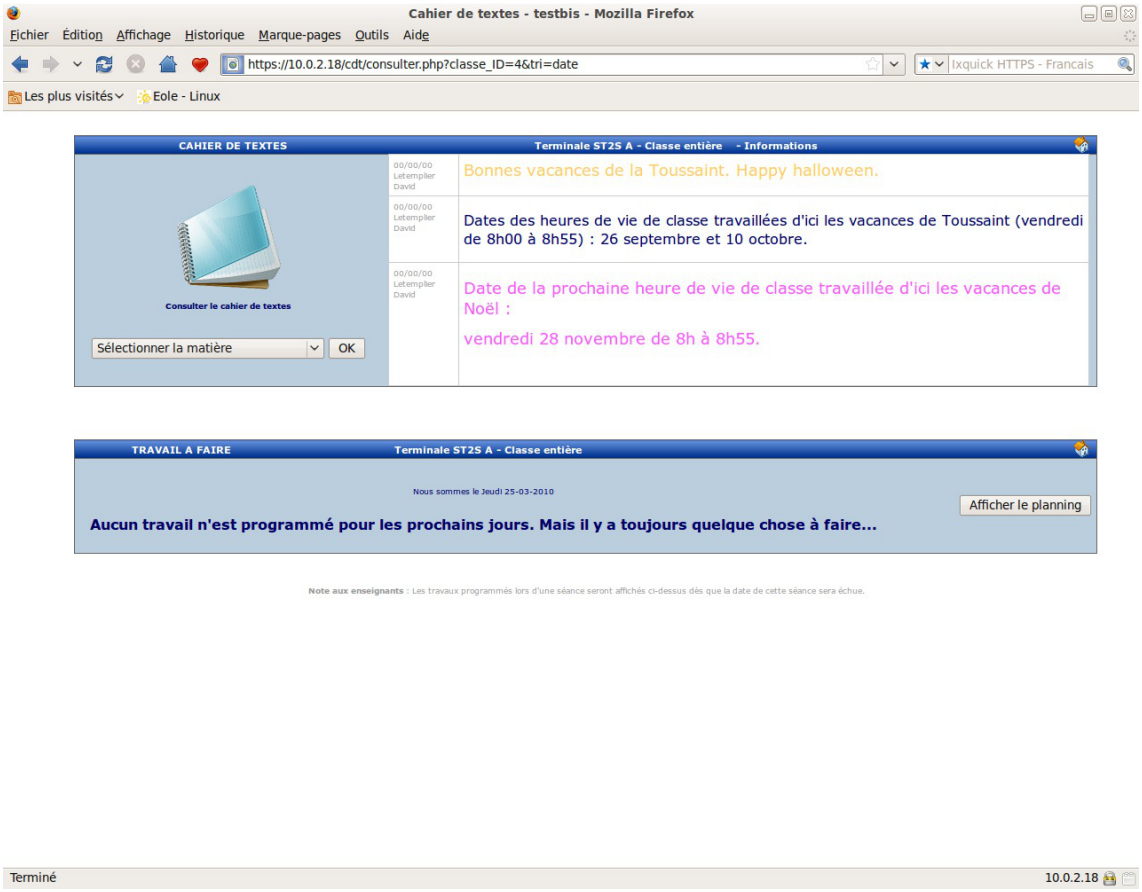
Remarques

Les comptes sont créés par l'intermédiaire d'un script d'importation LDAP disponible dans le `Tableau de bord`.

12.4.6. Cdt : cahier de texte numérique

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Utilisation de Cdt

Cdt est un cahier de texte numérique.

Il permet aux enseignants la saisie des devoirs dans le cahier de texte et la consultation pour les élèves.

http://www.etab.ac-caen.fr/bsauveur/cahier_de_texte [http://www.etab.ac-caen.fr/bsauveur/cahier_de_texte]

Cdt est également surnommé *Chocolat*.

Cette application est sous licence GPL mais en marge de cette licence vous êtes convié à offrir une tablette de chocolat au développeur de l'application.

http://www.etab.ac-caen.fr/bsauveur/cahier_de_texte/?page_id=6

Installation

Cdt s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-cdt
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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 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 : `http://<adresse serveur>/cdt/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tout utilisateur présent dans l'annuaire possède un accès à l'application.

Les profils administrateur, élève, responsable, professeur, direction (DIR) et vie scolaire (EDU) sont automatiquement associés aux rôles correspondants dans l'application.

Tout autre profil se voit créé un compte bloqué, charge à l'administrateur d'y associer le bon rôle.

Administrateur

L'utilisateur `admin` est administrateur de l'application, il peut notamment procéder à l'import des emplois du temps depuis les fichiers issus de SIECLE : sts_emp_xxx.xml / emp_sts_xxx.xml .

Professeur

Les enseignants ont un accès professeur à l'application, ils enregistrent leur emploi du temps afin de pouvoir ensuite gérer leurs séances de cours.

Élève

Les élèves peuvent seulement consulter le cahier de texte, ils ne peuvent pas l'éditer mais accèdent automatiquement au contenu de leur classe (séances et travail à faire).

Responsable

Les responsables peuvent seulement consulter le cahier de texte, ils ne peuvent pas l'éditer mais accèdent automatiquement au contenu des classes de leurs enfants (séances et travail à faire).

Personnel de direction

Ils gèrent les visas, diffusent des messages, planifient des événements et accèdent aux différentes

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

données du cahier de textes.

Vie Scolaire
Ils diffusent des messages, planifient des événements et accèdent aux différentes données du cahier de textes.

Invité
Ce rôle permet de donner un accès à certains cahiers de textes.On peut être "invité" sans avoir de compte (ldap), pour cela la direction (pour chaque enseignant), ou un enseignant lui-même, dispose d'une url sécurisée à transmettre pour un accès anonyme.

Importation des emplois du temps

L'importation s'effectue depuis le menu de l'administrateur : `Importation de données depuis SIECLE/STS-Web`.

Pour plus de détails, consulter la page : http://dev-eole.ac-dijon.fr/projects/cdt/wiki/Wiki#Importation-des-emplois-du-temps

Activation des sondes piwik

Les sondes permettent de comptabiliser les accès enseignant et en consultation.

Elles ne sont pas actives par défaut.

On les active en renseignant les valeurs `envole_piwik_url` (sans le http://) et `envole_piwik_idsite` dans la table `cdt_params` qui sont présentes mais valant respectivement "" et 0.

Pour plus de détails, consulter la page : http://dev-eole.ac-dijon.fr/projects/envole/wiki/SondesPiwik

Exemples de requêtes

```
UPDATE `cdt_params` SET `param_val`="etablissement.ac-creteil.fr/piwik2/" WHERE `param_nom`='envole_piwik_url';
UPDATE `cdt_params` SET `param_val`="2" WHERE `param_nom`='envole_piwik_idsite';
```

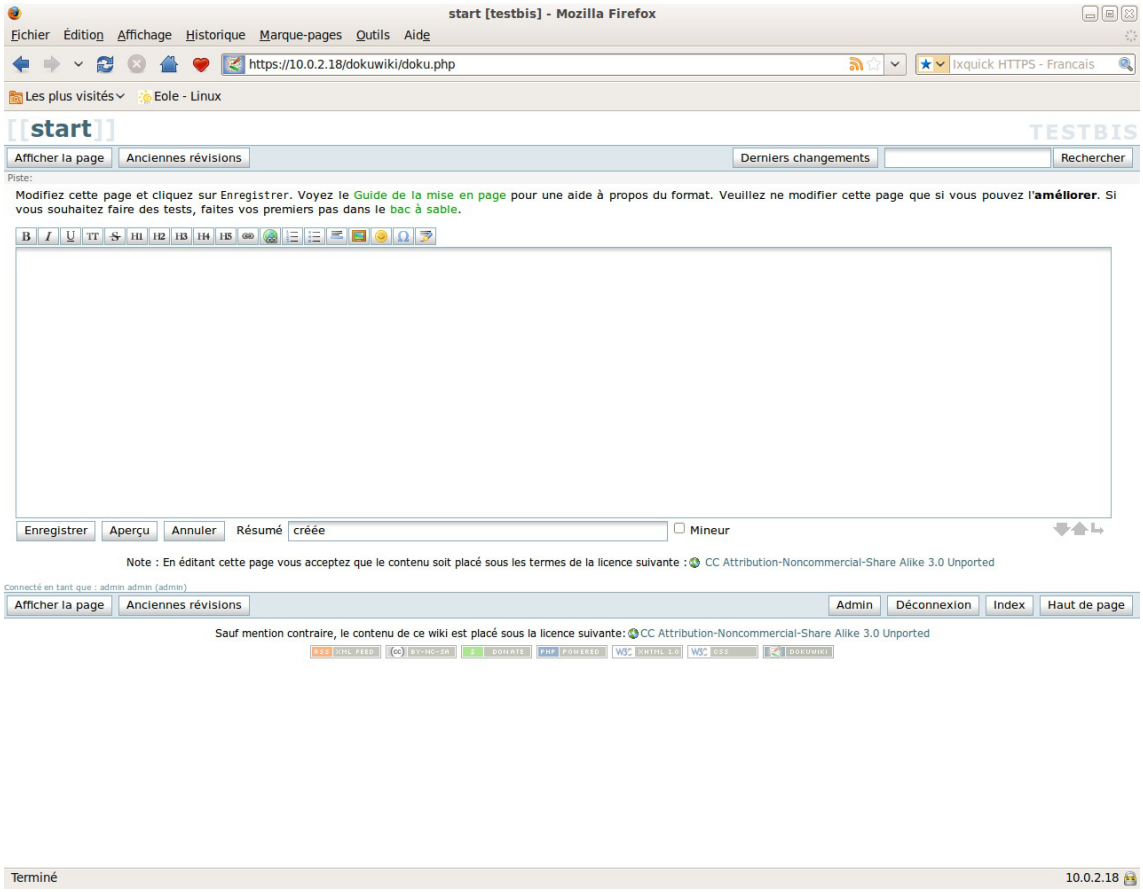
Remarques

- Lorsque **Webcalendar** est activé en même temps que **Cdt**, les informations rentrées dans le cahier de texte (emploi du temps importé depuis SIECLE, devoirs) sont automatiquement visibles sur l'agenda d'un enseignant ou d'un élève. Cette fonctionnalité est activée par défaut.
- Depuis la version 4.9.0.2, la mise à jour de la base de données est réalisée automatiquement sans intervention de l'administrateur.

12.4.7. Dokuwiki : rédaction à plusieurs

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Page d'accueil de Dokuwiki

DokuWiki est un Wiki simple d'utilisation. Il permet l'édition et la rédaction commune entre plusieurs utilisateurs.

http://www.dokuwiki.org/

Installation

DokuWiki s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-dokuwiki
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Il existe un paquet **dokuwiki** qu'il ne faut pas confondre avec le paquet **eole-dokuwiki**.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 `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 : `http://<adresse_serveur>/dokuwiki/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

- **administrateur**

  Seul l'utilisateur `admin` est administrateur de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer se rôle à un autre utilisateur mais aussi à un groupe d'utilisateurs.

  Il peut aussi, ajouter des privilèges à un ou plusieurs utilisateurs.

- **@ALL**

  Toute personne ayant un compte authentifié sur Scribe est "ALL" mais n'a aucun droit.

- **@professeurs**

  Les enseignants peuvent créer des nouvelles pages et éditer.

- **@eleves**

  Les élèves ont le droit de lecture sur l'ensemble du wiki.

- **@administratifs**

  Les administratifs n'ont pas de droit sur le wiki

- **visiteur anonyme**

  Ne peut pas accéder à l'application.

Sur le module Horus, l'utilisateur `admin` est administrateur de l'application et les autres utilisateurs n'ont par défaut aucun droit.

Les rôles sont directement modifiables dans l'application par l'administrateur :

`http://<adresse_serveur>/dokuwiki/doku.php?id=start&do=admin&page=a`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Remarques

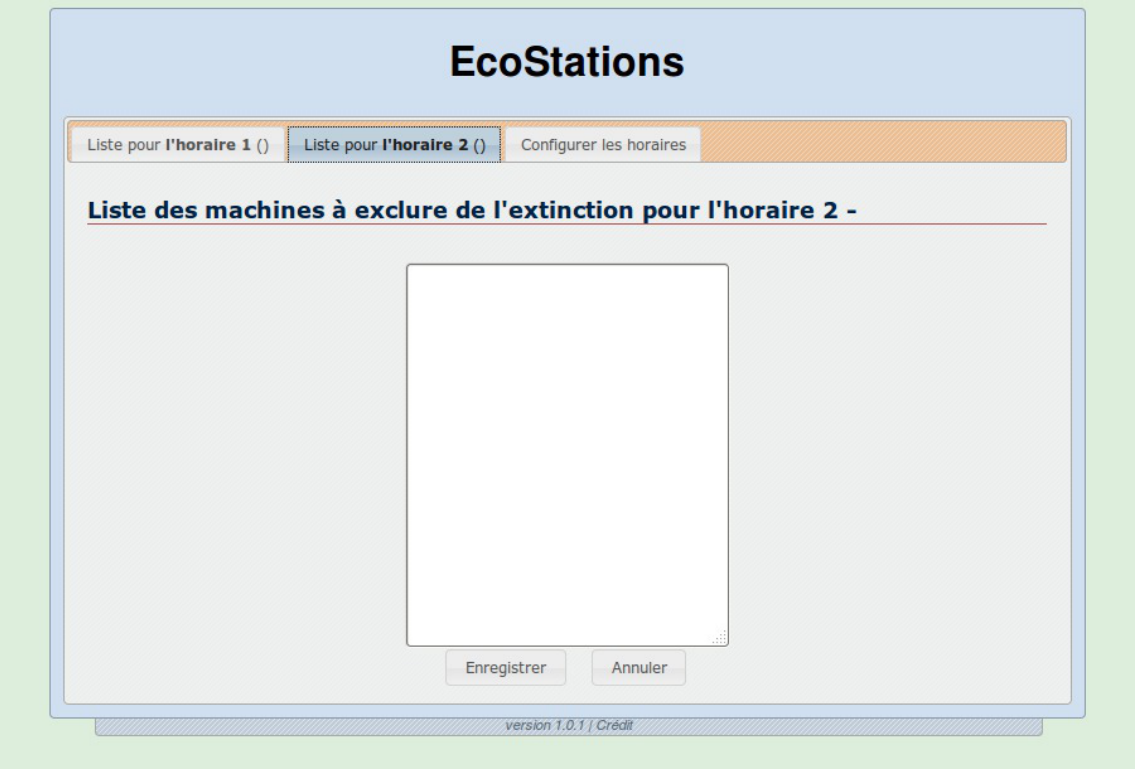
Les données utilisateurs relatives à l'application sont stockées dans le répertoire `data/` de l'application et sont sauvegardées par Bareos.

Il existe 3 fichiers de configuration pour Dokuwiki :

- `dokuwiki.php` → le fichier principal ;
- `local.php` → le fichier secondaire est vide pour utilisation ultérieure ;
- `local.protected.php` → le fichier protégé qui contient les configurations sensibles :
  - la méthodes d'authentification ;
  - les informations relatives à l'annuaire LDAP ;
  - l'emplacement du répertoire qui contient les données de Dokuwiki.

12.4.8. ecoStations : gérer l'extinction et l'allumage des postes à des horaires donnés

Présentation



ecoStations est un outil qui permet d'éteindre le parc informatique d'un établissement suivant une procédure assez souple pour permettre d'intégrer la notion d'internat par exemple ou de station à laisser allumée constamment.

Il faut renseigner via une interface web, deux listes de stations du parc L1 et L2 ainsi que deux horaires distincts H1 et H2.

À l'heure H1, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L1 ; puis à l'heure H2, toutes les stations de l'établissement seront éteintes exceptées les stations listées dans L2.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ainsi, les stations listées dans L1 et L2 ne seront pas éteintes.

ecoStations a été développé en étroite collaboration entre Olivier Hacquard, Pascal Ratte, Laurent Etignard, Frédéric Lamy, Valéry Georges et Jérôme Labriet.

La documentation d'utilisation (disponible dans l'espace contribution) a été rédigée par Pierre Mariot.

http://dev-eole.ac-dijon.fr/projects/ecostations/

Montée de version de l'application ecoStations

L'application ecoStations qui permet de gérer l'extinction et l'allumage des postes à des horaires donnés passe en version 2.4.8.

L'ajout d'un script permet notamment d'annuler le re-démarrage d'une station.

Installation d'ecoStations

ecoStations s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-ecostations
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



L'application fonctionne uniquement sur le module Scribe.



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
```

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/ecostations`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

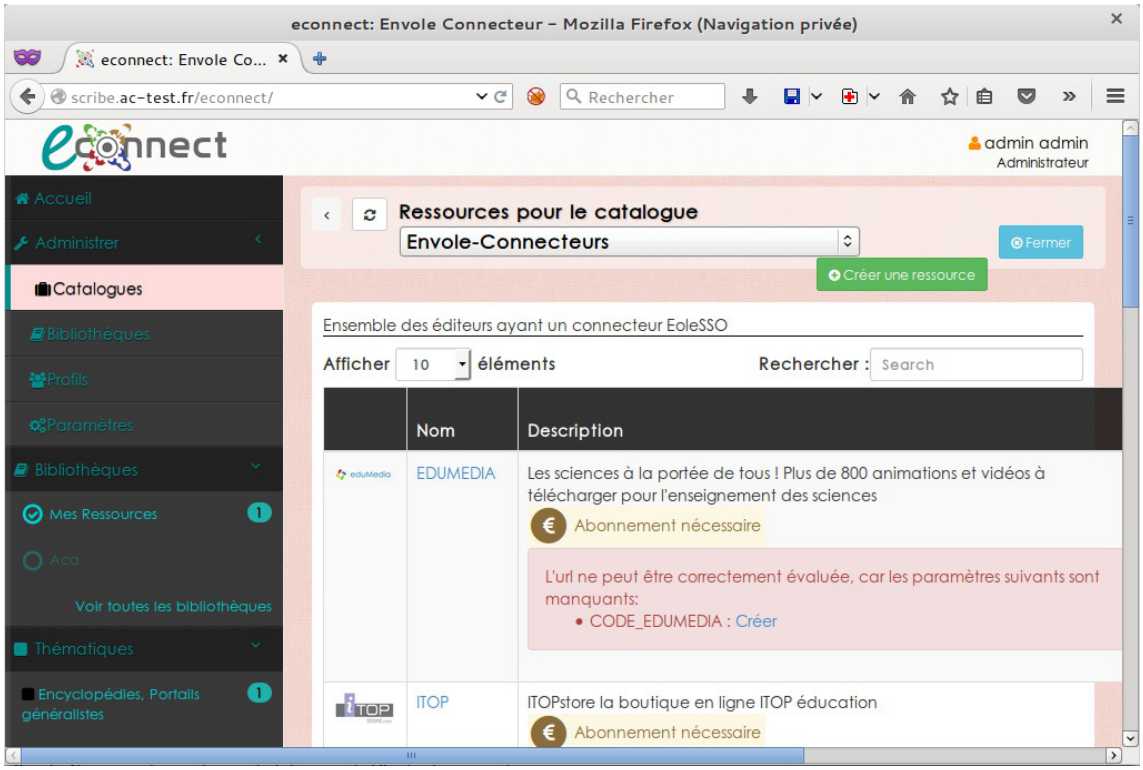
Utilisation

Les postes clients doivent avoir été pré-configurés avec `power_config.cmd` afin de supprimer la mise en veille automatique qui bloque l'ordre d'extinction.

Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante :
http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

12.4.9. eConnect : centralisation et mise à disposition de ressource en ligne

Présentation



Page d'accueil de Dokuwiki

eConnect une application permettant de centraliser l'activation/configuration via une interface web des connecteurs et la mise à disposition des ressources dans Envole pour les utilisateurs.
http://dev-eole.ac-dijon.fr/projects/envole-connecteur/

Installation

eConnect s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
# apt-eole install eole-envole-connecteur
```

L'application n'est pas disponible immédiatement après l'installation.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `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 : `http://<adresse_serveur>/econnect/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Seul l'utilisateur `admin` est administrateur de l'application.

Remarques

eConnect, n'a pas vocation à gérer les abonnements avec l'éditeur, mais uniquement de configurer le serveur eoleSSO et de mettre à disposition les ressources. Il est donc toujours nécessaire que l'établissement prenne contact avec l'éditeur pour acheter la ressource. D'une manière générale, l'éditeur va configurer son service SSO et communiquer un code d'activation à l'établissement. Code d'activation que l'établissement pourra gérer directement dans eConnect.

eConnect, va permettre également de mettre à disposition des ressources ne nécessitant pas de connecteurs SSO. Comme par exemple, des ressources gratuites.



eConnect, pourra aussi bien s'installer sur un serveur Scribe que sur un serveur Seshat pour une centralisation académique. Dans le cas d'une centralisation académique, un profil administrateur local sera créé donnant ainsi à une (ou des) personne(s) d'un établissement

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> les droits pour la mise à disposition des ressources en fonction de ses abonnements.

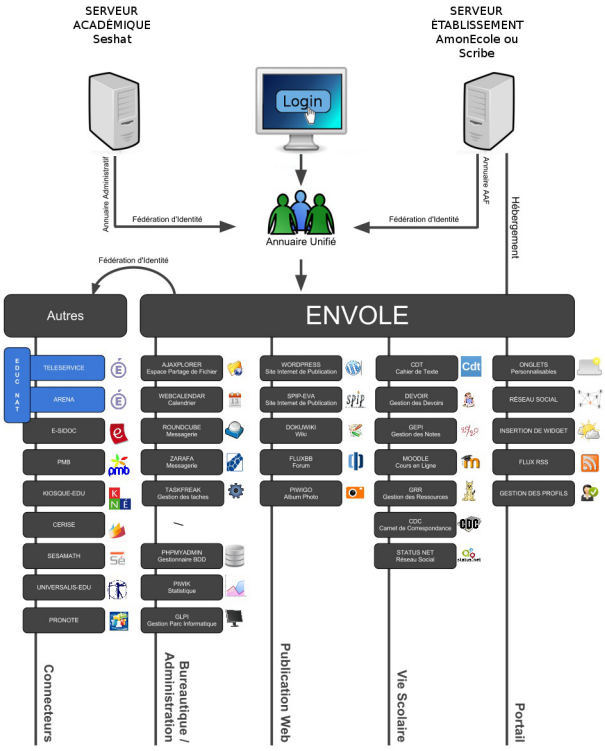
12.4.10. Envole : Espace Numérique Personnel pour l'Éducation

Présentation

Envole est un Espace Numérique Personnel[p.889] pour l'Éducation.

Il propose une interface de type portail Web 2.0[p.904] qui permet l'interaction entre un utilisateur et son environnement numérique résultant de l'utilisation de services hétérogènes.

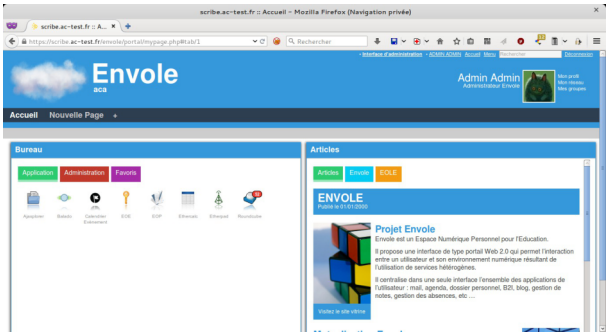
Il centralise dans une seule interface l'ensemble des applications de l'utilisateur : mail, agenda, dossier personnel, B2I, blog, gestion de notes, gestion des absences, etc ...



Panorama d'Envole

Envole est adapté pour mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Établissement (PIE) ou un Espace Numérique de Travail (ENT).

Envole est personnalisable par l'administrateur (changer le thème, imposer des onglets et des widgets, concevoir des widgets) et par l'utilisateur (ajouter des onglets et des boutons, gérer ses marque-pages, utiliser des widgets).



Portail et Bureau d'accès rapide aux applications

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le site de la mutualisation interacadémique : http://envole.ac-dijon.fr
Le site de l'ENT Envole : http://www.ent-envole.com

Installation du portail Envole

Envole s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-posh
```



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire possèdent un accès à l'application.

- **administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application, il peut :

  - Configurer les onglets
  - Configurer des widgets
  - Administrer la gestion des profils.

Remarques

Une partie dédiée de la documentation détaille le paramétrage de Envole.

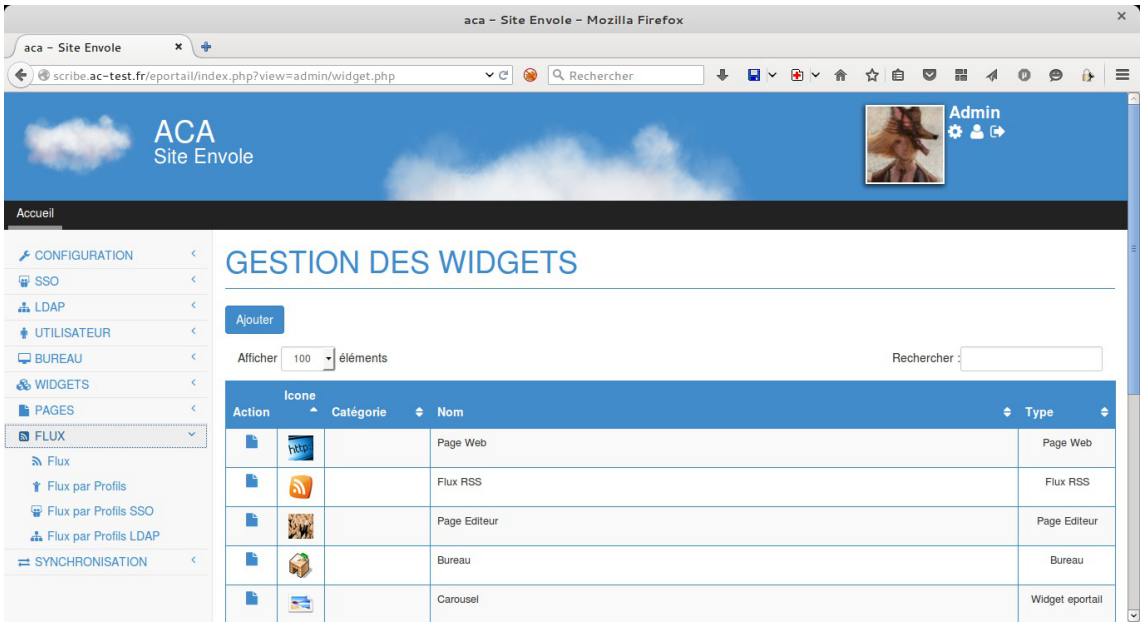
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Voir aussi...

> Espace Numérique Personnel pour l'Éducation avec Envole [p.649]

12.4.11. ePortail : portail d'entreprise

Présentation



Page d'accueil de Dokuwiki

ePortail est un portail d'entreprise tourné vers l'intranet comme l'extranet.

http://dev-eole.ac-dijon.fr/projects/eole-eportail

Installation

ePortail s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-eportail
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .



> 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
> ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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 `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 : `http://<adresse serveur>/eportail/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire possèdent un accès à l'application.

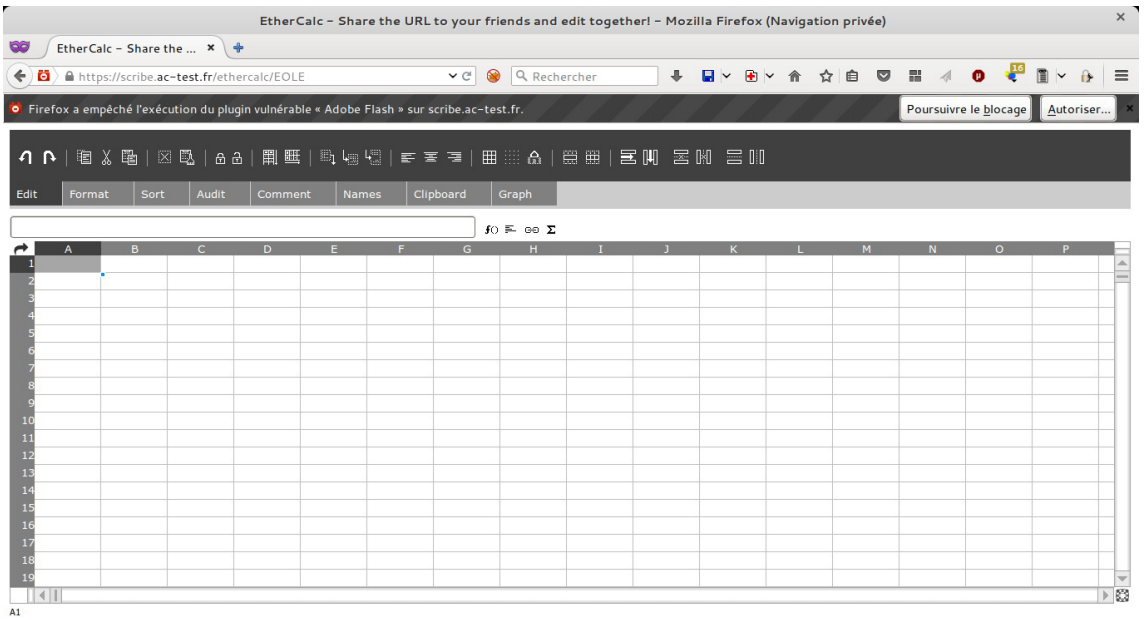
- **administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application, il peut :

  - Configurer les onglets
  - Configurer des widgets
  - Administrer la gestion des profils.

12.4.12. EtherCalc : tableur collaboratif

Présentation



EtherCalc est un tableur collaboratif en temps réel, libre, écrit en JavaScript. Il s'agit donc d'une feuille de calcul où les contributions de chacun apparaissent immédiatement sur l'écran de tous les participants.

http://ethercalc.net/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Installation de EtherCalc

EtherCalc s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-ethercalc
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/ethercalc/`

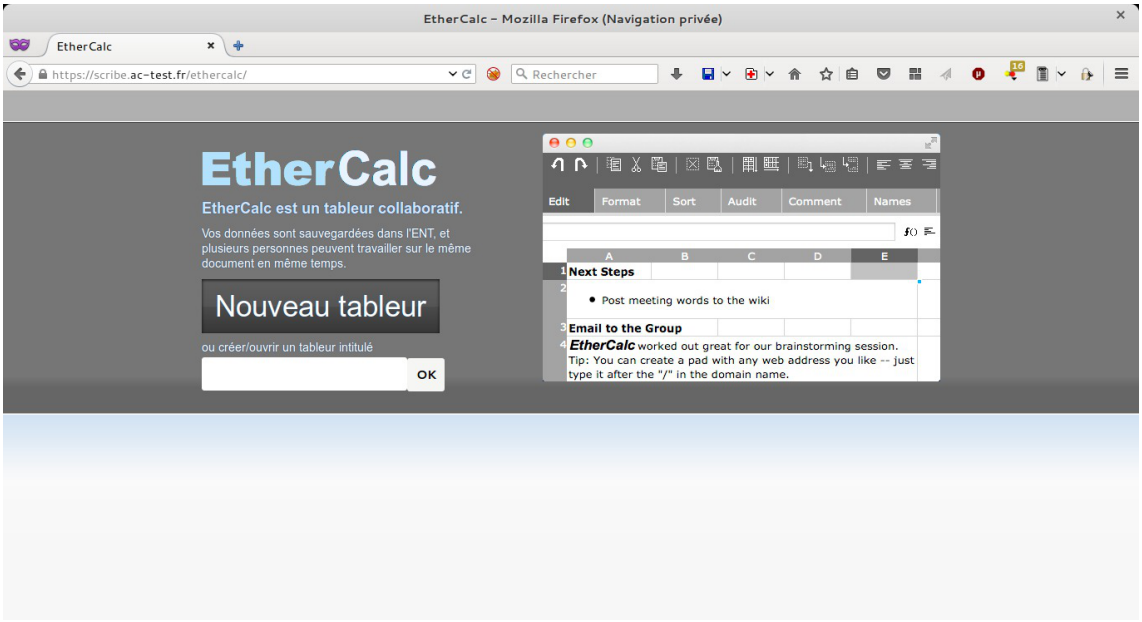
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.



Le symbole `/` est obligatoire à la fin de l'URL pour pouvoir accéder à l'application : `http://<adresse_serveur>/ethercalc/`

À la connexion l'application propose la création d'un nouveau tableur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Rôles des utilisateurs

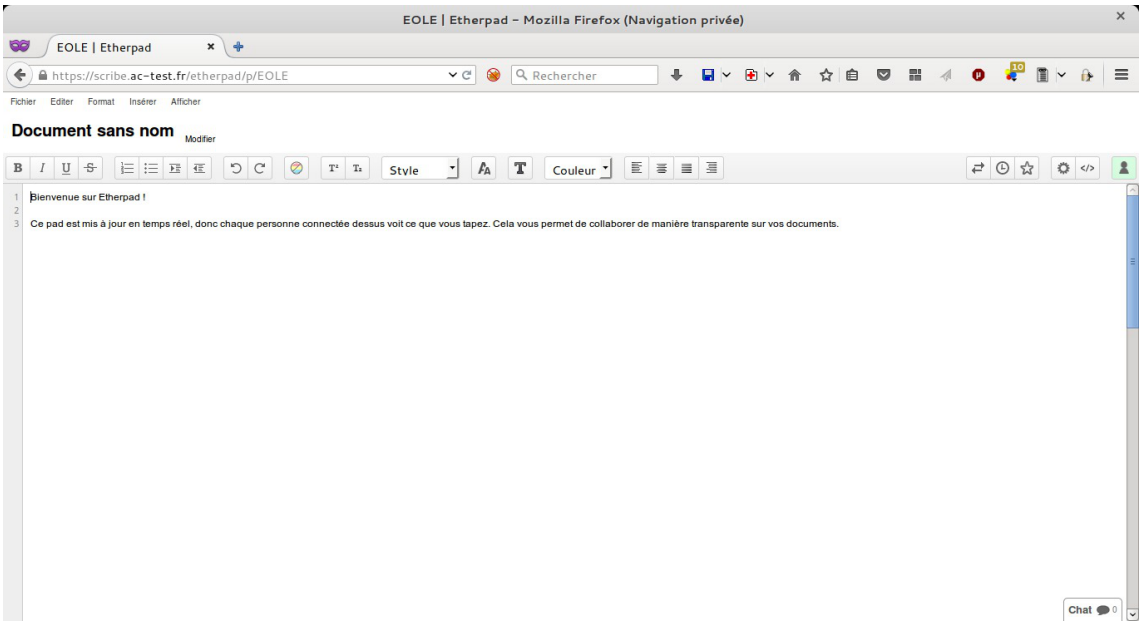
Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

Remarques

Le port d'écoute d'EtherCalc est par défaut `9002`, ce paramètre peut être changé dans l'onglet `Applications web` de l'interface de configuration du module.

12.4.13. EtherPad : écriture collaborative

Présentation



EtherPad est un éditeur de texte libre en ligne fonctionnant en mode collaboratif et en temps réel. Il

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

permet à plusieurs personnes (16 par défaut) de partager l'élaboration simultanée d'un texte, et d'en discuter en parallèle, via une messagerie instantanée.

Il peut avoir des usages pédagogiques, notamment pour l'apprentissage collaboratif.

http://etherpad.org/

Installation de EtherPad

EtherPad s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-etherpad
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/etherpad/`

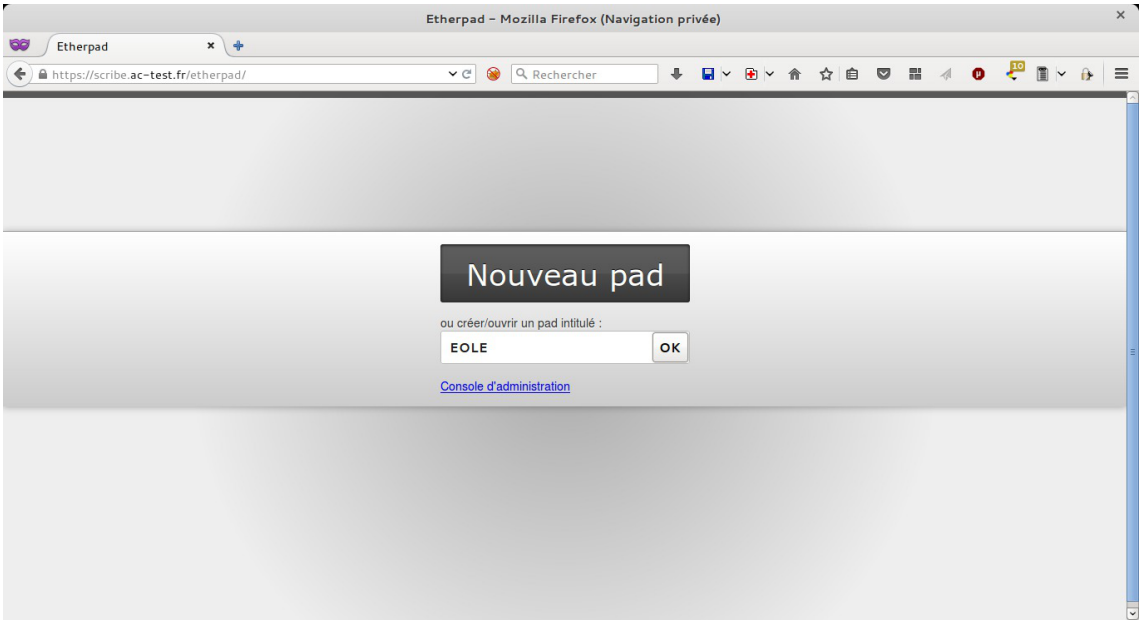
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.



Le symbole `/` est obligatoire à la fin de l'URL pour pouvoir accéder à l'application : `http://<adresse serveur>/etherpad/`

À la connexion l'application propose la création d'un nouveau pad[p.897].

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Rôles des utilisateurs

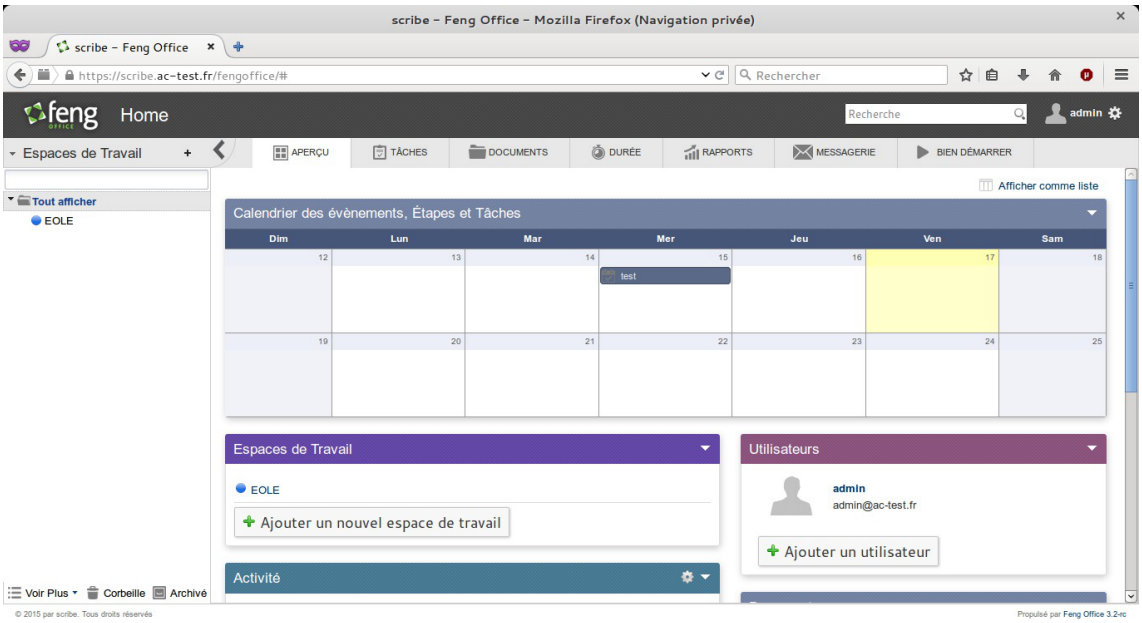
Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

Remarques

Le port d'écoute d'EtherPad est par défaut `9001`, ce paramètre peut être changé dans l'onglet `Applications web` de l'interface de configuration du module.

12.4.14. Feng Office : plateforme collaborative

Présentation



Feng Office est une suite bureautique en ligne comparable à Google Apps et Zimbra. Les

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

caractéristiques principales incluent entre autres la gestion documentaire, la bureautique, les contacts, les courriels, la gestion de projet.

Feng Office peut aussi être vue comme une suite collaborative et comme un logiciel de Gestionnaire d'informations personnelles.

http://www.fengoffice.com

Installation de Feng Office

Feng Office s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-fengoffice
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/fengoffice/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

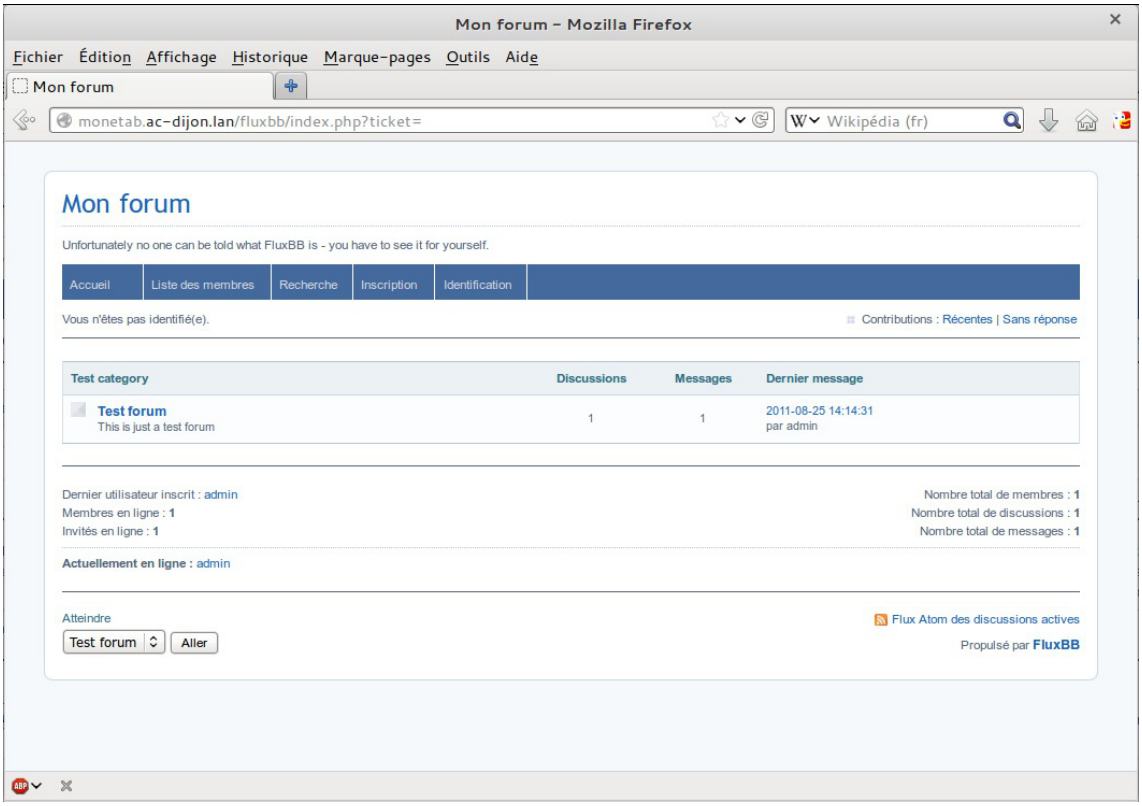
L'application est CASsifiée et une synchronisation des comptes est disponible dans posh-profil mais uniquement mode synchronisation "annuaire".

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Le mode de synchronisation "annuaire" est paramétrable dans l'interface de configuration du module dans l'onglet Envole.

12.4.15. FluxBB : forum de discussions

Présentation



Page d'accueil d'un forum FluxBB

FluxBB est une application web de forum de discussions basé sur PunBB.

Il offre moins de fonctionnalités que beaucoup d'autres forums, mais il est généralement plus rapide.

http://fluxbb.fr/

Installation de FluxBB

FluxBB s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-fluxbb
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande reconfigure.



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/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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 `Applications web`.
>
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/fluxbb/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire possèdent un accès à l'application.

- **administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application, il peut :

  - Organiser les catégories et forums.
  - Définir les options et préférences pour chaque forum.
  - Contrôler les permissions pour les utilisateurs et les invités.
  - Afficher les statistiques IP des utilisateurs.
  - Exclure des utilisateurs.
  - Censurer des mots.
  - Paramétrer les statuts d'utilisateurs.
  - Élaguer d'anciens messages.
  - Traiter les signalements de messages.

- **modérateur**

  Seuls les professeurs sont modérateurs du forum, ils peuvent :

  - Exclure des utilisateurs.
  - Censurer des mots.
  - Paramétrer les statuts d'utilisateurs.
  - Traiter les signalements de messages.

- **membre**

  Les élèves sont membres du forum, ils peuvent :

  - créer de nouvelle discussion
  - répondre à une discussion

- **invité**

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les personnes non authentifiées, les responsables et les administratifs ont le rôle invité.

Ils peuvent consulter le forum.

12.4.16. Gepi : gestion des notes, des absences, et des cahiers de texte

Présentation



Administration de Gepi

Gepi est un logiciel libre de gestion des notes, des absences, et des cahiers de texte pour les établissements francophones du second degré.

http://gepi.mutualibre.org

Une grande quantité de documentation est disponible ici :

https://www.sylogix.org/projects/gepi/wiki/

Installation

Gepi s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-gepi
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 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>/gepi/`

L'authentification peut se faire :

- par le biais d'une authentification SSO (`Utilisation du service SSO pour les applications de votre serveur scribe` à `oui`) ;
- par le biais d'une authentification LDAP.



Pour des raisons de sécurité évidentes, l'accès en HTTPS est fortement recommandé.

De plus il permet d'éviter l'affichage des messages d'avertissement lors d'une session en tant qu'utilisateur `admin`.

Importation des comptes

En début d'année, un outil de synchronisation des bases permet de créer l'ensemble des comptes utilisateurs depuis l'annuaire LDAP du module Scribe.



L'initialisation des bases supprime un grand nombre de données déjà entrées.

L'import ne doit donc être réalisé qu'**une seule fois** en début d'année.

La mise à jour des informations importées est réalisée lors de la connexion des utilisateurs.

- se connecter en tant qu'utilisateur `admin` à l'application ;
- si l'application était déjà utilisée, consulter http://www.sylogix.org/projects/gepi/wiki/Avant_initialisation ;
- se rendre dans Gestion générale / Initialisation à partir de l'annuaire LDAP du serveur Eole Scribe NG ;
- lancer les 7 étapes, dans l'ordre.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les données importées nécessitent par la suite quelques réglages :

- attribution des rôles adéquats au personnel administratif ;
- regroupement d'enseignements inter-classe ;
- ... .

Affectation des matières à des professeurs

En tant qu'utilisateur `admin`, aller dans :

`Gestion des bases` / `Gestion des comptes d'accès des utilisateurs` / `Personnels de l'établissement` / `Affecter les matières aux professeurs`.

Ajouts d'enseignements

- Aller dans `Gestion des bases` / `Gestion des classes` ;
- Choisir une classe dans le tableau puis cliquer sur `Enseignements` ;
- En haut à droite "Ajouter des enseignements" et choisir dans la liste "Sélectionner matière".
- Cliquer sur `Créer`.

Il est possible par la suite de ré-éditer ces enseignements pour :

- Ajouter un ou des professeurs à l'enseignement ;
- Associer une autre ou d'autres classes à l'enseignement.

Lors de la création d'un enseignement, tous les élèves de la classe sont par défaut inscrits dans l'enseignement.

Il faut passer en revue les enseignements optionnels pour décocher les élèves qui ne suivent pas l'enseignement.

Pour cela, toujours dans la Gestion des classes :

- `Gestion des bases` / `Gestion des classes`
- Choisir une classe dans le tableau puis cliquer sur `Enseignements`.
- Choisir dans le tableau l'enseignement puis cliquer sur `<Enseignement> Élèves inscrits (XX-XX-XX)`.
- Choisir un élève dans le tableau et utiliser les coches pour choisir les périodes ou utiliser la croix rouge pour tout décocher.
- Enregister vos changements.

Ajouter un enseignement à cheval sur plusieurs classes

- Aller dans `Gestion des bases` / `Gestion des classes` ;
- Choisir une classe dans le tableau puis cliquer sur `Enseignements`.
- En haut à droite, "Ajouter des enseignements" et choisir dans la liste "Sélectionner matière" en précisant qu'il concerne plusieurs classes (bouton radio) ;
- Cliquer sur `Créer` ;
- Préciser le nom de l'enseignement (regroupement) ;
- Cocher les classes et le(s) enseignant(s) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Cliquer ensuite sur le lien `Eleves (XX-XX-XX)` pour cocher / décocher les élèves qui doivent suivre ou non l'enseignement.

Fusionner des enseignements

Dans le cas où l'on a créé des enseignements dans deux classes alors qu'il s'agit d'un même enseignement regroupant les deux classes, il est possible de fusionner les deux enseignements :

- Aller dans `Gestion des bases` / `Gestion des classes` ;
- Choisir un enseignement dans le tableau puis cliquer sur `Enseignements` ;
- Cliquer sur le nom de l'enseignement, puis cliquer sur le lien `Fusionner le groupe avec un ou des groupes existants`.

Rôles des utilisateurs

Administrateur

Seul l'utilisateur `admin` a un accès à l'application, il est administrateur de celle-ci.

Il a un accès complet à l'application et à sa configuration. Il peut déléguer ce rôle en donnant les droits administrateur à un utilisateur.

Ce rôle permet notamment de :

- gérer les comptes utilisateurs ;
- gérer les groupes classes et autres ;
- sauvegarder les données ;
- bloquer l'accès à l'application ;
- observer l'historique des connexions.

Les autres utilisateurs ont accès à l'application uniquement si leur compte créé lors de l'initialisation annuelle.

Les rôles sont assignés comme suit :

Professeur principal

Les enseignants responsables de classes ont un accès en tant que professeur principal.

Professeur

Les enseignants qui ne sont pas professeur principal ont un accès professeur leur permettant :

- d'accéder au cahier de texte ;
- d'accéder à l'outil de gestion des notes ;
- de saisir les bulletins ;
- de préparer les conseils de classe (impression des bulletins, tableaux, graphiques ...).

Scolarité

Les personnels administratifs ont un accès scolarité, ces comptes doivent être édités manuellement afin de leur attribuer des rôles plus précis.

L'accès scolarité permet :

- une vérification détaillée de la saisie des notes et la saisie des appréciations sur les bulletins ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- de visualiser et d'imprimer des relevés de notes ;
- de visualiser et d'imprimer des bulletins.

Élève

Les élèves ont un accès élève leur permettant de :

- consulter le cahier de texte;
- consulter leurs notes et leurs bulletins.

Responsable légaux

Les responsables légaux ont un accès responsable légal leur permettant de consulter les informations (notes, absences ...) concernant les élèves dont ils sont responsables.



Plus d'informations sur les fonctionnalités disponibles directement ici :
http://www.sylogix.org/wiki/gepi/ListeDesFonctionnalités

Remarques



Tant qu'un élève n'a pas de note dans un groupe, il est facile de le désinscrire.

Si un professeur s'aperçoit qu'un élève ne devrait pas être dans un groupe, il est important qu'il n'ajoute aucune donnée à cet élève.

Mécanisme de synchronisation des élèves / parents / profs disponible

Cela se situe dans posh-profil > Synchronisation > Gepi

Attention contrairement aux autres mécanismes de synchronisation, celui de Gepi ne se lance pas toute les nuits en automatique

Il est nécessaire de l'exécuter en allant dans l'écran de posh-profil et cliquer sur le bouton `Synchroniser`

12.4.17. GRR : gestion de réservation de salles et de matériels

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Administration de GRR

GRR (Gestion et Réservation de Ressources) est un outil de gestion de réservation de salles et de matériels.

http://grr.mutualibre.org

Installation

GRR s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-grr
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .



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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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 `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 : `http://<adresse serveur>/grr/`

L'authentification peut être réalisée par le biais du serveur SSO ou être gérée par l'application.

Rôle des utilisateurs (SSO activé)

Il est possible dans le menu "Configuration SSO" de sélectionner le rôle à donner aux différents profils existants lors de leur première connexion.

Par défaut les rôles sont restreints, l'administrateur doit donc définir finement les rôles avant même le lancement de l'application.

- **Administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur ayant initialisé son compte.

- **Gestionnaire**

  Le gestionnaire à les droits pour gérer telle ou telle ressource.

- **Gestionnaire utilisateur**

  Le gestionnaire d'utilisateur peut ajouter, éditer, supprimer des utilisateurs ayant pour statut "usager" ou "visiteur",

  L'administrateur peut déléguer le droit de gérer les utilisateurs.

- **Usager**

  Les professeurs ont par défaut un accès "usager" à l'application.

  L'usager peut créer, modifier ou effacer ses propres réservations.

- **Visiteur**

  Les administratifs, les élèves, les responsables et les invités ont par défaut un accès "visiteur" à l'application.

  Un « visiteur » peut voir les réservations mais ne peut pas agir dessus.

Remarques

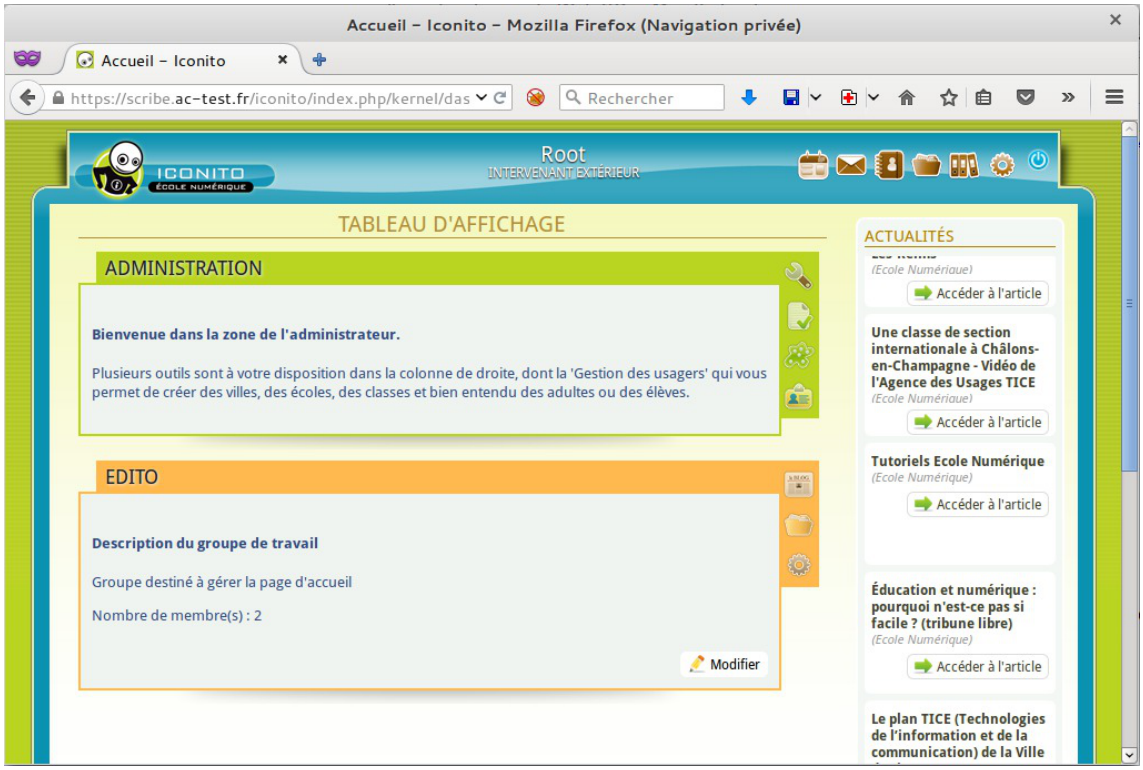
- Si l'authentification est gérée par l'application et non pas le serveur SSO, il faut utiliser le compte "administrateur" avec pour mot de passe `azerty` (par mesure de sécurité le mot de passe doit absolument être changé).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- Lors d'un changement de version, il se peut qu'une mise à jour de la base de données soit nécessaire. Dans ce cas, une page d'avertissement s'affiche avec un lien "Mettre à jour la base MySQL" permettant à l'administrateur d'effectuer cette action.
- Les comptes sont créés dans GRR lors de la première connexion des utilisateurs (initialisation du compte).

12.4.18. ICONITO : Espace Numérique de Travail pour le 1er degré

Présentation



Page d'accueil d'un forum FluxBB

ICONITO est un Espace Numérique de Travail que sa simplicité et son graphisme original destinent sans équivoque aux écoles primaires avant tout.

ICONITO est doté d'outils personnels, d'outils collaboratifs et d'outils d'administration.

http://iconito.fr/

Installation de ICONITO

ICONITO s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
# apt-eole install eole-iconito
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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 `Applications web`.
>
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/iconito/`

Une synchronisation de l'annuaire ICONITO est réalisée automatiquement sur la base de l'annuaire du module Scribe.

A la différence des autres applications ICONITO n'utilise pas le serveur SSO car elle devrait se suffire à elle même dans le cadre du 1er degrés. Elle dispose malgré tout d'un connecteur LDAP.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Remarques

Gestion des usagers → Gestion des années scolaires → Créer une nouvelle année scolaire

12.4.19. Gestion 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).

12.4.19.a. Visualisation des quotas disque dans l'EAD

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

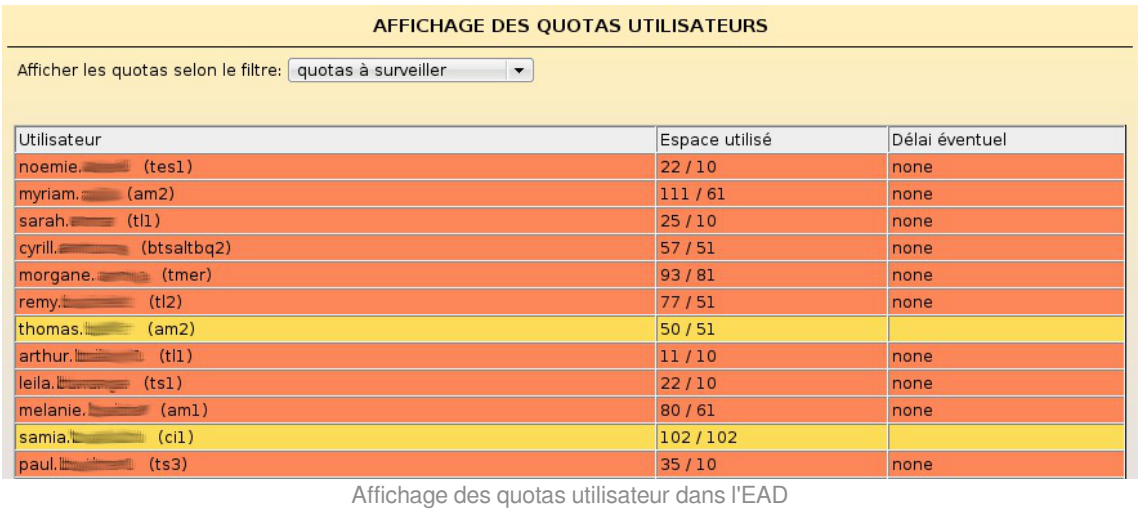
1. arrêter les différents services susceptibles d'écrire sur la partition (samba, proftpd, exim4, ...) ;
2. démonter les éventuels montages liés à cette partition (images ISO, ...) ;
3. désactiver les quotas sur la partition : `quotaoff /home` ;
4. lancer la vérification des quotas : `quotacheck -vug /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.

Les quotas sur le module Scribe

Pour consulter les quotas, le menu `Outils/Quotas disque` de l'EAD permet d'afficher les quotas utilisateurs selon 3 filtres :

- Quotas dépassés
- Quotas à surveiller (quotas presque atteint)
- Tous les quotas



Affichage des quotas utilisateur dans l'EAD

Les quotas sont appliqués sur la partition `/home`. Les quotas concernent, ainsi, l'ensemble des fichiers créés par l'utilisateur sur le serveur (dossiers personnels, partages équipe pédagogique, classe, groupes, etc.).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

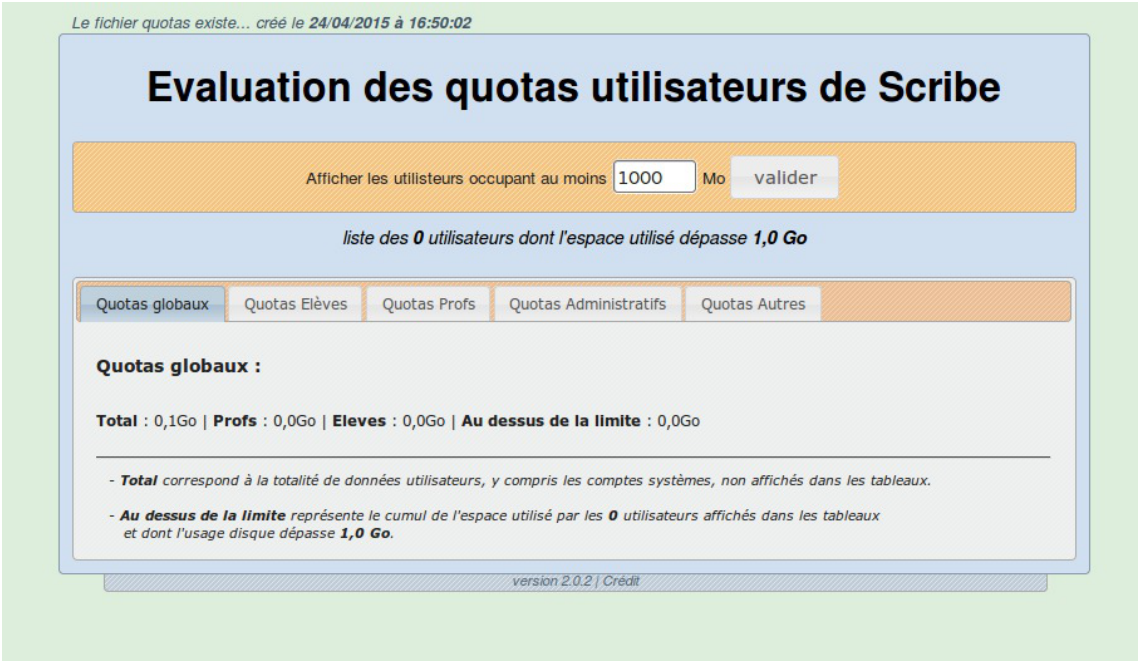
Sur les modules Scribe et Horus, la limite dure vaut le double de la limite douce.

12.4.19.b. Infosquota : gestion des quotas utilisateurs

Présentation

Infosquota est un outil qui permet de mettre en place les quotas de manière très souple et très pédagogique. Chaque utilisateur apprend à gérer son quota en suivant une information claire sur son évolution.

Grâce à son outil de visualisation, Infosquota permet de retrouver les fichiers que les utilisateurs ont ventilé hors de leur lecteur partagé personnel. En effet les fichiers dispersés dans d'autres volumes sont comptabilisés dans le quota de l'utilisateur.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Infosquota a été développé par Olivier Hacquard et Jérôme Labriet (Académie de Besançon) en étroite collaboration avec Bruno Debeve (Académie de Bordeaux), Frédéric Poyet (Académie de Dijon) et Pierre Mariot (Académie de Besançon) dans le cadre du projet EOLE.

http://dev-eole.ac-dijon.fr/projects/infquot

Les derniers développements mis à disposition par Bruno Debeve ont également été intégrés.

http://www.debeve.net/infosquota_dev/

Installation d'Infosquota

Infosquota s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-infosquota
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .



L'application fonctionne uniquement sur le module Scribe.



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
```

L'initialisation de l'application (recherche des fichiers) s'effectue lors de l'instance ou du reconfigure suivant l'installation du paquet.

La mise à jour des fichiers s'effectue de façon hebdomadaire.

Accès à l'application web

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/quotas/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

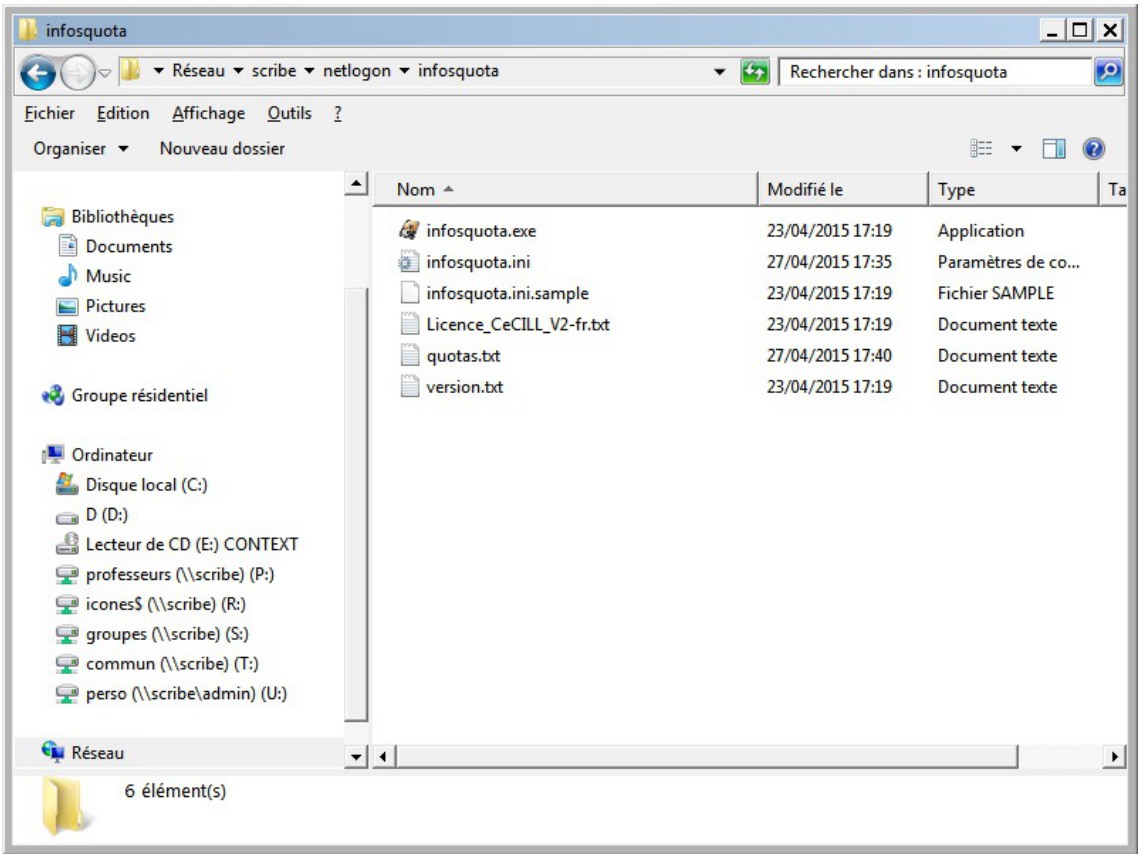
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Rôles des utilisateurs

Seul l'utilisateur `admin` est autorisé à se connecter à l'application.

Utilisation

L'exécutable `infosquotas.exe` est lancé au démarrage de la session et affiche les messages qui conviennent selon la configuration des quotas établie dans l'EAD et celle des alertes saisies dans le fichier `\\scribe\netlogon\infosquota.ini`.



Une documentation d'utilisation est disponible dans l'espace de contributions EOLE à l'adresse suivante : http://eoleng.ac-dijon.fr/documentations/2.4/contributions/

Remarques

L'utilisation du disque par utilisateur est enregistrée dans le fichier : `/home/netlogon/infosquota/quotas.txt`.

Le journal généré par le script de recherche des fichiers est disponible dans : `/var/log/infosquota/recherche-fich-users.log`.

La liste des fichiers ventilés d'un utilisateur est stockées dans le fichier : `/var/www/html/outils/quotas/log/<login>.log`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.4.19.c. Envoi de courrier électronique en cas de dépassement des quotas

Dans l'onglet Samba de l'interface de configuration du module en mode expert, il est possible d'activer l'envoi d'un courrier électronique à un utilisateur dans le cas où celui-ci dépasse le quota disque.

Il faut bien sûr que l'utilisateur ait une adresse de courrier électronique valide définie dans l'annuaire.

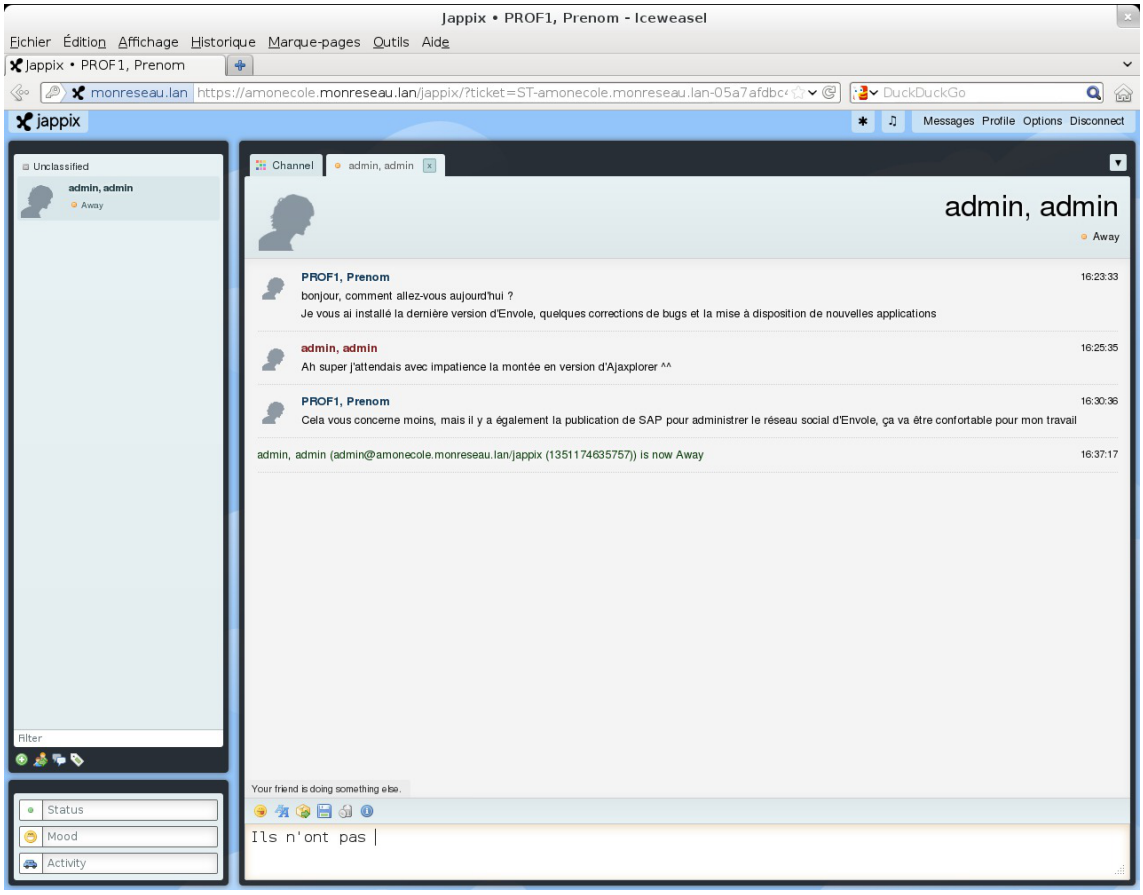
> Les fichiers déplacés dans la corbeille sont inclus dans le calcul de l'espace disque occupé par l'utilisateur. Pour limiter les dépassements de quota disque, il est conseillé de paramétrer une durée de conservation assez courte.

Voir aussi...

Onglet Samba : Configuration du contrôleur de domaine

12.4.20. Jappix : client web Jabber

Présentation



Fenêtre de discussion de Jappix

Jappix est un client web de communication instantanée. Il est libre et basé sur le protocole XMPP[p.906].

Il permet une communication en temps réel entre les personnes possédant un compte XMPP.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette communication se fait simplement en utilisant un navigateur web moderne.

Un canal est à disposition pour laisser des messages de statut.

http://jappix.com

Installation

Jappix s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-jappix
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Si le serveur Jabber n'est pas installé un conteneur supplémentaire doit être créé, il faut donc exécuter la commande `gen conteneurs` comme le propose la commande reconfigure.

Cette commande doit être suivie de la ré-instanciation du module avec la commande instance :

```
# instance /etc/eole/config.eol
```



L'application nécessite que le service `ejabberd` soit activé.

Dans l'interface de configuration du module, onglet `Services`, mettre `Activer le serveur de messagerie instantanée ejabberd` à `oui`.

L'application est très sensible à la configuration réseau mise en œuvre et son fonctionnement requiert notamment des noms DNS.

La configuration recommandée est donc la suivante :

domain_jabber_etab = eolesso_adresse = web_url = ssl_subjectaltname_ns = "nom_de_domaine"

Si cette configuration n'est pas respectée, l'erreur suivante s'affichera :

```
Erreur » Service indisponible
```

Attention la modification de certains de ces paramètres nécessite de régénérer les certificats.



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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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`.

Accéder à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/jappix/`

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Remarques

Par défaut il n'est pas possible de téléverser des fichiers dans le canal car il n'y a pas de gestion des quotas et la partition du conteneur pourrait se remplir très vite :

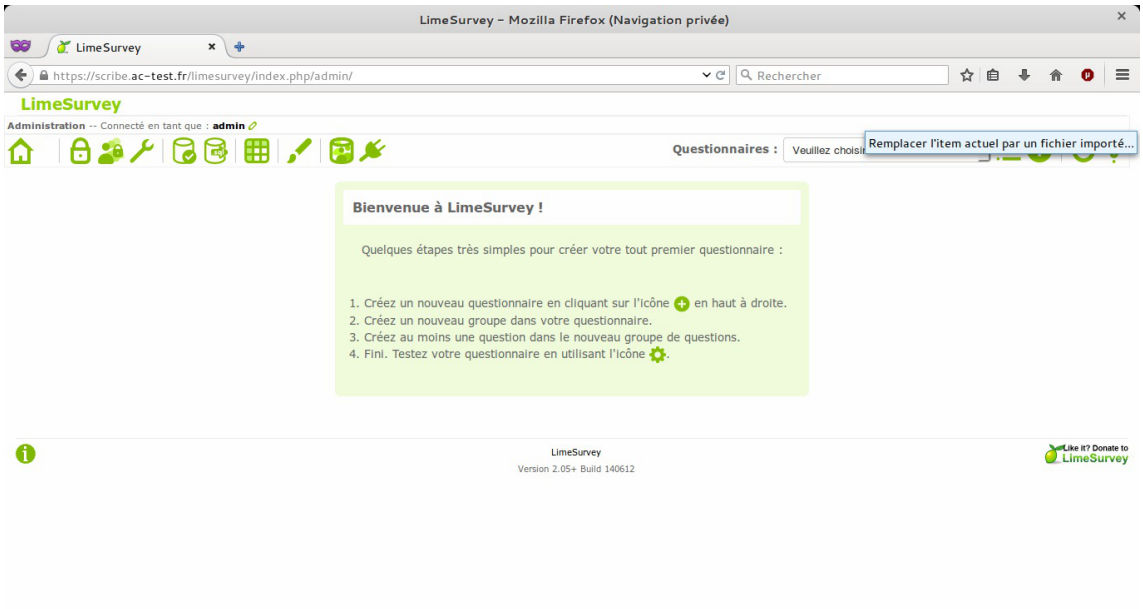
En attendant, il est tout de même possible d'activer cette fonctionnalité en créant un répertoire accessible en écriture à Apache :

```
# ssh reseau
# mkdir /usr/share/jappix/store/share
# chown www-data:root /usr/share/jappix/store/share
```

`ctrl + d` pour sortir de la connexion SSH.

12.4.21. LimeSurvey : sondage et enquête statistique

Présentation



LimeSurvey est un logiciel d'enquête statistique, de sondage, et autres types de formulaires en ligne. Il permet aux utilisateurs, enquêteurs et statisticiens, de publier des questionnaires pour en collecter les réponses.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

http://www.limesurvey.org [http://etherpad.org/]

Installation de LimeSurvey

LimeSurvey s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-limesurvey
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/limesurvey/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

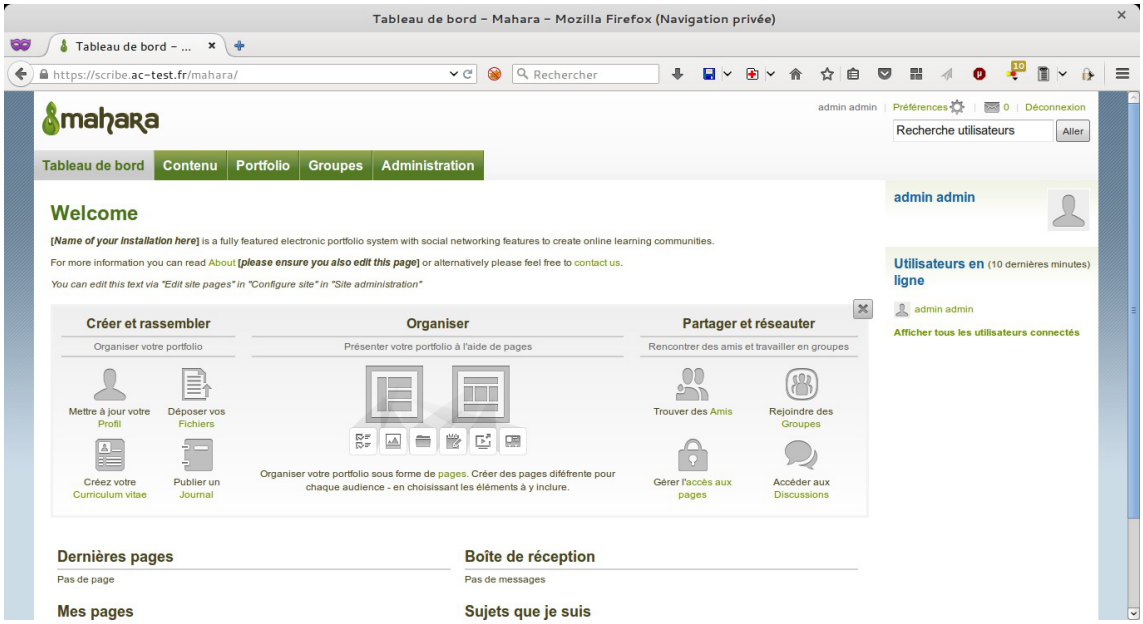
Remarques

Pour administrer l'application il faut se rendre à l'adresse : `http://<adresse_serveur>/limesurvey/index.php/admin/`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.4.22. Mahara : portfolio électronique

Présentation



Page d'accueil d'un forum FluxBB

Mahara est le trait d'union entre espace personnel et profil dans un réseau social, blogs, homepage, site professionnel, espace collaboratif virtuel...

Mahara est un système de gestion d'ePortfolios, mais aussi d'un système de réseau social, combinés.

Un système de gestion d'ePortfolios est un système qui permet aux étudiants de collecter et ordonnancer leurs preuves « d'apprentissage tout au long de la vie » — comme des essais littéraires, des travaux artistiques ou tous autres documents qu'ils produisent dans le monde numérique. Ces documents sont appelés artefacts ou productions dans Mahara.

En ce qui concerne les réseaux sociaux, ils sont déjà rentrés dans les mœurs et ne nécessitent pas beaucoup d'explication. En résumé, ils permettent à des personnes d'interagir avec des amis et de créer ses propres communautés dans un monde virtuel, en ligne.

Mahara est bien plus qu'un simple dépôt où stocker des documents, il comprend aussi des outils de blog, un système de création de curriculum vitae, ainsi qu'un système de collaboration avec Moodle.

http://mahara.org/

Installation de Mahara

Mahara s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-mahara
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/mahara/`

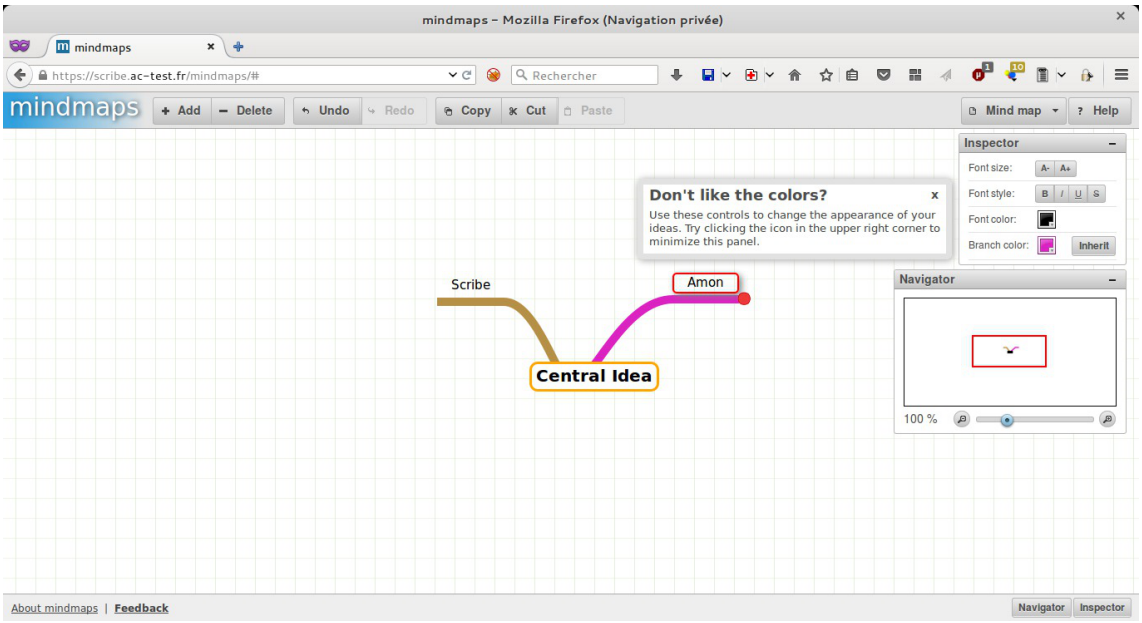
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

12.4.23. mindmaps : conception de cartes cognitives

Présentation



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

mindmaps est un logiciel servant à dresser des cartes heuristiques. Une carte heuristique (carte cognitive, carte mentale), est un schéma, supposé refléter le fonctionnement de la pensée, qui permet de représenter visuellement et de suivre le cheminement associatif de la pensée.

Cela permet de mettre en lumière les liens qui existent entre un concept ou une idée, et les informations qui leur sont associées.

La structure même d'une carte heuristique est en fait un diagramme qui représente l'organisation des liens sémantiques entre différentes idées ou des liens hiérarchiques entre différents concepts.

http://github.com/drichard/mindmaps

Installation de mindmaps

mindmaps s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-mindmaps
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/mindmaps /`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

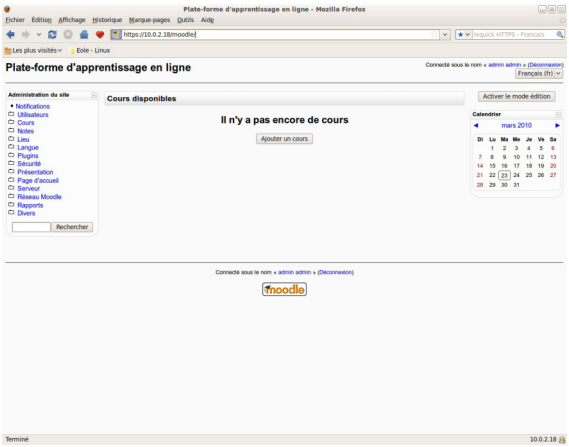
Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.4.24. Moodle : plate-forme d'apprentissage en ligne

Présentation



Page d'accueil de Moodle

Moodle est une plate-forme d'apprentissage en ligne (e-learning en anglais) servant à créer des communautés d'apprenants autour de contenus et d'activités pédagogiques

À un système de gestion de contenu, Moodle ajoute des fonctions pédagogiques ou communicatives pour créer un environnement d'apprentissage en ligne.

C'est une application permettant de créer, par l'intermédiaire du réseau, des interactions entre des pédagogues, des apprenants et des ressources pédagogiques.

http://moodle.org/

Installation

Moodle s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-moodle-update
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



Il existe un paquet moodle qu'il ne faut pas confondre avec le paquet **eole-moodle**.



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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 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 : `http://<adresse serveur>/moodle/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tout utilisateur présent dans l'annuaire possède un accès à l'application.

Administrateur

Seul l'utilisateur `admin` est "administrateur" de l'application.

Il a un accès complet à l'application et à sa configuration.

Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur ayant initialisé son compte :

Utilisateurs / Attribution des rôles système / choisir un rôle -> ajouter un utilisateur pour le rôle choisi.

Par défaut les rôles sont très restreints, l'administrateur doit donc définir finement les rôles avant même le lancement de l'application :

Utilisateurs / Permissions / Définition des rôles -> choisir le rôle à modifier

Créateur de cours

Les enseignants sont "créateur de cours", ils peuvent créer des cours et y convier des élèves (ainsi que d'autres utilisateurs), il peut être intéressant de leur mettre un rôle enseignant (voir plus bas).

Utilisateur authentifié

Les élèves, les administratifs et les invités sont par défaut "utilisateur authentifié", par défaut ils peuvent voir les cours disponibles et s'y inscrire.

Remarques

- Seul l'enseignant a le choix de son adresse de messagerie lors de sa première connexion.
- Il existe des problèmes d'encodage pour certaines pages de l'application essentiellement dans la partie administration.

Attention !

- Les données ajoutées à Moodle sont stockées dans /var/www/moodledata/ donc attention à l'espace dont vous disposez sur la partition.
- Les règles d'authentification sont directement modifiables dans Moodle par l'administrateur.

  L'authentification : Utilisateurs / Authentification

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> Une modification pourrait rendre inutilisable l'authentification par le biais du serveur SSO.

Premiers pas

Pour synchroniser les comptes de l'annuaire ldap de Scribe directement dans moodle.

L'opération nécessite le lancement de la commande suivante :

```
/usr/bin/php -c /etc/php5/cli/php.ini /var/www/html/moodle/auth/cas/cas_ldap_sync_users.php
```



Nous allons décrire comment créer la classe de seconde 1 ainsi que le cours de mathématiques de cette classe.

- Dans l'interface d'administration de l'application, aller dans `Cours` / `Gestion des cours` ;
- Créer un cours "seconde_1" au format `Informel` (ce cours correspondra à votre classe) ;
- Créer un cours "seconde_1_math" mettre `S'agit-il d'un méta-cours ?` à `Oui` (ce cours correspondra au cours de mathématiques) ;
- Choisir les options, valider, une page `Cours descendants` apparaît ;
- Mettre le cours seconde_1 comme cours descendants, valider.

La classe et le cours sont alors créés.

Inscription des utilisateurs



Inscrivons à présent les élèves dans leur classe.

- Depuis la liste des cours disponibles, aller dans le `cours seconde_1` ;
- Dans `Attribution des rôles`, cliquer sur `Etudiant` ;
- Ajouter les élèves de la classe ;
- Cliquer sur `Attribuer les rôles dans Cours : seconde_1`.

Inscrivons l'enseignant de mathématique à son cours :

- Depuis la liste des cours disponibles, aller dans le cours `seconde_1_math` ;
- Dans `Attribution des rôles`, cliquer sur `Enseignant` ;
- Ajouter l'enseignant ;
- Cliquer sur `Attribuer les rôles dans Cours : seconde_1_math`.

Améliorer les accès

Un créateur de cours voit l'ensemble des cours ce qui rend la vue complexe.

Les enseignants sont créés par défaut avec ce rôle.

A l'usage, il peut être plus judicieux d'attribuer le rôle Enseignant.

Pour ce faire, dans l'interface d'administration :

- Aller dans `Utilisateurs` / `Permissions` / `Attribution des rôles système` et cliquer sur `Enseignant` ;
- Choisir les comptes `Créateur de cours` et cliquer sur `Attribuer les rôles Système`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

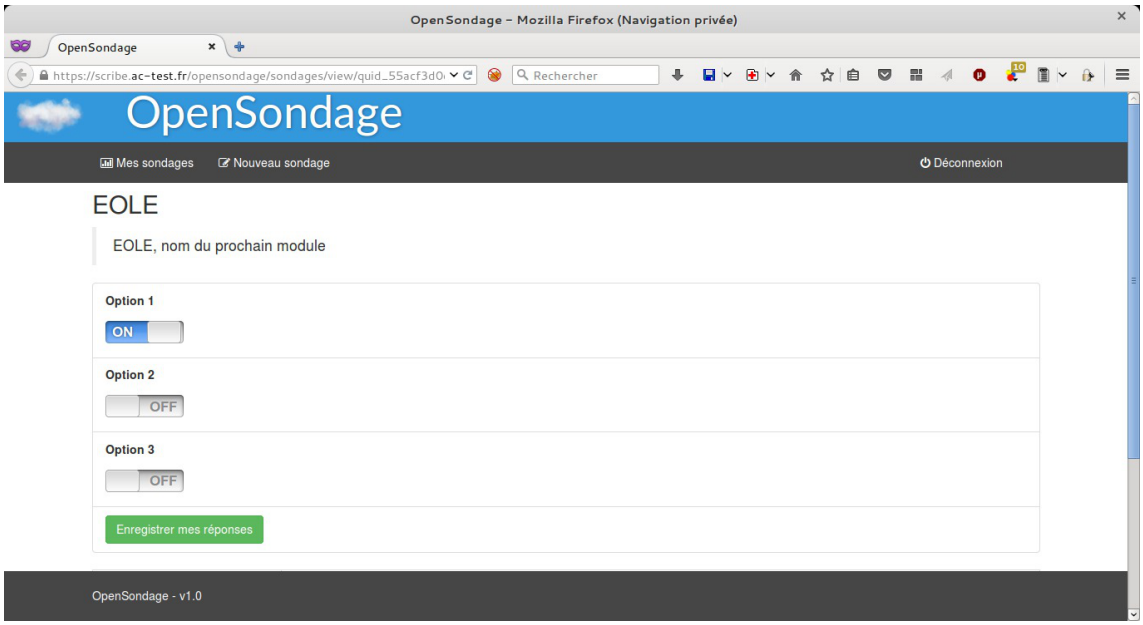
L'affichage par défaut d'un cours peut paraître surchargé, il est possible de supprimer des blocs d'affichage.

Pour ce faire, dans l'interface d'administration :

- Aller dans `Plugins` / `Blocs` / `Gestion des blocs` ;
- Désactiver les blocs inutiles.

12.4.25. OpenSondage : planification de rendez-vous et mini-sondage

Présentation



OpenSondage sert à faire des sondages pour déterminer à plusieurs une date de réunion qui convienne au plus grand nombre.

Vous pouvez également utiliser cette application pour proposer des choix multiples et ainsi se mettre d'accord sur un lieu de rendez-vous, un thème de réunion ou la marque de votre prochaine machine à café (à base de capsules libres bien entendu).

OpenSondage est basé sur STUdS.

http://studs.u-strasbg.fr

Installation de OpenSondage

OpenSondage s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-opensondage
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .



Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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 `Applications web`.
>
> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/opensondage/`

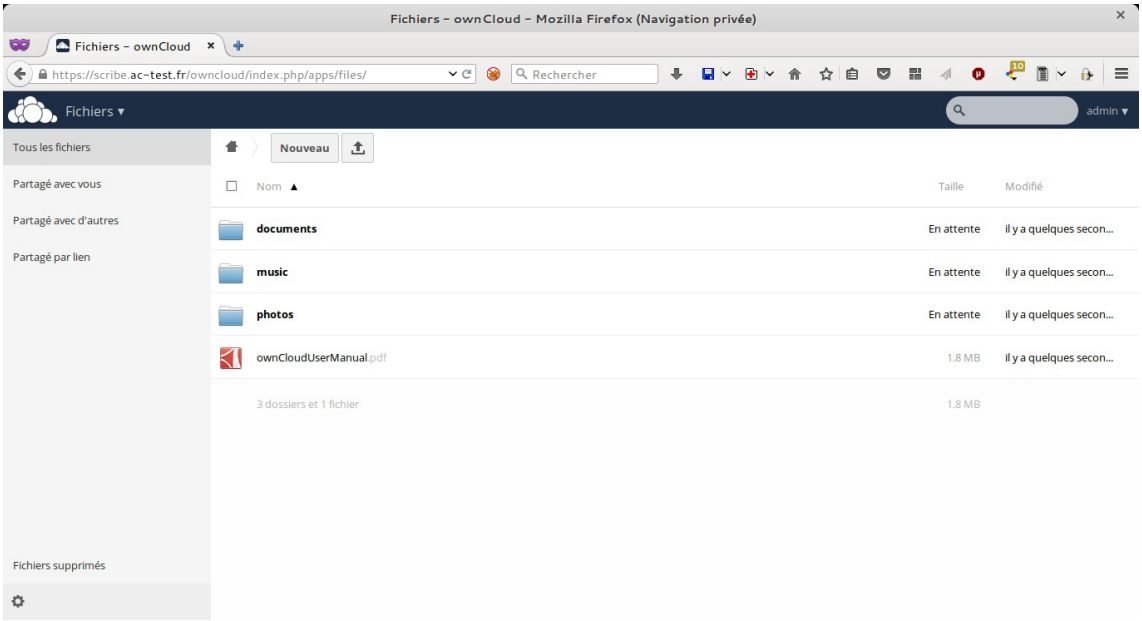
L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

12.4.26. ownCloud : stockage et partage de fichiers

Présentation



ownCloud est un logiciel libre offrant une plateforme de services de stockage et partage de fichiers et

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

d'applications diverses en ligne. Dans ownCloud, le stockage des données se fait au sein de l'infrastructure de l'entreprise et les accès sont soumis à la politique de sécurité informatique de celle-ci.

http://owncloud.org/

Installation de ownCloud

ownCloud s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
```

```
# apt-eole install eole-owncloud
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/owncloud/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

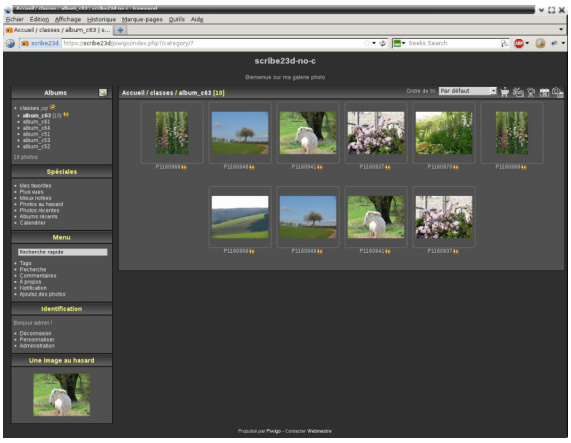
Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

12.4.27. Piwigo : gestionnaire de galerie photo

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Navigation dans une galerie de Piwigo

Piwigo est une application de gestion de galerie photo en ligne.

http://fr.piwigo.org/

Installation de Piwigo

Piwigo s'installe manuellement, en saisissant les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-piwigo
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application, se rendre à l'adresse : `http://<adresse serveur>/piwigo/`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Par défaut les rôles des utilisateurs sont assignés comme suit :

- **Administrateur**

  Seul l'utilisateur `admin` est "webmaster" de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.
- **Enseignant**

  Les enseignants peuvent téléverser des nouvelles images dans les galeries de leurs classes d'appartenance.
- **Élèves**

  Ils peuvent consulter la galerie de leur classe d'appartenance.
- **Autres**

  Par défaut, les autres utilisateurs peuvent se connecter à l'application mais n'ont pas accès à la consultation des galeries.

Remarques

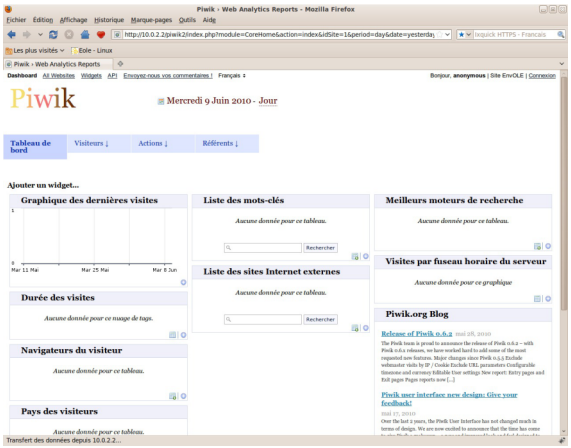
Les comptes sont créés dans Piwigo lors de la première connexion à l'application (initialisation du compte).

L'application est configurée pour que chaque classe ait sa propre galerie photo.

Les galeries portant le nom d'une classe ne se créent qu'à l'initialisation d'un compte enseignant ou élève de cette classe.

12.4.28. Piwik : outil statistique

Présentation



La page d'accueil de Piwik

Piwik est une application web de statistiques collectant des données dans une base MySQL dédiée.

Son interface très esthétique et totalement personnalisable via des modules que l'on choisit d'afficher ou

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

non.

http://piwik.org/

Piwik est configuré pour dresser des statistiques sur l'utilisation du portail Envole.

Installation

Piwik s'installe manuellement, en saisissant les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-piwik
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/piwik/`

Nul besoin d'être authentifié pour accéder à l'application.

Rôles des utilisateurs

- **Administateur**

  L'utilisateur `admin` peut suivre la procédure de récupération de mot de passe depuis Piwik en indiquant son adresse de courrier électronique.

  Il pourra notamment ajouter des applications à surveiller qui ne sont pas accessibles depuis Envole.

  Il peut aussi obtenir le code pour créer des widgets à ajouter dans Envole.

- **Anonymous**

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Tous les utilisateurs ont ce rôle.

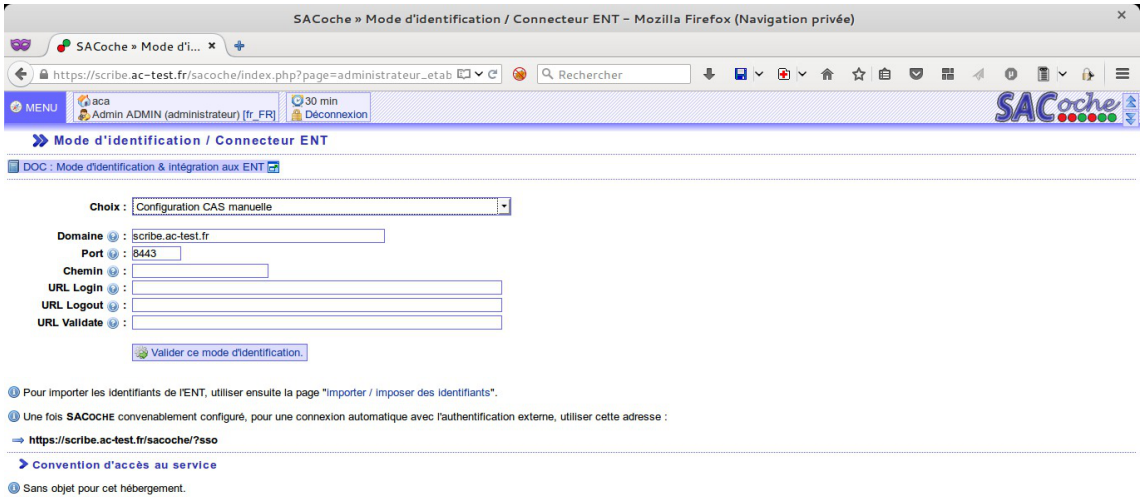
Ils ont un rôle uniquement consultatif.

Remarques

Seul les clics sur l'onglet `Mon bureau` sont référencés dans les statistiques.

12.4.29. SACoche : évaluation et suivi d'acquisitions de compétences

Présentation



L'application SACoche permet :

- d'évaluer les élèves par compétences ;
- de conserver un historique de leur parcours ;
- de déterminer un état d'acquisition de chaque compétence :
- de collecter les compétences pour assister la validation du socle commun.

http://sacoche.sesamath.net/

Installation de SACoche

SACoche s'installe manuellement, saisir les commandes suivantes dans un terminal :

```
# Query-Auto
# apt-eole install eole-sacoche
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .

Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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 Applications web.
>
> L'opération nécessite une reconfiguration du module avec la commande reconfigure.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/sacoche/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur le module Scribe possèdent un accès à l'application.

Remarques

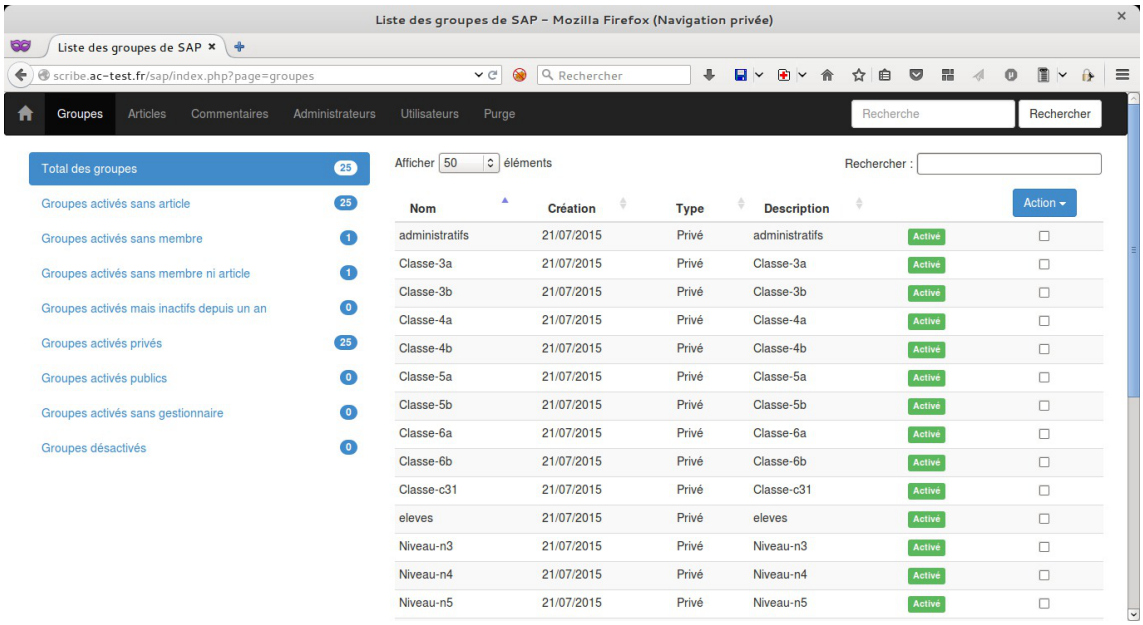
Les utilisateurs sont auto-générés lors de leur première connexion.

Par contre il n'existe pas encore de synchronisation des classes, des matières et des niveaux.

12.4.30. SAP : administration du réseau social d'Envole

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de l'application SAP

SAP pour Social Admin POSH est une application permettant l'administration du réseau social d'Envole.

http://dev-eole.ac-dijon.fr/projects/sap [http://dev-eole.ac-dijon.fr/projects/sap]

Installation de SAP

SAP s'installe manuellement, en saisissant les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-sap
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Accès à l'application

Pour accéder à l'application, se rendre à l'adresse : `http://<adresse serveur>/sap/`

L'authentification se fait **obligatoirement** par le biais du service SSO, ce service doit donc être actif.

Rôles des utilisateurs

Seul l'utilisateur `admin` a un accès à l'application.

Il a un accès complet à l'application et à sa configuration.

Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.

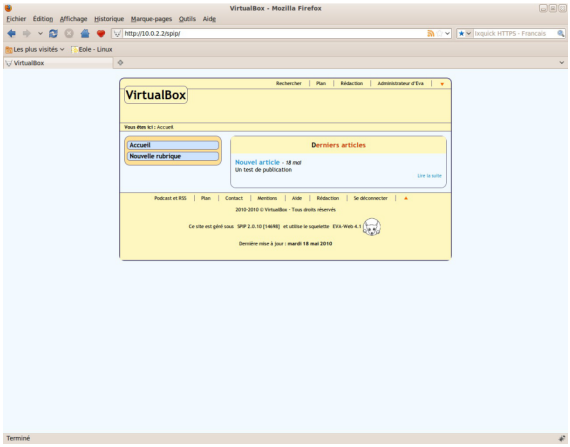
Remarques

Pour une meilleur intégration dans Envole l'application SAP n'est pas pourvu de bouton de déconnexion.

Il est donc fortement recommandé d'ajouter l'application sous forme d'onglet dans Envole via le gestionnaire de profil.

12.4.31. SPIP Eva : gestion de contenu

Présentation



SPIP est un logiciel libre de gestion de contenu.

http://www.spip.net

Il se démarque d'un système de gestion de contenu classique par le soin apporté aux standards de l'édition (respect des règles typographiques, organisation des rôles des participants).

Il est personnalisé à l'aide d'un squelette Eva.

http://www.eva-web.edres74.ac-grenoble.fr

Installation

SPIP-Eva s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-spipeva
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.



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 `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 : `http://<adresse serveur>/spip/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Pour pouvoir rédiger un article il faut cliquer sur le lien `Rédaction`

Il est également possible de s'y rendre directement avec l'adresse : `http://<adresse serveur>/spip/ecrire/`

Rôles des utilisateurs

Chacun des utilisateurs présents dans l'annuaire du module possède un accès à l'application.

- **administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application, il peut :

  - gérer les utilisateurs ;
  - configurer le site ;
  - gérer et configurer les greffons installés ;
  - créer des rubriques ;
  - rédiger et publier des articles ;
  - déléguer son rôle à une autre personne.

- **rédacteur**

  Les professeurs, les élèves et les parents sont rédacteurs, ils peuvent :

  - rédiger des articles ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- proposer un article à l'évaluation.

Remarques

Pour écrire un article il faut commencer par `créer une rubrique`,

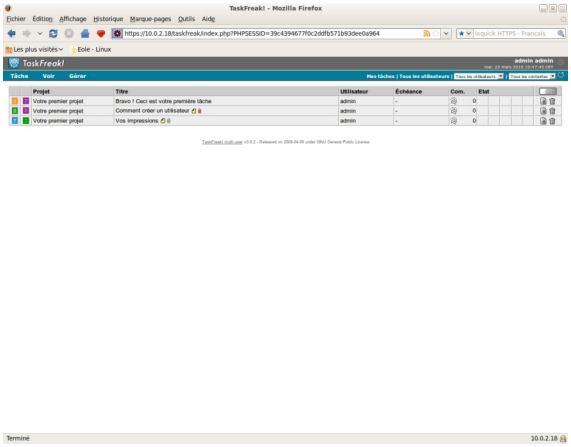
puis colonne de gauche `écrire un nouvel article`.

Pour être être visible l'article doit être `publié en ligne` (voir la colonne de gauche dans l'interface d'administration de l'application)

SPIP ne gère pas les ACL et n'a pas de module pour le faire.

12.4.32. Taskfreak : gestionnaire de projet

Présentation



Page d'accueil de Taskfreak

Taskfreak est un gestionnaire de projet qui permet de suivre l'avancée d'un projet réalisé en équipe. Il permet de créer des tâches au sein d'une interface simple et ergonomique. Selon le niveau de permission de l'utilisateur, celui-ci peut créer de nouvelles tâches, de nouveaux projets, de nouveaux utilisateurs. Il permettra une gestion de projet simple ou servira de pense-bête.

Chaque utilisateur peut créer des tâches privées visibles de lui seul et peut agir sur les tâches qu'il a créées comme bon lui semble. Chaque tâche peut appartenir à un projet et l'état d'avancement est très facilement modifiable. L'administrateur et le chef de projet peuvent modifier la liste des utilisateurs s'occupant d'un projet. L'application est compatible avec le système d'identification de l'ENT.

http://www.taskfreak.com

Installation

Taskfreak s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-taskfreak
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 `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 : `http://<adresse_serveur>/taskfreak/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Par défaut les rôles des utilisateurs sont assignés comme suit :

- **Administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.
- **Chef de projet**

  Les enseignants sont "chef de projet", ils peuvent créer des nouveaux projets et des nouvelles tâches.

  Il peuvent également ajouter des utilisateurs existants à un projet et/ou à une tâche.
- **Participant**

  Les élèves sont "participant", ils peuvent créer des nouvelles tâches, les assigner et les faire avancer.
- **Invité**

  Aucun utilisateur n'est lié à ce rôle.
- **Visiteur anonyme**

  Ne peut pas accéder à l'application.

Il n'est pas possible de modifier les rôles dans l'application.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

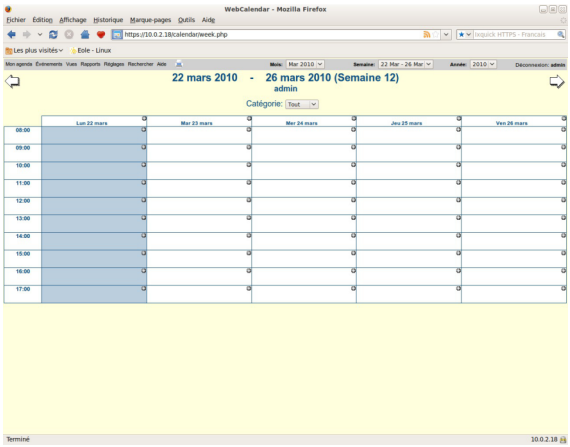
Remarques

Les comptes sont créés dans Taskfreak lors de la première connexion à l'application (initialisation du compte).

Les enseignants ne peuvent donc pas assigner à un projet des élèves n'ayant pas initialisé leur compte.

12.4.33. Webcalendar : agendas partagés

Présentation



Page d'accueil de Webcalendar

Webcalendar est une application d'agendas partagés.

http://www.k5n.us/webcalendar.php [http://www.k5n.us/webcalendar.php]

Installation

Webcalendar s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-webcalendar
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure` .

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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> `# 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.

Accéder à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/calendar/` ou `http://<adresse serveur>/webcalendar/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Tout utilisateur présent dans l'annuaire, excepté les responsables, a accès à l'application.

- **Administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.

- **Enseignant/Administratif**

  Il a un accès aux agendas de tous les autres utilisateurs.

- **Elève**

  Un élève accède aux agendas des classes et à ceux des autres élèves.

- **Assistant**

  Tout utilisateur peut définir un (des) assistant(s) pour déléguer la gestion de son agenda.

  Dans ce cas, tout évènement créé par un assistant dans l'agenda d'un utilisateur est créé dans le sien et soumis à validation dans l'autre.

Remarques

- Lors d'un changement de version, les mises à jour de la base de données sont automatisées et aucune intervention de l'administrateur n'est nécessaire.
- Lorsque **Cdt** est activé en même temps que **Webcalendar**, les informations rentrées dans le cahier de texte (emploi du temps importé depuis SIECLE, devoirs,...) sont automatiquement visibles sur l'agenda d'un enseignant ou d'un élève.

  Cette fonctionnalité est activée par défaut.

- Il est possible d'autoriser les élèves à accéder aux agendas des enseignants :

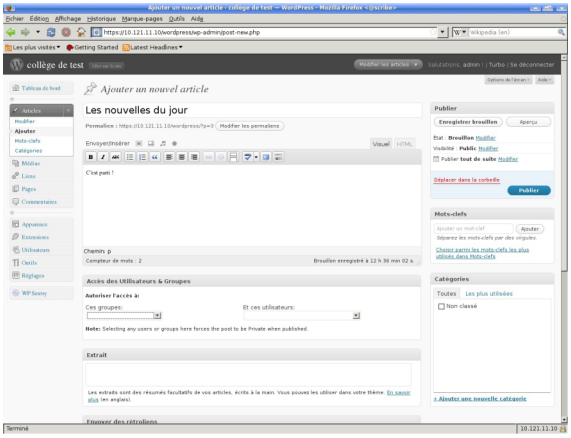
  Réglages -> Réglages du système -> onglet réglages -> chapitre Restrictions.

  Cette option est inactive dès que le Contrôle d'accès Utilisateur est activé et nécessite une configuration manuelle des droits pour chaque utilisateur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.4.34. WordPress : système de gestion de contenu

Présentation



Edition d'un article dans Wordpress

WordPress est un système de gestion de contenu (CMS).

Il permet de créer et gérer du contenu sous forme d'un site web ou plus simplement d'un blog.

http://fr.wordpress.org/

Installation

WordPress s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-wordpress
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande `reconfigure`.

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 `Applications web`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accès à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse serveur>/wordpress/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

L'accès à l'interface d'administration de l'application se fait par l'URL `http://<adresse serveur>/wordpress/wp-admin`

Rôles des utilisateurs

Un utilisateur de WordPress peut avoir l'un des rôle suivant :

- **administrateur**

  Seul l'utilisateur `admin` est "administrateur" de l'application.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur ayant initialisé son compte.
- **éditeur**

  L'éditeur peut gérer les catégories, les liens et les commentaires.
- **auteur**

  L'auteur peut écrire des articles et les publier. Il peut également publier les articles proposés par les contributeurs.
- **contributeur**

  Le contributeur peut écrire des articles.
- **abonné**

  L'abonné peut lire les articles.

Par défaut, les utilisateurs ont le rôle d'abonné.

L'administrateur peut modifier ce comportement et modifier le rôle de chaque utilisateur.

Contrôle de l'accès aux articles

L'extension `WP Sentry` permet à l'administrateur de gérer les droits d'accès aux articles en fonction des profils du module Scribe.



> La gestion des droits d'accès est totalement indépendante de celle des profils.

L'extension Private WP est pré-installée. Elle permet, après activation, de rendre WordPress complétement inaccessible par les visiteurs non authentifiés.

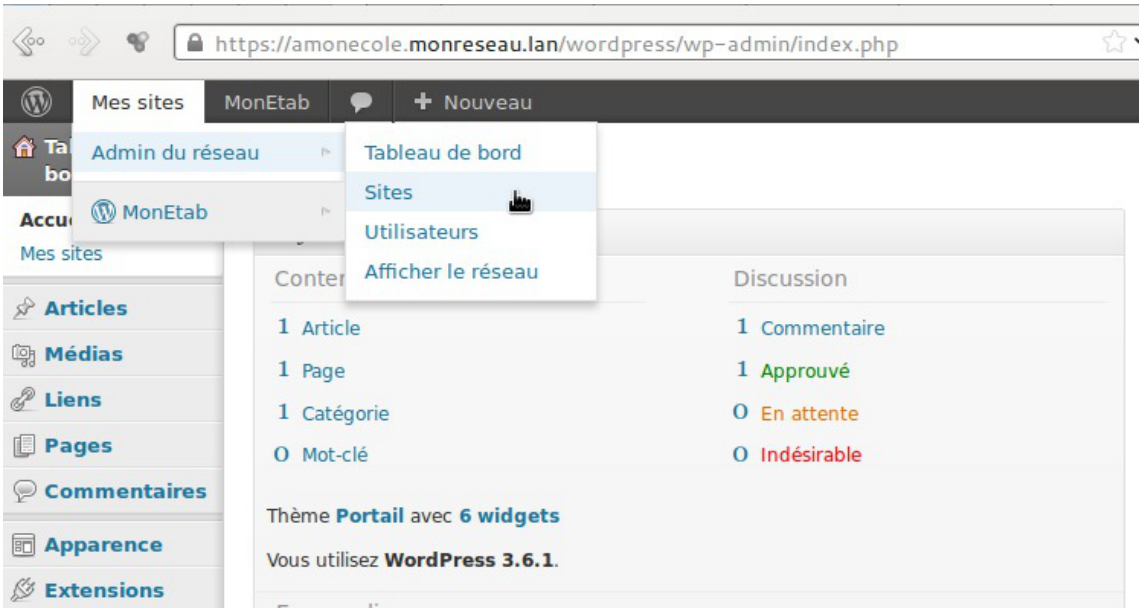
Multisite

Pour gérer plusieurs blogs sur la même instance de WordPress il faut se rendre dans la page dédiée nommée `Sites` en tant qu'utilisateur `admin`.

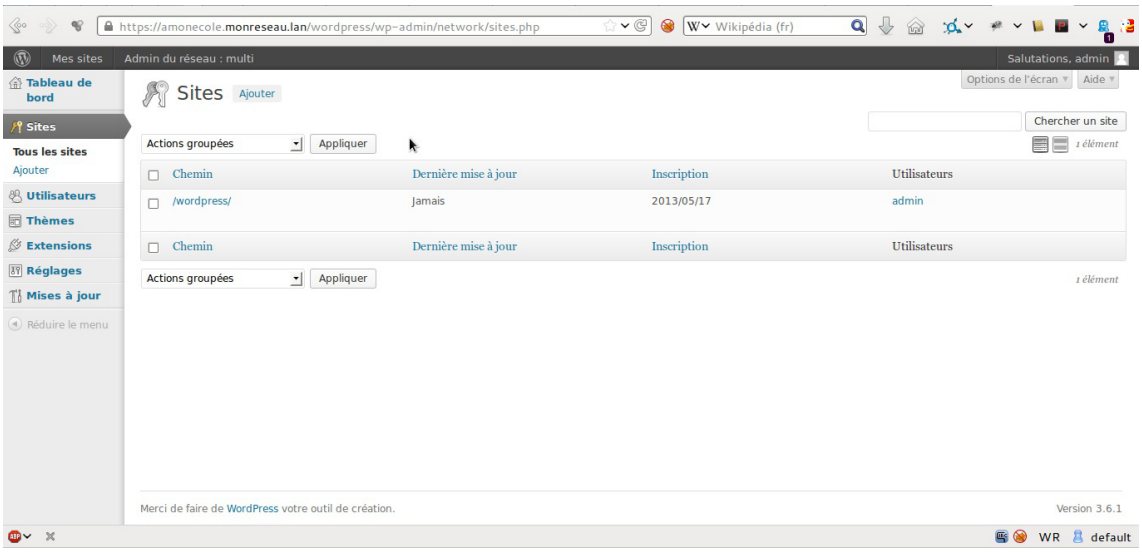
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour cela il faut suivre le menu `Mes sites` → `Admin du réseau` → `Sites`.

Sous l'entrée `Admin du réseau` du menu se trouve le nom de l'instance principale de WordPress. Il porte le nom de l'établissement saisi dans l'interface de configuration du module.

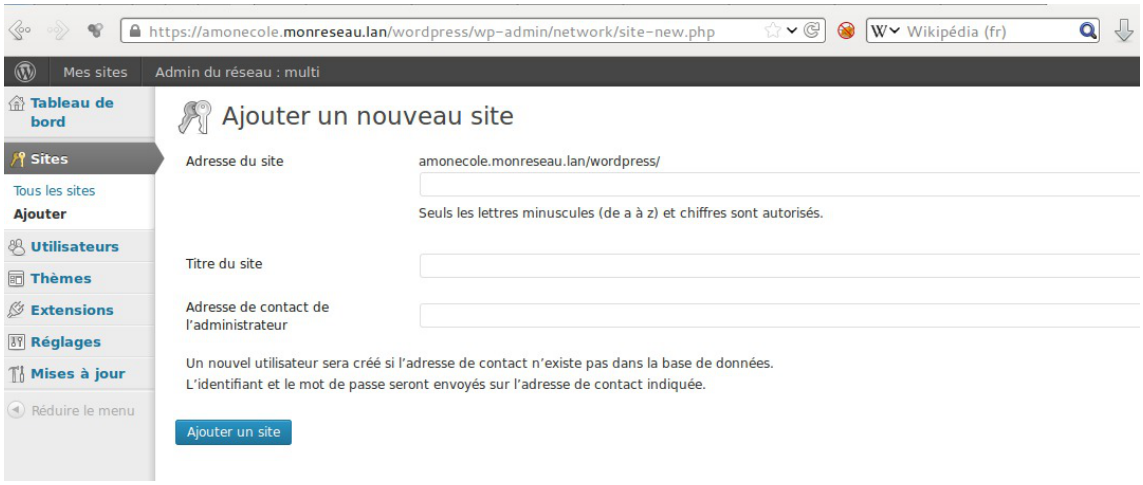


La page `Sites` permet d'ajouter, de modifier et de supprimer un blog.



Pour ajouter un blog il suffit de cliquer sur le bouton `Ajouter` et de saisir les paramètres demandés : le chemin, le titre et l'adresse de contact de l'administrateur de ce nouveau blog. Le chemin sera ajouté au domaine affiché.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



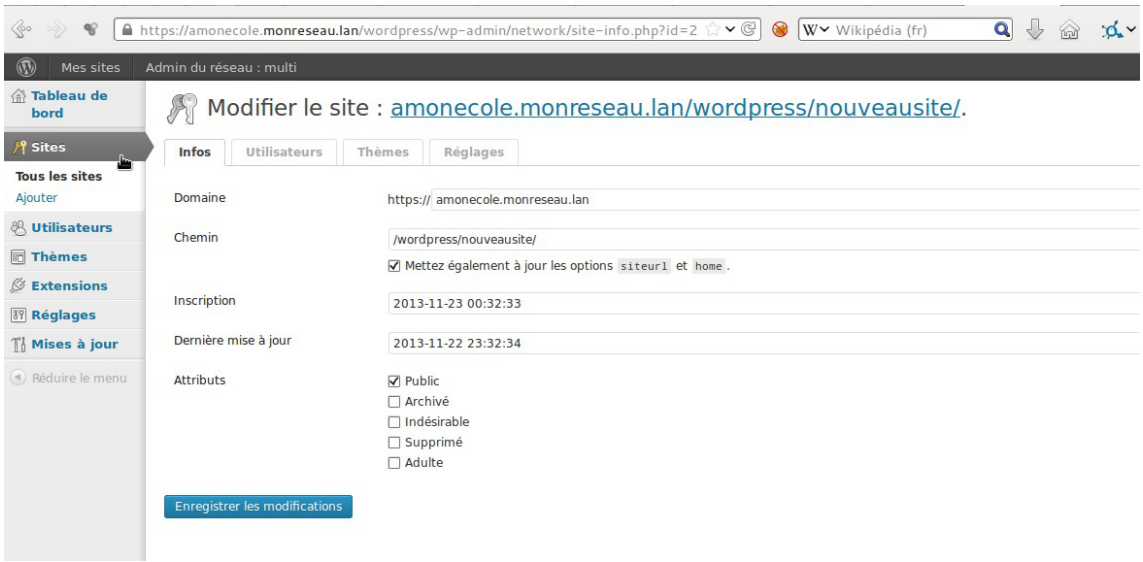
Exemple de valeurs :

Le chemin : `nouveausite`

Titre du site : `Nouveau Site`

Le nouveau blog sera accessible à l'adresse `https://<adresse serveur>/wordpress/nouveausite`

La personnalisation du blog s'effectue dans la liste des sites en cliquant sur le lien modifier.



Il est possible de choisir un thème et une langue spécifique pour le blog.

Il faut pour chaque nouvelle instance passer le site en français

La synchroniser des utilisateurs se fait via la gestion des profils sinon il faut ajouter manuellement les utilisateurs au blog.

Remarques

- Si l'utilisateur est déjà authentifié auprès du serveur SSO son authentification auprès de WordPress est automatique sinon il accède à la partie publique de l'application ;
- Les comptes sont créés dans WordPress lors de la première connexion des utilisateurs (initialisation) ;

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

12.5. 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.

12.5.1. 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
```

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)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 :

  `# apt-eole install-conteneur web php5-imap`

Voir aussi...

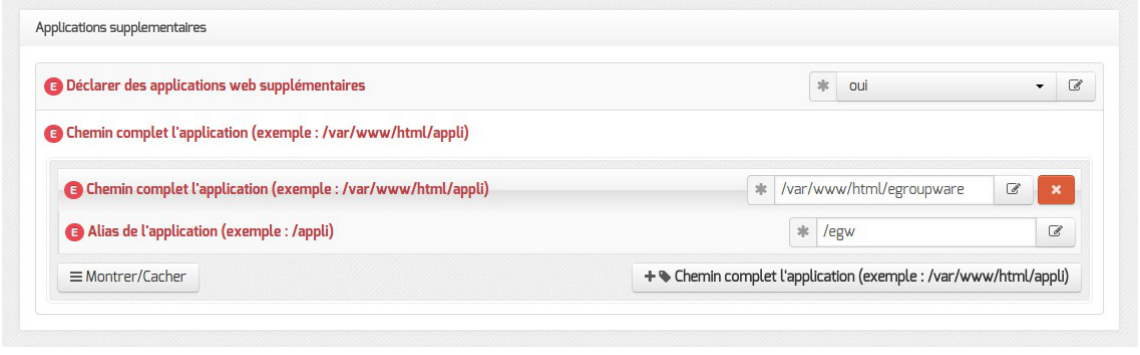
Installation manuelle de paquets

12.5.2. 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` ;



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 #
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.886] :
  `# 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

fonctionnement d'EGroupware.

12.5.3. 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

- 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`.

12.5.4. 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

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.882] 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

13. Gestion des tunnels : RVP

Pré-requis

Le réseau virtuel privé (RVP)[p.899] est activé au moment de la configuration et de l'instanciation du module.

Sur le module Amon, il faut au préalable avoir activé et configuré le réseau virtuel privé dans l'interface de configuration du module. Sur le module Sphynx, ce paramètre est forcé et n'apparaît pas.

Le mode de configuration de strongSwan (database ou fichier plat) doit être le même que sur le serveur ARV qui a généré la configuration IPsec.

ARV[p.883] permet de gérer les RVP de plusieurs serveurs Sphynx. Un serveur Sphynx autre que le serveur Sphynx-ARV sera appelé Sphynx distant. Sur un serveur de ce type, la mise en place du RVP se fera comme sur un serveur Amon.

Activation du RVP au moment de l'installation du serveur Amon

La configuration du Réseau Virtuel Privé peut se faire avec un serveur Zéphir ou manuellement.

Dans le cas d'une configuration manuelle il faut préparer la configuration avant l'instanciation :

- copier le répertoire `/home/data/vpn/<UAI>/<UAI>-amon.tar.gz` présent sur le module Sphynx sur le module Amon dans `/tmp/sphynx.tar.gz` ;
- sur le module Amon créer le répertoire `ConfIpsec` : `# mkdir -p /root/tmp/ConfIpsec` ;
- se rendre dans le répertoire `/root/tmp/ConfIpsec` : `# cd /root/tmp/ConfIpsec` ;
- désarchiver sphynx.tar.gz : `# tar xzf /tmp/sphynx.tar.gz`

Au lancement de la première instanciation, la question suivante vous sera posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non] [non] :`

Vous devez répondre `oui` à cette question.

Puis le choix `1.Manuel` ou `2.Zéphir` est proposé.

- Le choix `1.Manuel` permet de prendre en compte la configuration RVP présente sur le serveur, attention cette opération doit être effectuée avant d'exécuter l'instanciation ;
- Le choix `2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur le serveur Zéphir. Il sera demandé un utilisateur et mot de passe Zéphir et l'identifiant Zéphir du serveur Sphynx.

Dans les deux cas, la phrase de passe (passphrase) de la clé privée est demandée. Si le mot de passe est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Lors de cette phase de configuration du VPN sur Amon, les tunnels peuvent se couper dans les secondes qui suivent et dans certaines circonstances uniquement. Le problème est corrigé à partir de la version strongSwan 5.5.0 qui n'est pas disponible sur cette version d'EOLE.

Toutefois, le problème est très ponctuel et les tunnels seront relancés automatiquement par l'agent Zéphir assez rapidement.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

14. Résoudre des dysfonctionnements liés au MTU

Le PMTUd (Path MTU[p.893] discovery), activé par défaut sur les modules EOLE, est une technique permettant de déterminer, dans un réseau informatique, la taille du MTU[p.893] sur le chemin entre deux hôtes IP, afin d'éviter la fragmentation des paquets.



Cette configuration peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP[p.891] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTUd est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Il est possible de forcer la valeur du MTU pour une interface donnée dans l'onglet `Réseau avancé` de l'interface de configuration du module en mode expert.



Les commandes `ping`, `ip route` et `tracepath` sont utilisées pour ajuster les valeurs.

Utilisation de la commande `ping`

La commande `ping` permet de réaliser des tests en forçant la taille des paquets :

- ping OK avec une taille forcée à la valeur 1400 :

```
root@amon:~#  ping -M do -s 1400 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1400(1428) bytes of data.
1408 bytes from platon.ac-dijon.fr (194.167.18.17): icmp_seq=1 ttl=62 time=1.38 ms

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.380/1.380/1.380/0.000 ms
```

- ping KO avec une taille forcée à la valeur 1500 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
root@amon:~#  ping -M do -s 1500 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1500(1528) bytes of data.
ping: local error: Message too long, mtu=1500

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Utilisation de la commande `ip route`

La commande `ip route get to` permet de visualiser les problèmes de MTU.

```
# ip route get to 172.X.Y.Z
172.X.Y.Z dev eth0 src 10.67.V.W
cache expires 508sec mtu 1400
```

La commande `ip route flush cache` permet quant à elle de vider le cache.

Utilisation de la commande `tracepath`

La commande `tracepath` permet d'identifier où se trouvent les limitations du MTU.

```
# tracepath 172.X.Y.Z
1?: [LOCALHOST] pmtu 1500
1?: [LOCALHOST] pmtu 1438
1: 192.168.A.B 1.353ms
1: 192.168.C.D 1.972ms
2: 192.168.E.F 2.014ms
3: 192.168.G.H 1.657ms
4: 192.168.I.J 3.026ms
5: 192.168.K.L 2.543ms pmtu 1400
5: 172.M.N.O 9.930ms
6: no reply
...
```

Voir aussi...

> Onglet Réseau avancé [p.139]

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 7

Paramétrage des postes client

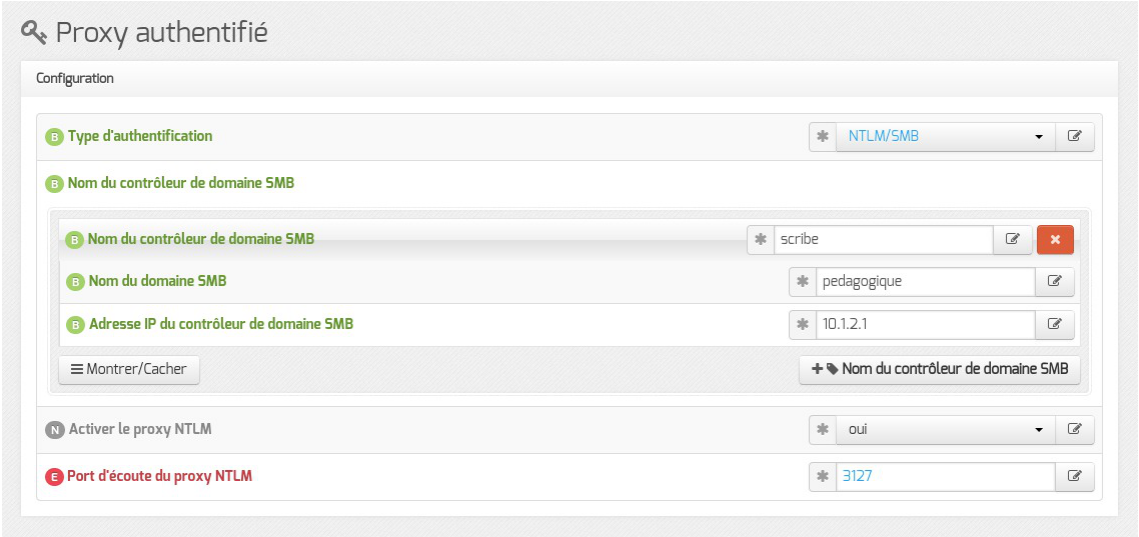
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine

L'authentification NTLM[p.895] pour des postes hors domaine est facilité par l'utilisation du proxy Cntlm[p.886].

Installation et activation

Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.

L'activation du service se fait dans l'interface de configuration du module dans l'onglet `Proxy authentifié`. Cet onglet n'est disponible que si l'authentification web a été, elle-même, activée dans l'onglet `Authentification`.



Vue de l'onglet Proxy authentifié dans l'interface de configuration du module

Il faut choisir le type d'authentification sur le proxy `NTLM/SMB` ou `NTLM/KERBEROS`.

Ensuite il faut passer la variable `Activer le proxy NTLM` à `oui`.

Par défaut, le port de Cntlm est le `3127` mais sa valeur peut être modifiée par le biais de la variable experte intitulée : `Port d'écoute du proxy NTLM`.

L'activation du service est effective après une reconfiguration du serveur avec la commande :

```
# reconfigure
```



Attention, si l'authentification de type `NTLM/SMB` est choisie, c'est le premier domaine spécifié qui sera utilisé par Cntlm.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Configuration des clients hors domaine

L'authentification proxy NTLM/SMB et NTLM/KERBEROS nécessite une configuration particulière des postes clients Windows.

Par défaut, il est nécessaire, par exemple, de modifier la base de registre sur le poste Windows Seven.

Mais dans le cas de l'utilisation de Cntlm aucun changement n'est requis dans la base de registre pour les postes hors domaine.

Les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Configuration des clients du domaine

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Il est donc nécessaire de configurer correctement les postes du domaine avec, par exemple, ESU[p.889].

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy .

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.247]

Onglet Proxy authentifié : 5 méthodes d'authentification [p.95]

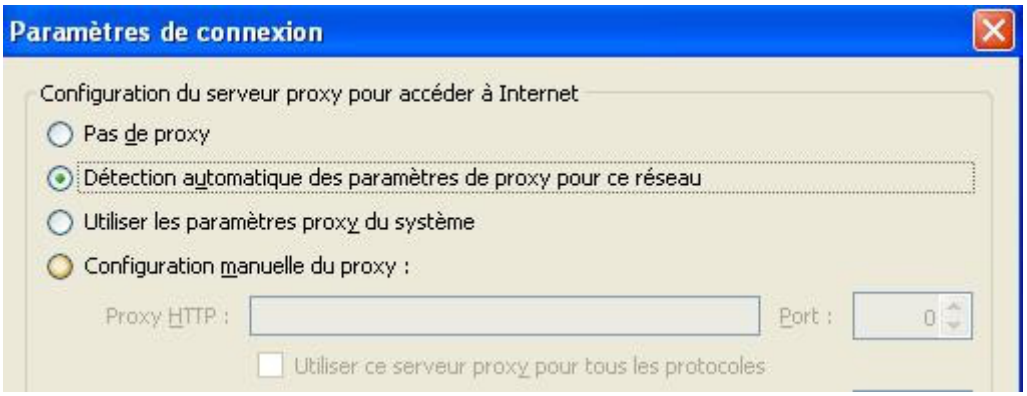
2. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.905] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine_local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm[p.886] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx[p.894] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom domain local>` qui pointe vers le serveur web ;
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

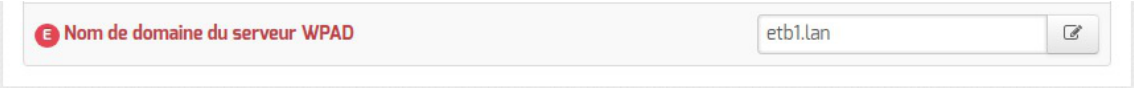
Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.

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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.



Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.

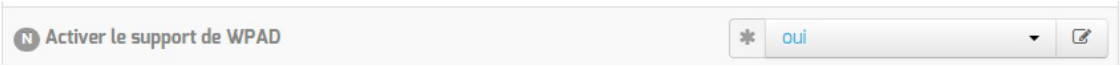
> Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

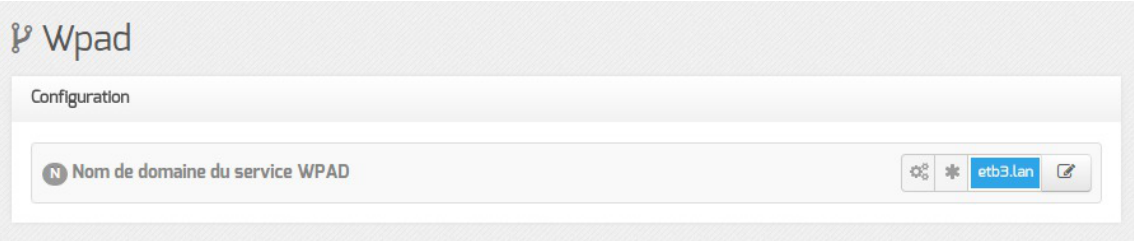
Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

> Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

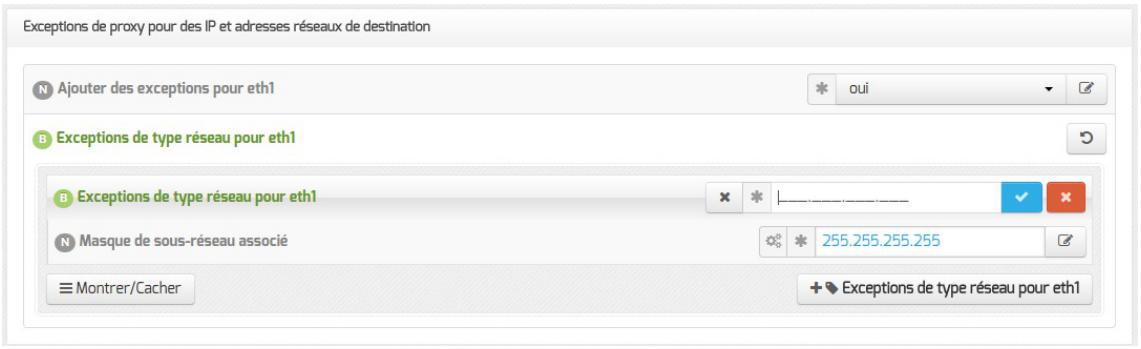
Ajouter des exclusions dans la configuration automatique du proxy

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton `Exceptions de type réseau pour eth-n` permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour lequelle on ne passe pas par le proxy.

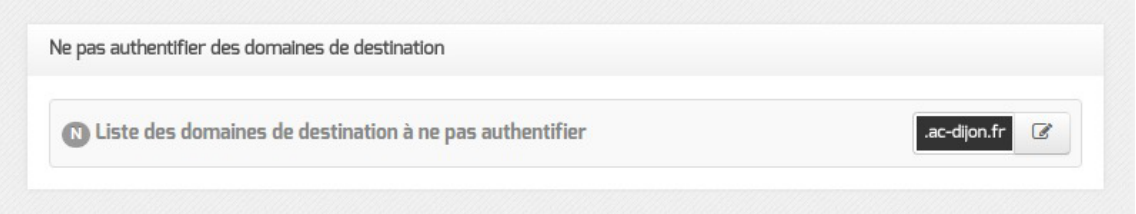


Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



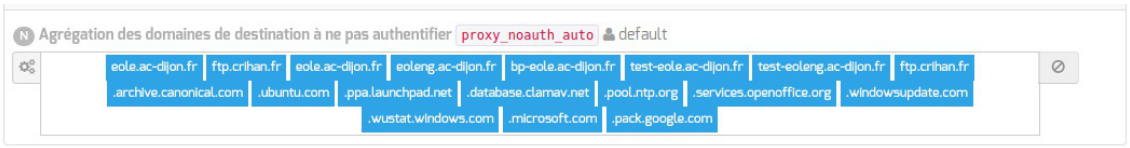
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

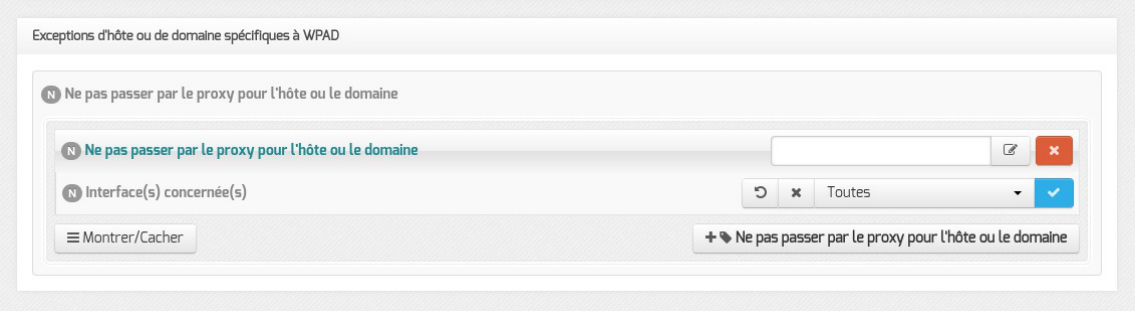
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.



Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `|| localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.



Compléments sur `Ne pas passer par le proxy pour le domaine` (dnsDomainIs) :

http://findproxyforurl.com/netscape-documentation/#dnsDomainIs

Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs

Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP [p.158]

3. Proxy non configuré dans le navigateur : redirection ou page d'information

Redirection transparente HTTP sur Amon

Sur le module Amon, les flux HTTP provenant des réseaux internes sont redirigés vers le proxy.



La redirection transparente ne fonctionne pas avec le protocole HTTPS car il s'agit d'un mode connecté qui ne supporte pas ce genre de manipulation sur les paquets. La redirection est faite uniquement pour obliger les postes à utiliser le proxy.

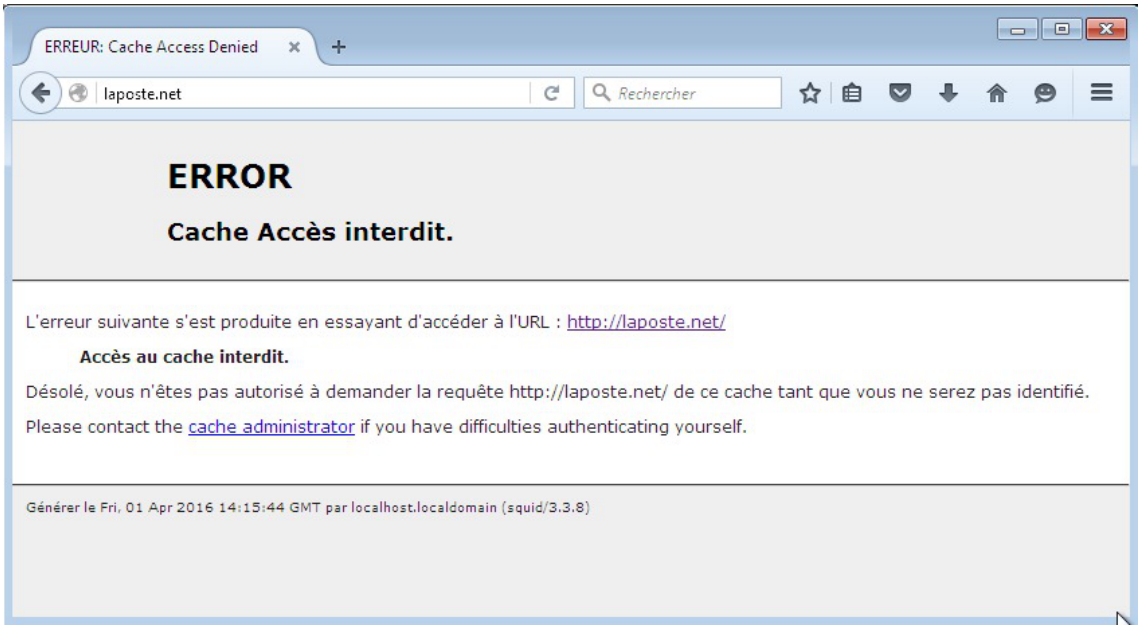


La redirection transparente n'est pas mise en place sur le module AmonEcole et ses variantes.



Si l'authentification du proxy est activée sur l'interface, la redirection fonctionnera mais pas l'authentification et l'utilisateur obtiendra une page d'erreur explicite provenant du logiciel Squid.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Page d'erreur renvoyée par Squid en cas d'erreur d'authentification

Dans l'onglet `Exceptions proxy` de l'interface de configuration du module, il est possible de déclarer des adresses de destination qui seront exclues de la redirection vers le proxy.

Page d'information renvoyée par Nginx

Sur les modules Amon et AmonEcole, la configuration du logiciel Nginx a été adaptée afin de détecter le cas où le navigateur du client n'a pas été configuré correctement et lui renvoyer un message d'erreur suffisamment explicite.



Page d'erreur renvoyée par Nginx en cas de proxy non configuré

La page d'erreur affichée dans le navigateur peut être personnalisée.

Personnaliser la page renvoyée par Nginx à l'aide d'un patch

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La page d'erreur affichée dans le navigateur est un template Creole : `/usr/share/eole/creole/distrib/nginx.no_proxy.html`

Il est possible de le modifier de façon pérenne en utilisant un patch pour Creole.

Il faut copier le template d'origine dans le répertoire `/usr/share/eole/creole/modif/`

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html /usr/share/eole/creole/modif/nginx.no_proxy.html
```

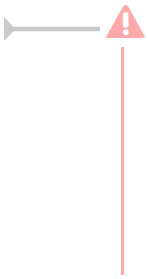
Il faut éditer, modifier et enregistrer le fichier copié

```
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Puis il faut générer le patch à l'aide de la commande `gen_patch`

```
root@amon:~# gen_patch
```

Le fichier contenant les différences est créé dans le répertoire `/usr/share/eole/creole/patch/`

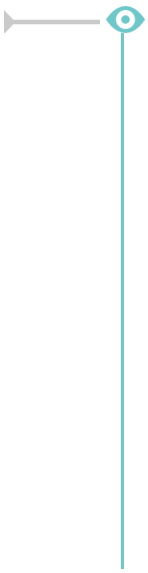


Les changements prennent effet après la reconfiguration du serveur à l'aide de la commande reconfigure

```
root@amon:~# reconfigure
```

La page servie par Nginx contient les modifications :

```
root@amon:~# vim /var/www/index.html
```



```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
/usr/share/eole/creole/modif/nginx.no_proxy.html
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
[...]
root@amon:~# gen_patch

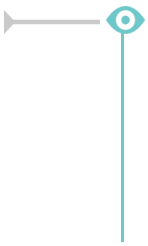
** Génération des patches à partir de modif **

Génération du patch nginx.no_proxy.html.patch

** Fin de la génération des patch **

root@amon:~# ls /usr/share/eole/creole/patch/
nginx.no_proxy.html.patch  variante
root@amon:~# reconfigure
[...]
root@amon:~# vim /var/www/index.html
```

Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
    <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
    <head>
<title>Veuillez configurer le proxy de votre navigateur</title>
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
<style>
.main {
        background:#bbbbbb;
        text-align:center;
}
h1 {
    /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
    color: #91e842;
    font-size: 50px;
    text-align:center;
    text-shadow: 0 1px 0 #eee,
              0 2px 0 #e5e5e5,
              -1px 3px 0 #C8C8C8,
              -1px 4px 0 #C1C1C1,
              -2px 5px 0 #B9B9B9,
              -2px 6px 0 #B2B2B2,
              -2px 7px 2px rgba(0,0,0, 0.6),
              -2px 7px 8px rgba(0,0,0, 0.2),
              -2px 7px 45px rgba(0,0,0, 0.4);
}
.message {
    top:25%;
    text-align:center;
    margin-left: 50px;
    margin-right: 50px;

    padding: 40px;
    background: #d2ff52;
    border: 1px solid #000000;

    border-radius: 10px;
    -moz-border-radius: 10px;
    -webkit-border-radius: 10px;

    box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
    -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
    -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
}
</style>
    </head>
    <body class='main'>
    <img src="./img/logoEolePt.png">
    <h1>%%libelle_etab</h1>
    <h2>Votre navigateur n'est pas correctement configuré !!</h2>
    <div class="message">Pour naviguer sur internet, un proxy doit être déclaré dans votre navigateur.<br />
Si vous accédez à la présente page, c'est que votre navigateur n'est pas configuré pour utiliser le proxy. Veuillez contacter le service informatique de l'établissement.</div>
    </body>
</html>

```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Page d'erreur renvoyée par Nginx en cas de proxy non configuré

4. Synthèse des paramètres proxy à utiliser pour les postes client

Module Amon standard

Sur une installation standard du module Amon, l'adresse du proxy sera l'adresse du serveur Amon sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau administratif : `adresse_ip_eth1:3128`
- proxy sur le réseau pédagogique : `adresse_ip_eth2:3128`
- proxy sur la DMZ : `adresse_ip_eth3:3128`

Module AmonEcole et ses variantes

Sur une installation standard des modules AmonEcole/AmonHorus, l'adresse du proxy sera l'adresse IP réservée pour le proxy sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3128`

On notera que, comme sur un module Amon standard, la passerelle est l'adresse du module Amon sur le réseau (adresse_ip_eth1). Mais par contre pour le DNS, il faut utiliser la même adresse IP que celle du proxy.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Double authentification

Si la double authentification est configurée, le port à utiliser pour le second proxy sera celui de la troisième configuration e2guardian (variable `dansguardian_port3` : 3129 par défaut), soit :

- proxy2 sur le réseau eth1 Amon : `adresse_ip_eth1:3129`
- proxy2 sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3129`

Proxy NTLM

Si l'authentification NTLM pour des postes hors domaine est configurée :

- les postes intégrés au domaine doivent continuer à utiliser le port de e2guardian (3128 par défaut) ;
- les postes nomades (hors domaine) doivent utiliser le port défini par la variable `cntlm_port` (3127 par défaut) pour passer par Cntlm.

Filtrage web désactivé

Si le filtrage web est désactivé, le proxy Squid écoute sur le port 3128 en lieu et place du logiciel de filtrage e2guardian.

En cas de double authentification, le second proxy répondra sur le port 3129.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 8

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 AmonEcole

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un serveur OpenLDAP.

L'installation d'`eole-annuaire` entraîne celle d'`eole-client-annuaire`.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

http://www.openldap.org/

Historique

L'annuaire LDAP est la brique centrale de plusieurs modules EOLE.

Grâce au paquet `eole-annuaire`, la configuration de base est identique sur les modules Horus, Scribe, Zéphir, Seshat et Thot bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `annuaire (id=10)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

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 [http://www.clamav.net/] et clamav-freshclam.

Historique

À 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 les modules AmonEcole et AmonHorus, 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-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).

1.4. eole-bareos

Le paquet `eole-bareos` permet d'installer et de configurer la solution de sauvegarde Bareos.

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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Conteneurs

Le service s'installe sur le système hôte (maître).

1.5. 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.

1.6. eole-courier

Le paquet `eole-courier` permet la mise en place d'un serveur POP/IMAP.

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 les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Remarques

Le greffon authProg fourni par le paquet `courier-eolecas` permet au serveur IMAP d'être compatible avec une authentification CAS.

1.7. eole-cups

Le paquet `eole-cups` permet la mise en place d'un serveur d'impression.

La gestion des imprimantes fait l'objet d'une documentation dédiée : Imprimantes.

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 les modules AmonEcole et AmonHorus, 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`).

1.8. 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).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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).

1.9. eole-dhcp

Le paquet `eole-dhcp` permet la mise en place d'un serveur DHCP local et/ou d'un serveur PXE.

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 (module Scribe et module 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 les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `partage (id=52)`.

Sur le module Eclair 2.3 et AmonEcole+, il est installé dans le groupe de conteneurs : `ltspserver (id=54)`.

Remarques

Ne pas confondre ce paquet avec le paquet `eole-dhcrelay` qui est pré-installé sur le module Amon.

1.10. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS local.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.884].

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)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.11. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP Exim.

Logiciels et services

Le paquet `eole-exim` s'appuie principalement sur le service exim4.

http://www.exim.org/

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais utilisé sur tous les modules.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur le module AmonEcole et ses variantes, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.12. eole-fichier-primaire

Le paquet `eole-fichie-primaire` permet la mise en place d'un serveur de fichiers complet.

Logiciels et services

Le paquet `eole-fichie-primaire` permet de gérer les services suivants :

- smbd, nmbd et Scannedonly[p.901] (serveur de fichiers) ;
- nscd (cache).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 les modules AmonEcole et AmonHorus, 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`).

1.13. eole-mysql

Le paquet `eole-mysql` permet la mise en place d'un serveur de base de données MySQL.

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 les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.14. 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).

1.15. eole-proftpd

Le paquet `eole-proftpd` permet la mise en place d'un serveur FTP.

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

Le service est configuré pour s'installer dans le conteneur : `ftp (id=25)`.
Sur les modules AmonEcole et AmonHorus, 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`).

1.16. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

La gestion du proxy et du filtrage web fait l'objet d'une documentation dédiée : Proxy.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- e2guardian : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM/KERBEROS.

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 les modules AmonEcole et AmonHorus, 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`).

Remarques

Afin d'assurer l'authentification 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* .

1.17. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur RADIUS[p.899].

Logiciels et services

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 serveur maître.

1.18. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.
Le logiciel utilisé, Nginx[p.894], peut aussi faire office de serveur web.
http://nginx.org/

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.19. 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 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 : `mail (id=13)`.
Sur les modules Scribe/AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.20. eole-sympa

Le paquet `eole-sympa` permet la mise en place d'un serveur de listes de diffusion.

La gestion des listes de diffusion fait l'objet d'une documentation dédiée : ListesDeDiffusion.

Logiciels et services

Le paquet `eole-sympa` s'appuie principalement sur le service sympa.
Son interface d'administration nécessite un serveur web apache2.
http://www.sympa.org/



L'installation d'`eole-sympa` entraîne celle d'`eole-exim`.

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 les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

1.21. 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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 les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Ce paquet sert de brique de base pour toutes les applications web packagées par les équipes des projets EOLE et Envole.

1.22. eole-wpad

Le paquet `eole-wpad` permet la mise en place du service de découverte automatique du proxy par les navigateurs (WPAD[p.905]).

Le logiciel utilisé, Nginx[p.894], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

http://nginx.org/

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

Historique

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, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

2. Ports utilisés sur le module AmonEcole

Le module AmonEcole propose de nombreux services.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ce document donne la liste exhaustive des ports utilisés sur un module AmonEcole standard.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.
Il est possible de lister les ports ouverts sur le serveur par la commande :
`netstat -ntulp`



En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 25/tcp : smtp (Exim4)
- 68/udp : dhclient
- 123/udp : ntpd
- 514/udp : rsyslogd (réception des journaux distants)
- 3493/tcp : nut (gestion des onduleurs)
- 4200/tcp : ead-web
- 4201/tcp : ead-server
- 4202/tcp : ead-server (transfert de fichiers)
- 5000/tcp : eoleflask/eolegenconfig (application admin)
- 7000/tcp : gen_config
- 8000/tcp : creoled
- 8090/tcp : z_stats (consultation des statistiques Zéphir locales), mise à jour automatique du client Zéphir
- 8443/tcp : EoleSSO
- 10514/tcp : rsyslogd (réception des journaux distants, protocole TCP)
- 12560/tcp : rsyslogd (réception des journaux distants, protocole RELP)

Ports spécifiques au module Amon

- 50/esp : IPsec
- 53/tcp+udp : bind (DNS)
- 67/udp : dhcrelay
- 500/udp : charon (VPN)
- 953/tcp : bind (RNDC)
- 1812/udp : radius
- 1813/tcp+udp : radius accounting

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 3127/tcp : Cntlm (proxy NTLM)
- 3128/tcp : e2guardian (filtrage web)
- 3129/tcp : e2guardian (filtrage web)
- 3401/udp : squid (agent SNMP)
- 4500/udp : charon (VPN)
- 8062/tcp : cgi lightsquid (consultation des statistiques de navigation)
- 8080/tcp : squid (proxy)
- 8081/tcp : squid (proxy)

Le proxy inverse Nginx est susceptible d'écouter sur de nombreux ports afin d'assurer ses missions de redirection :

- 80/tcp : nginx (redirection http)
- 81/tcp : nginx (erreur proxy http)
- 82/tcp : nginx (erreur proxy https)
- 443/tcp : nginx (redirection https)
- 4203/tcp : nginx (redirection vers un EAD)
- 7070/tcp : nginx (redirection vers un portail Envole)
- 8443/tcp : nginx (redirection vers un serveur EoleSSO)

Ports spécifiques au module Scribe

- 21/tcp : ftp (ProFTPD)
- 25/tcp : smtp (Exim4)
- 67/udp : dhcp
- 69/udp : tftp
- 80/tcp : http (Apache2)
- 110/tcp : pop3 (Courier)
- 137/udp : nmbd
- 138/udp : nmbd
- 139/tcp : samba (netbios)
- 143/tcp : imap (Courier)
- 389/tcp : ldap (OpenLDAP)
- 443/tcp : https (Apache2)
- 445/tcp : samba (sans netbios)
- 631/tcp+udp : CUPS
- 783/tcp: Spamassassin
- 993/tcp : imap-SSL (Courier)
- 995/tcp : pop3-SSL (Courier)

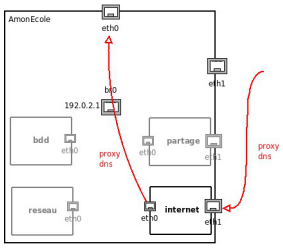
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 1099/tcp : Synchronisation LSC (EoleAD)
- 3306/tcp : MySQL
- 7070/tcp : admin-posh-profil
- 7080/tcp : posh-profil (XML-RPC)
- 8787/tcp : application web Sympa (domaine externe)
- 8789/tcp : controle-vnc (serveur de commandes)
- 8790/tcp : controle-vnc (serveur de fichiers)
- 8888/tcp : application web Sympa (domaine interne)
- 9101/tcp : bareos-dir
- 9102/tcp : bareos-fd
- 9103/tcp : bareos-sd
- 10000/tcp : eoleflask/eolegenconfig (application non admin)

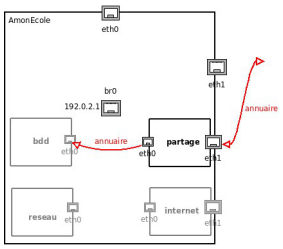
Services et numéro de ports

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

3. Les flux réseaux entre conteneurs du module AmonEcole



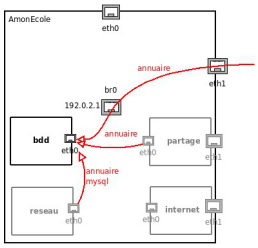
Le conteneur "internet"



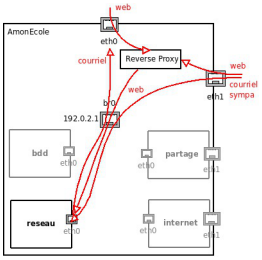
Le conteneur "partage"

Les deux autres conteneurs ne sont accessibles que par le réseau interne.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Le conteneur "bdd"



Le conteneur "réseau"

4. L'annuaire LDAP du module Scribe

L'annuaire LDAP[p.892] du module Scribe 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.

Il fournit les services suivants :

- authentification utilisateur ;
- comptes Samba et messagerie électronique ;
- définition des groupes et des partages.

Les modules Scribe et AmonEcole utilisent 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 au module Scribe :
  - `eleves`
  - `professeurs`
  - `administratifs`

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 `professeurs`, `eleves` et `administratifs` permettant d'appliquer des méthodes de gestion spécifiques comme l'appartenance à une classe (élève) ou à une équipe pédagogique (professeur).

Ces groupes permettent aussi d'accorder des autorisations :

- d'observer ou la possibilité d'être observé ;
- de bloquer l'accès Internet d'un autre utilisateur ;
- et de distribuer des documents (devoirs).

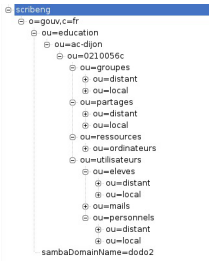
4.1. Arborescence de l'annuaire

La racine de l'annuaire *(basedn)* est : **o=gouv,c=fr**

Chaque établissement possède une arborescence distincte grâce à l'utilisation des variables `nom academie` et `numero etab` pour les unités organisationnelles suivantes *(ou)*.

Exemple : `ou=0210056c,ou=ac-dijon,ou=education,o=gouv,c=fr`

Cela implique qu'il n'est plus possible de modifier ces deux variables, une fois le serveur instancié.



L'arborescence de l'annuaire d'un module Scribe

4.2. Utilisateurs spéciaux

Le compte d'administration

L'administrateur LDAP[p.892] 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 :

`/etc/smbldap-tools/smbldap_bind.conf`

ou de le modifier "manuellement" à l'aide de la commande `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.882]. 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
```

4.3. Entrée groupe

Les groupes de l'établissement sont placés dans la branche :

`ou=local,ou=groupes,ou=numero_etab,ou=nom_academie,ou=education,o=gouv,c=fr`

Classes d'objet

Les groupes héritent des classes d'objet suivantes :

- posixGroup (`nis.schema`)
- sambaGroupMapping (`samba.schema`)
- eolegroupe (`eole.schema`)
- ENTGroupe (`ent.schema`)

Les classes (au sens Éducation nationale du terme) possèdent des classes d'objet supplémentaires :

- classe (`eole.schema`)
- ENTClasse (`ent.schema`)

Attributs

Attributs Unix et Samba

- gidNumber
- memberUid : uid des membres du groupe
- sambaSID : SID du groupe
- sambaGroupType : "2"

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Autres attributs

Les attributs spécifiques aux groupes sont les suivants :

- cn : nom du groupe
- type : "Niveau", "Classe", "Equipe", "Matiere", "Service", "Groupe"...
- description : libellé du groupe
- mail : adresse électronique de la liste de diffusion du groupe, si elle existe
- LastUpdate : date de dernière modification du groupe, au format *aaaammjj*

Les classes (au sens Éducation nationale du terme) ont un attribut supplémentaire :

- niveau : niveau associé à la classe

4.4. Entrée élève

Les élèves de l'établissement sont placés dans la branche :

```
ou=local,ou=eleves,ou=utilisateurs,ou=numero_etab,ou=nom_academie,ou=educat
```

Classes d'objet

Les élèves héritent des classes d'objet suivantes :

- posixAccount (`nis.schema`)
- sambaSAMAccount (`samba.schema`)
- inetOrgPerson (`inetorgperson.schema`)
- shadowAccount (`nis.schema`)
- Eleves (`eole.schema`)
- ENTPerson (`ent.schema`)
- ENTEleve (`ent.schema`)
- radiusprofile (`radius.schema`)

Attributs

Attributs communs à tous les utilisateurs

- uid : login de l'utilisateur
- cn : nom complet
- sn : nom de famille
- givenName : prénom
- displayName : nom complet
- gecos : nom complet sans caractères spéciaux
- userPassword : mot de passe de l'utilisateur (type Unix) **[accès restreint]**
- mail : adresse électronique (locale ou externe)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- mailHost : "localhost" si la boite est locale, absent sinon
- mailDir : chemin Unix du MailDir si la boite est locale, absent sinon
- ENTPersonLogin : identifiant ENT (par défaut : l'uid de l'utilisateur)
- ENTPersonJointure : clés de jointures (par défaut : "ENT")
- ENTPersonProfils : profils associés (eleve, enseignant, administratif ou responsable)
- ENTPersonNomPatro : nom patronymique
- personalTitle : titre de civilité (M., Mme ou Mlle)
- codecivilite : code de civilité (1->M., 2->Mme, 3->Mlle)
- ENTPersonSexe : sexe (M ou F)
- dateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonDateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonAutresPrenoms : autres prénoms que le prénom usuel (facultatif)
- intid : identifiant interne (en général le code associé dans SIECLE ou AAF)
- LastUpdate : date de dernière modification du compte, au format *aaaammjj*

Attributs Unix

- uidNumber
- gidNumber
- homeDirectory : chemin Unix du partage personnel
- loginShell : shell de l'utilisateur (par défaut : "/bin/false")
- shadowLastChange : date de dernière modification du mot de passe (Unix)
- shadowMax : nombre de jours d'utilisation maximum du mot de passe (Unix)

Attributs Samba

- sambaAcctFlags : bits de contrôle samba (par défaut : "[U]")
- sambaHomeDrive : lettre associé au partage personnel (par défaut : "U:")
- sambaHomePath : chemin UNC du partage personnel
- sambaKickoffTime : timestamp utilisé pour déconnecter un utilisateur automatiquement
- sambaLMPassword : mot de passe (format Windows 9x) **[accès restreint]**
- sambaLogoffTime : date de la dernière fermeture de session
- sambaLogonTime : date de la dernière ouverture de session
- sambaNTPassword : mot de passe (format NT) **[accès restreint]**
- sambaPrimaryGroupSID : sambaSID du groupe principal de l'utilisateur
- sambaProfilePath : chemin UNC du profil (absent si profil local)
- sambaPwdCanChange : l'utilisateur peut changer son mot de passe
- sambaPwdLastSet : date de la dernière modification du mot de passe (Windows)
- sambaPwdMustChange : l'utilisateur doit changer son mot de passe

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- sambaSID : SID du compte de l'utilisateur

Attributs FreeRADIUS

- radiusTunnelType : "VLAN"
- radiusFilterId : "Enterasys:version=1:policy=Enterprise User"
- radiusTunnelMediumType : "IEEE-802"

Attributs spécifiques aux élèves

- employeeNumber : numéro interne (elenoet) **[accès restreint]**
- Ine : Identifiant National Élève[p.891] **[accès restreint]**
- ENTEleveStructRattachId : numéro unique de l'élève dans la structure de rattachement **[accès restreint]**
- Divcod : classe
- ENTEleveClasses : dn de l'établissement $ classe
- Meflcf : niveau
- ENTEleveMEF : niveau
- ENTEleveLibelleMEF : libellé du niveau
- ENTEleveEnseignements : enseignements suivis (optionnel)
- ENTEleveFiliere : filière (optionnel)
- ENTEleveMajeur : élève majeur (optionnel)
- ENTEleveNivFormation : niveau de formation (optionnel)
- ENTEleveStatutEleve : statut de l'élève (par défaut : "ELEVE")
- ENTEleveRegime : régime de l'élève (INTERNE, 1/2 PENSION, ...)

4.5. Entrée enseignant

Les enseignants de l'établissement sont placés dans la branche :

```
ou=local,ou=personnels,ou=utilisateurs,ou=numero_etab,ou=nom_academie,ou=edu
```

Classes d'objet

Les enseignants héritent des classes d'objet suivantes :

- posixAccount (`nis.schema`)
- sambaSAMAccount (`samba.schema`)
- inetOrgPerson (`inetorgperson.schema`)
- shadowAccount (`nis.schema`)
- administrateur (`eole.schema`)
- ENTPerson (`ent.schema`)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- ENTAuxEnseignant (`ent.schema`)
- radiusprofile (`radius.schema`)

Attributs

Attributs communs à tous les utilisateurs

- uid : login de l'utilisateur
- cn : nom complet
- sn : nom de famille
- givenName : prénom
- displayName : nom complet
- gecos : nom complet sans caractères spéciaux
- userPassword : mot de passe de l'utilisateur (type Unix) **[accès restreint]**
- mail : adresse électronique (locale ou externe)
- mailHost : "localhost" si la boite est locale, absent sinon
- mailDir : chemin Unix du MailDir si la boite est locale, absent sinon
- ENTPersonLogin : identifiant ENT (par défaut : l'uid de l'utilisateur)
- ENTPersonJointure : clés de jointures (par défaut : "ENT")
- ENTPersonProfils : profils associés (eleve, enseignant, administratif ou responsable)
- ENTPersonNomPatro : nom patronymique
- personalTitle : titre de civilité (M., Mme ou Mlle)
- codecivilite : code de civilité (1->M., 2->Mme, 3->Mlle)
- ENTPersonSexe : sexe (M ou F)
- dateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonDateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonAutresPrenoms : autres prénoms que le prénom usuel (facultatif)
- intid : identifiant interne (en général le code associé dans SIECLE ou AAF)
- LastUpdate : date de dernière modification du compte, au format *aaaammjj*

Attributs Unix

- uidNumber
- gidNumber
- homeDirectory : chemin Unix du partage personnel
- loginShell : shell de l'utilisateur (par défaut : "/bin/false")
- shadowLastChange : date de dernière modification du mot de passe (Unix)
- shadowMax : nombre de jours d'utilisation maximum du mot de passe (Unix)

Attributs Samba

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- sambaAcctFlags : bits de contrôle samba (par défaut : "[U]")
- sambaHomeDrive : lettre associé au partage personnel (par défaut : "U:")
- sambaHomePath : chemin UNC du partage personnel
- sambaKickoffTime : timestamp utilisé pour déconnecter un utilisateur automatiquement
- sambaLMPassword : mot de passe (format Windows 9x) **[accès restreint]**
- sambaLogoffTime : date de la dernière fermeture de session
- sambaLogonTime : date de la dernière ouverture de session
- sambaNTPassword : mot de passe (format NT) **[accès restreint]**
- sambaPrimaryGroupSID : sambaSID du groupe principal de l'utilisateur
- sambaProfilePath : chemin UNC du profil (absent si profil local)
- sambaPwdCanChange : l'utilisateur peut changer son mot de passe
- sambaPwdLastSet : date de la dernière modification du mot de passe (Windows)
- sambaPwdMustChange : l'utilisateur doit changer son mot de passe
- sambaSID : SID du compte de l'utilisateur

Attributs FreeRADIUS

- radiusTunnelType : "VLAN"
- radiusFilterId : "Enterasys:version=1:policy=Enterprise User"
- radiusTunnelMediumType : "IEEE-802"

Attributs spécifiques aux enseignants

- typeadmin : 0 → enseignant, 1 → administrateur, 2 → enseignant responsable de classe, 3 → personnel administratif
- Divcod : liste des classes administrées par l'enseignant
- FederationKey : clé de fédération (en général l'adresse électronique académique)

4.6. Entrée personnel administratif

Les personnels administratifs de l'établissement sont placés dans la branche :

```
ou=local,ou=personnels,ou=utilisateurs,ou=numero_etab,ou=nom_academie,ou=edu
```

Classes d'objet

Les personnels administratif héritent des classes d'objet suivantes :

- posixAccount (`nis.schema`)
- sambaSAMAccount (`samba.schema`)
- inetOrgPerson (`inetorgperson.schema`)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- shadowAccount (`nis.schema`)
- administratif (`schema/eole.schema`)
- ENTPerson (`ent.schema`)
- ENTAuxNonEnsEtab (`ent.schema`)
- radiusprofile (`radius.schema`)

Attributs

Attributs communs à tous les utilisateurs

- uid : login de l'utilisateur
- cn : nom complet
- sn : nom de famille
- givenName : prénom
- displayName : nom complet
- gecos : nom complet sans caractères spéciaux
- userPassword : mot de passe de l'utilisateur (type Unix) **[accès restreint]**
- mail : adresse électronique (locale ou externe)
- mailHost : "localhost" si la boite est locale, absent sinon
- mailDir : chemin Unix du MailDir si la boite est locale, absent sinon
- ENTPersonLogin : identifiant ENT (par défaut : l'uid de l'utilisateur)
- ENTPersonJointure : clés de jointures (par défaut : "ENT")
- ENTPersonProfils : profils associés (eleve, enseignant, administratif ou responsable)
- ENTPersonNomPatro : nom patronymique
- personalTitle : titre de civilité (M., Mme ou Mlle)
- codecivilite : code de civilité (1->M., 2->Mme, 3->Mlle)
- ENTPersonSexe : sexe (M ou F)
- dateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonDateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonAutresPrenoms : autres prénoms que le prénom usuel (facultatif)
- intid : identifiant interne (en général le code associé dans SIECLE ou AAF)
- LastUpdate : date de dernière modification du compte, au format *aaaammjj*

Attributs Unix

- uidNumber
- gidNumber
- homeDirectory : chemin Unix du partage personnel
- loginShell : shell de l'utilisateur (par défaut : "/bin/false")

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- shadowLastChange : date de dernière modification du mot de passe (Unix)
- shadowMax : nombre de jours d'utilisation maximum du mot de passe (Unix)

Attributs Samba

- sambaAcctFlags : bits de contrôle samba (par défaut : "[U]")
- sambaHomeDrive : lettre associé au partage personnel (par défaut : "U:")
- sambaHomePath : chemin UNC du partage personnel
- sambaKickoffTime : timestamp utilisé pour déconnecter un utilisateur automatiquement
- sambaLMPassword : mot de passe (format Windows 9x) **[accès restreint]**
- sambaLogoffTime : date de la dernière fermeture de session
- sambaLogonTime : date de la dernière ouverture de session
- sambaNTPassword : mot de passe (format NT) **[accès restreint]**
- sambaPrimaryGroupSID : sambaSID du groupe principal de l'utilisateur
- sambaProfilePath : chemin UNC du profil (absent si profil local)
- sambaPwdCanChange : l'utilisateur peut changer son mot de passe
- sambaPwdLastSet : date de la dernière modification du mot de passe (Windows)
- sambaPwdMustChange : l'utilisateur doit changer son mot de passe
- sambaSID : SID du compte de l'utilisateur

Attributs FreeRADIUS

- radiusTunnelType : "VLAN"
- radiusFilterId : "Enterasys:version=1:policy=Enterprise User"
- radiusTunnelMediumType : "IEEE-802"

Attributs spécifiques aux personnels administratifs

- typeadmin : "3" pour les personnels administratifs
- FederationKey : clé de fédération (en général l'adresse électronique académique)

4.7. Entrée responsable légal

Les responsables légaux de l'établissement sont placés dans la branche :

```
ou=responsables,ou=utilisateurs,ou=numero_etab,ou=nom_academie,ou=education,
```

Classes d'objet

Les responsables légaux héritent des classes d'objet suivantes :

- inetOrgPerson (`inetorgperson.schema`)
- responsable (`eole.schema`)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- ENTPerson (`ent.schema`)
- ENTAuxPersRelEleve (`ent.schema`)

Attributs

Attributs communs à tous les utilisateurs

- uid : login de l'utilisateur
- cn : nom complet
- sn : nom de famille
- givenName : prénom
- displayName : nom complet
- gecos : nom complet sans caractères spéciaux
- userPassword : mot de passe de l'utilisateur (type Unix) **[accès restreint]**
- mail : adresse électronique (locale ou externe)
- mailHost : "localhost" si la boite est locale, absent sinon
- mailDir : chemin Unix du MailDir si la boite est locale, absent sinon
- ENTPersonLogin : identifiant ENT (par défaut : l'uid de l'utilisateur)
- ENTPersonJointure : clés de jointures (par défaut : "ENT")
- ENTPersonProfils : profils associés (eleve, enseignant, administratif ou responsable)
- ENTPersonNomPatro : nom patronymique
- personalTitle : titre de civilité (M., Mme ou Mlle)
- codecivilite : code de civilité (1->M., 2->Mme, 3->Mlle)
- ENTPersonSexe : sexe (M ou F)
- dateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonDateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonAutresPrenoms : autres prénoms que le prénom usuel (facultatif)
- intid : identifiant interne (en général le code associé dans SIECLE ou AAF)
- LastUpdate : date de dernière modification du compte, au format *aaaammjj*

Attributs spécifiques aux responsables légaux

- eleve : uid des élèves du responsable **[accès restreint]**
- ENTAuxPersRelEleveEleve : dn des élèves du responsable **[accès restreint]**
- ENTPersonAdresse : adresse **[accès restreint]**
- ENTPersonCodePostal : code postal **[accès restreint]**
- ENTPersonVille : ville **[accès restreint]**
- ENTPersonPays : pays **[accès restreint]**
- homePhone : numéro de téléphone **[accès restreint]**

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- telephoneNumber : numéro de téléphone professionnel **[accès restreint]**
- mobile : numéro de téléphone portable **[accès restreint]**
- mailPerso : adresse électronique fournie par le responsable (peut être différente de celle utilisée)

4.8. Entrée compte invité

Les comptes invités de l'établissement sont placés dans la branche :

```
ou=autres,ou=utilisateurs,ou=numero_etab,ou=nom_academie,ou=education,o=gouv
```

Classes d'objet

Les comptes invités héritent des classes d'objet suivantes :

- inetOrgPerson (`inetorgperson.schema`)
- autre (`eole.schema`)
- ENTPerson (`ent.schema`)

Attributs

Attributs communs à tous les utilisateurs

- uid : login de l'utilisateur
- cn : nom complet
- sn : nom de famille
- givenName : prénom
- displayName : nom complet
- gecos : nom complet sans caractères spéciaux
- userPassword : mot de passe de l'utilisateur (type Unix) **[accès restreint]**
- mail : adresse électronique (locale ou externe)
- mailHost : "localhost" si la boite est locale, absent sinon
- mailDir : chemin Unix du MailDir si la boite est locale, absent sinon
- ENTPersonLogin : identifiant ENT (par défaut : l'uid de l'utilisateur)
- ENTPersonJointure : clés de jointures (par défaut : "ENT")
- ENTPersonProfils : profils associés (eleve, enseignant, administratif ou responsable)
- ENTPersonNomPatro : nom patronymique
- personalTitle : titre de civilité (M., Mme ou Mlle)
- codecivilite : code de civilité (1->M., 2->Mme, 3->Mlle)
- ENTPersonSexe : sexe (M ou F)
- dateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonDateNaissance : date de naissance, au format *aaaammjj* **[accès restreint]**
- ENTPersonAutresPrenoms : autres prénoms que le prénom usuel (facultatif)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- intid : identifiant interne (en général le code associé dans SIECLE ou AAF)
- LastUpdate : date de dernière modification du compte, au format *aaaammjj*

Attributs spécifiques aux invités

les comptes invités n'ont pas d'attributs particuliers.

4.9. 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 :

- 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=*$
```

4.10. 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`)

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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)

4.11. Annuaire : diagnostic et résolution de problème

Exécuter le service en mode débogage

Les commandes suivantes permettent de relancer le service *slapd* en mode débogage :

```
# service slapd stop
# slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 256
```


L'option -d pour le débogage est suivie de la valeur de masquage 256 qui offre la verbosité nécessaire.

Ré-indexer l'annuaire

Dans certaines situations, la ré-indexation de l'annuaire s'avère nécessaire.

Les commandes suivantes permettent de re-créer les fichiers d'index :

```
# service slapd stop
# su openldap -s /bin/bash -c "slapindex -f /etc/ldap/slapd.conf -v"
```

Sauvegarde et restauration de l'annuaire

Export automatique de l'annuaire

Sur les modules EOLE possédant un annuaire local, un export de l'annuaire est réalisé toutes les nuits dans le fichier `/home/backup/sauv_ldap.ldif` .

C'est le cas même si la sauvegarde Bareos n'est pas activée car c'est `eole-schedule` qui gère l'export.

La programmation de l'export quotidien peut-être vérifiée à l'aide de la commande suivante :

```
# manage_schedule -l
```

Si l'export automatique est bien activé, les lignes suivantes apparaissent dans le résultat :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
  * les tâches journalières se feront tous les jours à 01:14 (hors
sauvegarde)
   - avant sauvegarde
    + Exportation de l'annuaire LDAP (annuaire)
```

Restauration de l'export quotidien

En cas de crash de l'annuaire OpenLDAP, restaurer l'annuaire tel qu'il était la nuit précédente peut permettre de gagner du temps sur la mise à disposition des services.

La restauration s'effectue à l'aide des commandes habituelles :

```
# service slapd stop
# rm -f /var/lib/ldap/[^D]*
# slapadd -f /etc/ldap/slapd.conf -l /home/backup/sauv_ldap.ldif
# chown -R openldap: /var/lib/ldap/
# service slapd start
```

Restauration de la dernière sauvegarde

Dans le cas où la sauvegarde Bareos est utilisée, il est possible de restaurer l'annuaire tel qu'il était lors de la dernière sauvegarde.

La restauration de l'annuaire depuis la sauvegarde s'effectue à l'aide de la commande :

```
# bareosrestore.py --ldap
```

Export manuel de l'annuaire

La commande suivante permet d'exporter le contenu de l'annuaire dans un fichier :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no > annuaire.ldif
```

Voir aussi...

- Gestion des tâches planifiées eole-schedule
- Restauration partielle [p.613]

5. Exportation des fichiers depuis SIECLE et STS

SIECLE

Ouvrir l'application Base élèves établissement et cliquer sur le lien `Mise à jour`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Accès à Base Élèves

Dans le menu de gauche, choisir : Exportations / En XML



Les Exports XML Génériques

Puis sélectionner successivement :

- Nomenclature ;
- Structures ;
- Élèves sans adresse ;
- Responsables avec adresse.

et enregistrer chacun des fichiers ZIP générés.

STS-Web

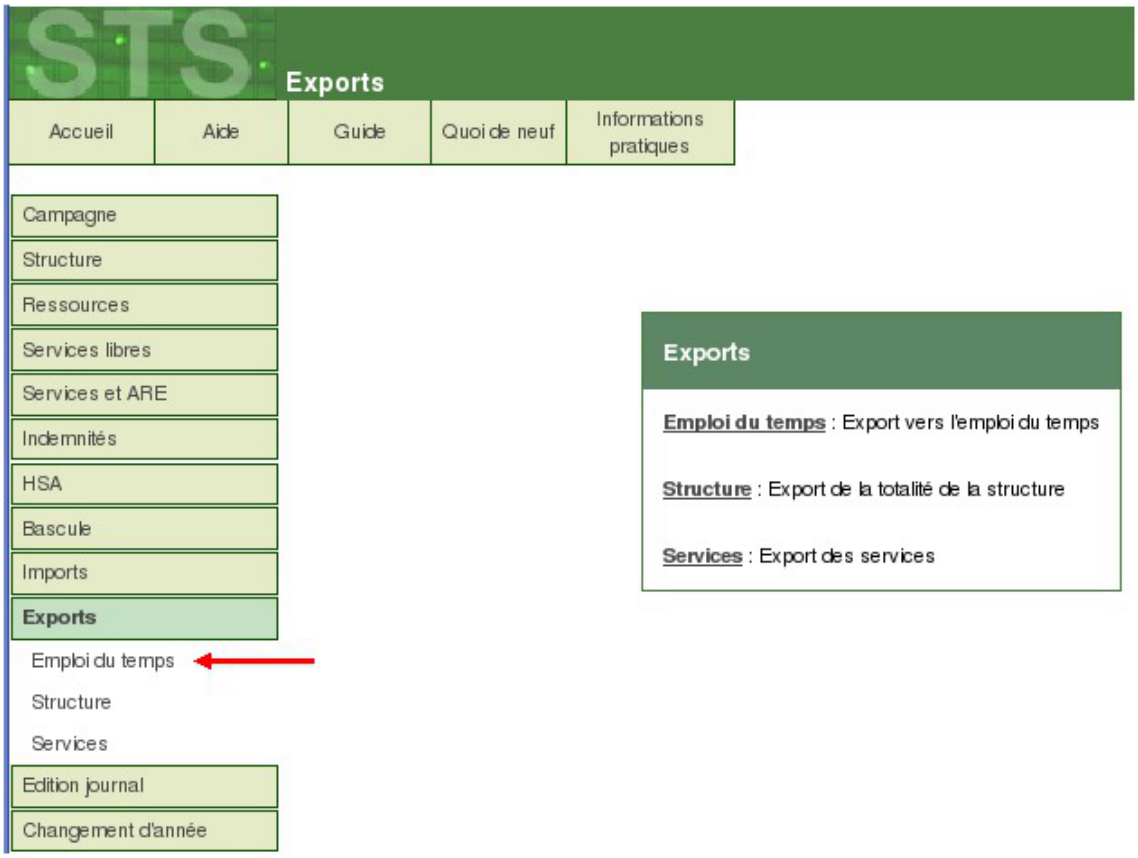
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Ouvrir l'application STS-Web et cliquer sur `STS - Mise à jour`



Accès à STS - Mise à jour

Dans `Exports` choisir `Emploi du temps` :



Les Exports dans STS

Enregistrer le fichier .xml qui servira à l'importation des professeurs et des personnels administratifs.

6. Le gestionnaire de listes électroniques Sympa

6.1. Architecture du gestionnaire de liste de diffusion

Les fichiers de configuration définissant chaque liste de diffusion sont stockés dans un répertoire du nom de la liste dans :

- `/var/lib/sympa/expl/` pour les listes du domaine Internet ;
- `/var/lib/sympa/expl/i-monetab.ac-acad.fr` pour les listes du domaine interne

C'est l'une des raisons pour lesquelles il n'est pas possible de modifier la variable `domaine messagerie etab` une fois l'instanciation du serveur effectuée.

Les archives des listes sont stockées dans le répertoire `/var/lib/sympa/wwsarchive`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour redémarrer Sympa il faut utiliser la commande `service sympa restart` . Avant cela il faut impérativement que MySQL soit démarré, sinon des erreurs se produiront.

L'interface web Sympa est gérée par le fichier `/usr/lib/cgi-bin/sympa/wwsympa.fcgi`. Il s'agit d'un script CGI[p.885] en perl qui utilise le mode *fcgid* d'apache2 pour fonctionner. La présence d'un sticky bit sur ce fichier est nécessaire pour assurer le bon fonctionnement de l'application.

Les alias des listes de diffusions (utilisés par le MTA[p.893] Exim4[p.889]) sont stockés dans le fichier `/etc/mail/sympa.aliases`

Pour plus d'information, veuillez vous référer à la documentation officielle du logiciel :

http://www.sympa.org/doc/index

Sur le module AmonEcole, tous les fichiers indiqués ci-dessus se trouvent dans le conteneur `bdd`.

Pour modifier les *Catégories de liste* proposées, il est obligatoire de patcher le template EOLE :

`/usr/share/eole/creole/distrib/topics.conf`.

6.2. Résoudre des dysfonctionnements liés aux listes de diffusion

Indications utiles au débogage du gestionnaire de listes Sympa :

- les messages d'erreur se trouvent dans le fichier journal : `/var/log/rsyslog/local/exim/exim.info.log` ;
- le gestionnaire de listes Sympa journalise également des informations dans `/var/log/syslog` ;
- les droits sur `/var/lib/sympa` doivent être `sympa:sympa` ;
- vérifier la présence du sticky bit (-rwsr-sr-x 1 sympa sympa) sur le fichier `/usr/lib/cgi-bin/sympa/wwsympa.fcgi` :

```
# ll /usr/lib/cgi-bin/sympa/wwsympa.fcgi
-rwsr-sr-x 1 sympa sympa 611477 avril 10 2014 /usr/lib/cgi-bin/sympa/wwsympa.fcgi*
```

- vérifier que la liste est bien référencée dans `/etc/mail/sympa.aliases` ;
- vérifier que toutes les composantes de l'application sont en service :

```
root@serv-pedago:~# ps -edf | grep sympa
root 21675 21649 0 13:56 pts/0 00:00:00 grep --color sympa
sympa 27000 1 0 07:00 ? 00:00:04 /usr/bin/perl /usr/lib/sympa/bin/sympa.pl
sympa 11183 1 0 07:00 ? 00:01:00 /usr/bin/perl /usr/lib/sympa/bin/bulk.pl
sympa 27003 1 0 07:00 ? 00:00:00 /usr/bin/perl /usr/lib/sympa/bin/archived.pl
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
sympa    27006    1    0    07:00    ?    00:02:31    /usr/bin/perl
/usr/lib/sympa/bin/task_manager.pl
sympa    27011    1    0    07:00    ?    00:00:00    /usr/bin/perl
/usr/lib/sympa/bin/bounced.pl
```

Sur le module AmonEcole, les fichiers et processus mentionnés ci-dessus, autres que les journaux systèmes, se trouvent dans le conteneur `bdd`.

Pour se connecter au conteneur `bdd` utiliser la commande :

```
# ssh bdd
```

7. Architecture messagerie académique

Pour fonctionner pleinement, le système de messagerie proposé sur les modules EOLE a besoin d'adaptations au niveau des serveurs académiques.

Il faut :

- un DNS[p.887] configuré avec les noms de domaines des établissements ;
- un relai SMTP[p.899].

Le relai académique doit être capable de distribuer les adresses Internet (`etab.ac-acad.fr`) et les adresses restreintes (`i-etab.ac-acad.fr`).

Si vous n'avez pas de relai académique, votre domaine restreint sera limité à l'établissement et non à l'Académie.

Le DNS

Au niveau du DNS académique, il faut écrire les MX de chacun des domaines Internet des établissements, en les faisant pointer vers le relai académique.

Le relai SMTP

Au niveau des modules Scribe, le relai de messagerie étant le relai académique, tous les courriers électroniques du domaine Internet ou restreint d'autres établissements arriveront sur le relai.

La distribution des courriers électroniques se fait ensuite grâce au routage SMTP (table de routage Postfix ou Exim).

En fonction de vos architectures, vous pouvez remonter sur le module Scribe, soit via votre réseau de concentration, soit via un réseau VPN (Amon-Sphynx), soit via Internet en mettant en place du SNAT sur le pare-feu établissement.

Nous recommandons de positionner le module Scribe sur une DMZ de l'établissement.

Il est recommandé d'utiliser une passerelle dédiée pour faire du routage SMTP avec anti-virus et anti-spam.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Comme toujours en architecture réseau il n'y pas de solution unique !



Le module Seshat permet de mettre en place simplement un relai académique.

8. 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.900] 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.892] 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
```

9. Présentation des répertoires partagés du module Scribe

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.901] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

9.1. Partages sous Windows

Sous Windows, chaque utilisateur peut accéder :

- à son répertoire personnel ;
- au partage `commun`.

Spécifiquement, un élève dispose :

- d'un dossier `groupes` contenant les partages de la classe, des groupes et des options dont il est membre ;

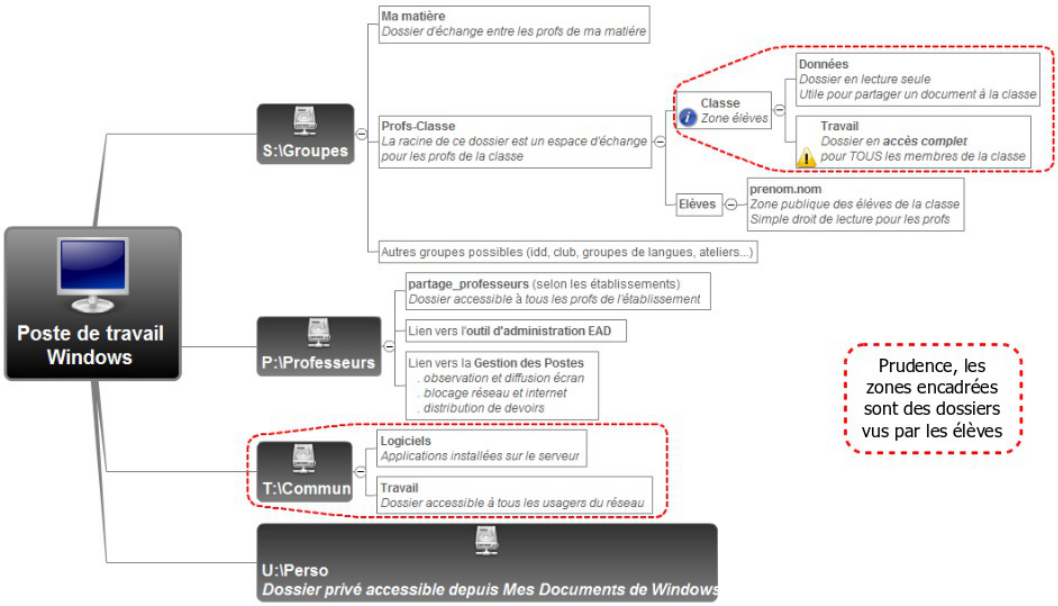
Spécifiquement, un enseignant dispose :

- d'un dossier `groupes` contenant les partages des groupes, des équipes pédagogiques et des matières dont il est membre ;
- du partage `professeurs` dans lequel se trouve l'outil `Gestion-postes` (Observation, diffusion, blocage réseau et distribution de devoirs).

Spécifiquement, un personnel administratif dispose :

- d'un dossier `groupes` contenant les partages des groupes et des services dont il est membre.

Voici un schéma tiré d'un support de formation rédigé par le DRT de l'académie de Lyon mis à disposition selon les termes de la licence CC Attribution-Noncommercial-Share Alike 3.0 Unported. Celui-ci montre les répertoires partagés du point de vue de l'enseignant.

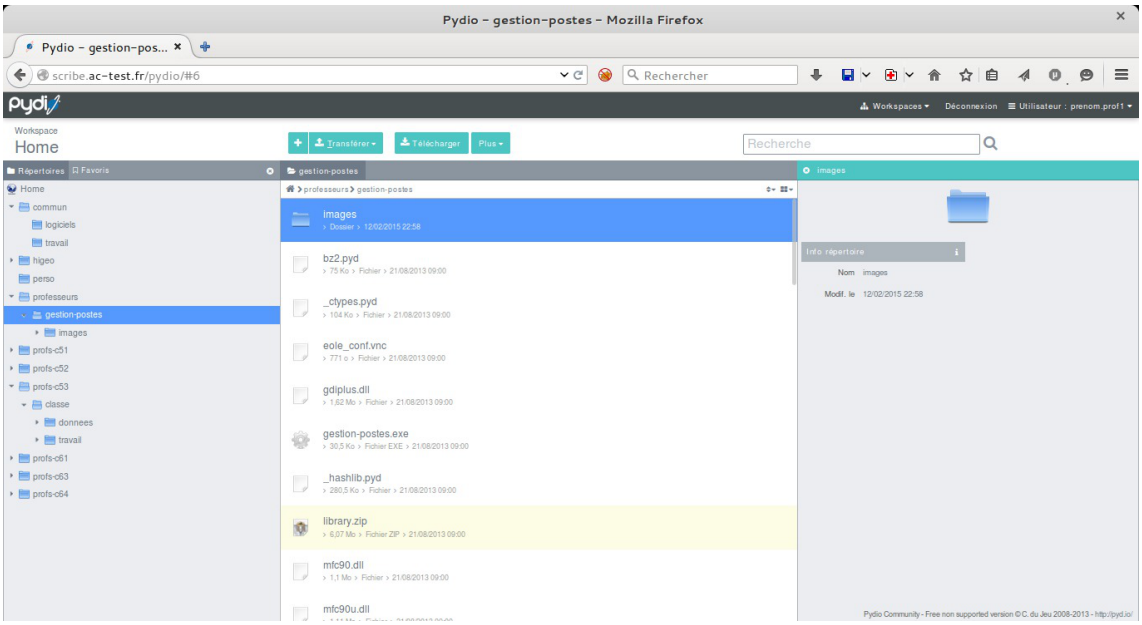


DRT Lyon – Site internet : *http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/*

9.2. Partages dans Pydio

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Pydio, anciennement Ajaxplorer, est un gestionnaire de fichiers en ligne.

Ce gestionnaire permet de naviguer dans l'arborescence des fichiers utilisateurs. Il permet également l'édition de fichiers, l'écoute de fichiers audio, l'affichage d'images, ...

http://pyd.io/

Répertoires

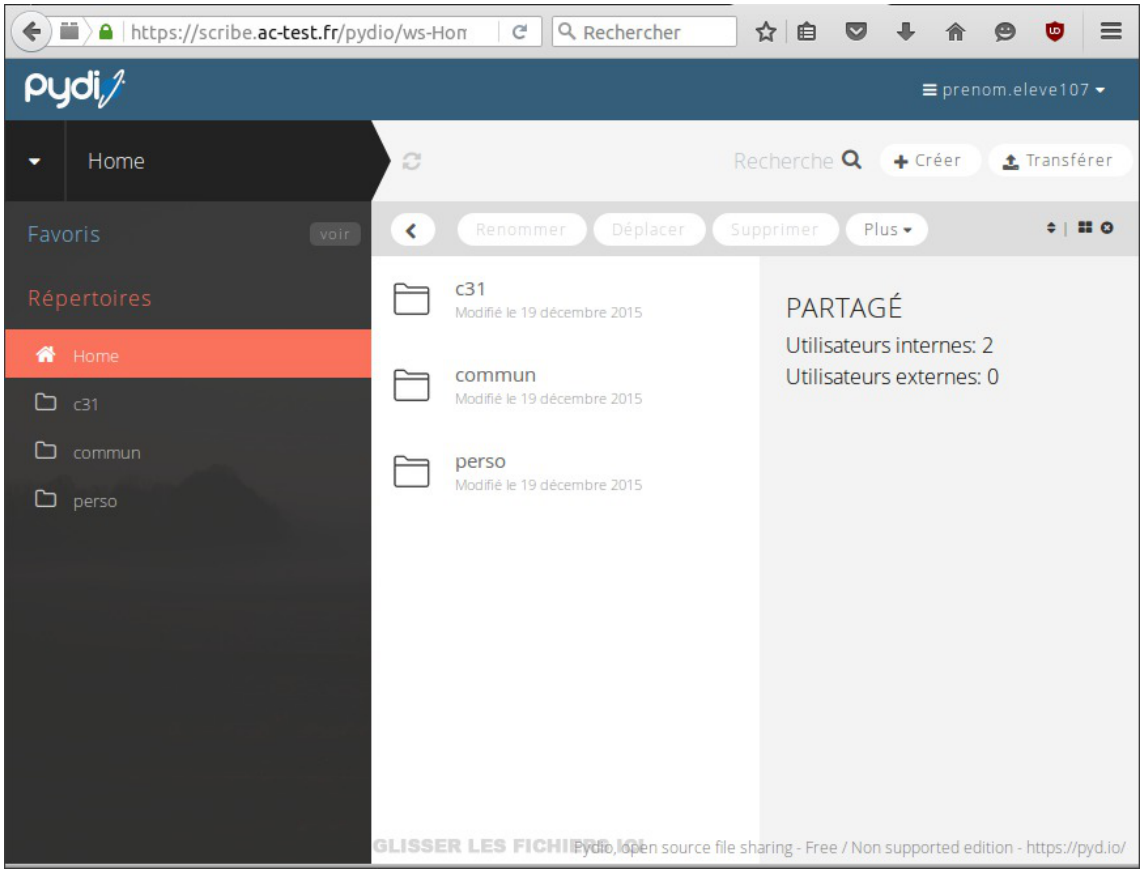
Par l'intermédiaire de Pydio, chaque utilisateur peut accéder :

- à son répertoire personnel ;
- au partage `commun`.

Spécifiquement, un élève dispose :

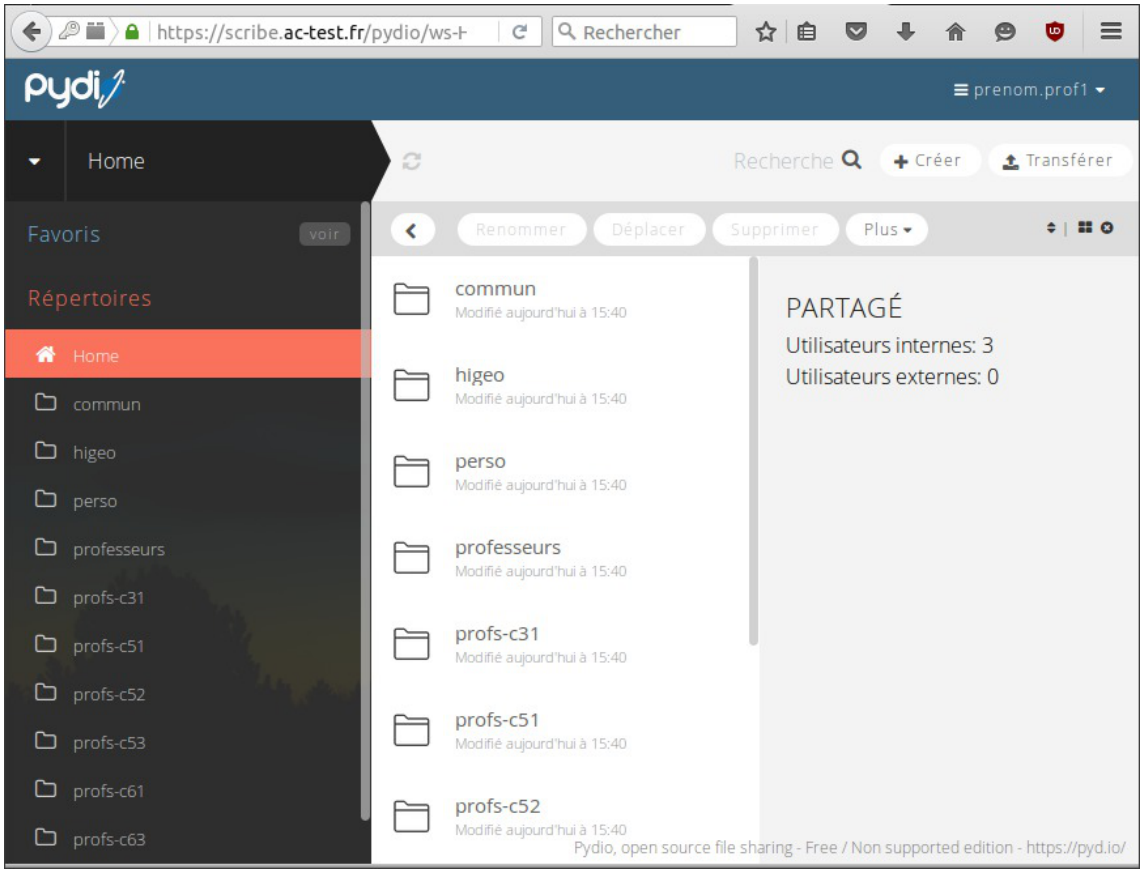
- des partages de la classe, des groupes et des options dont il est membre.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Spécifiquement, un enseignant dispose :

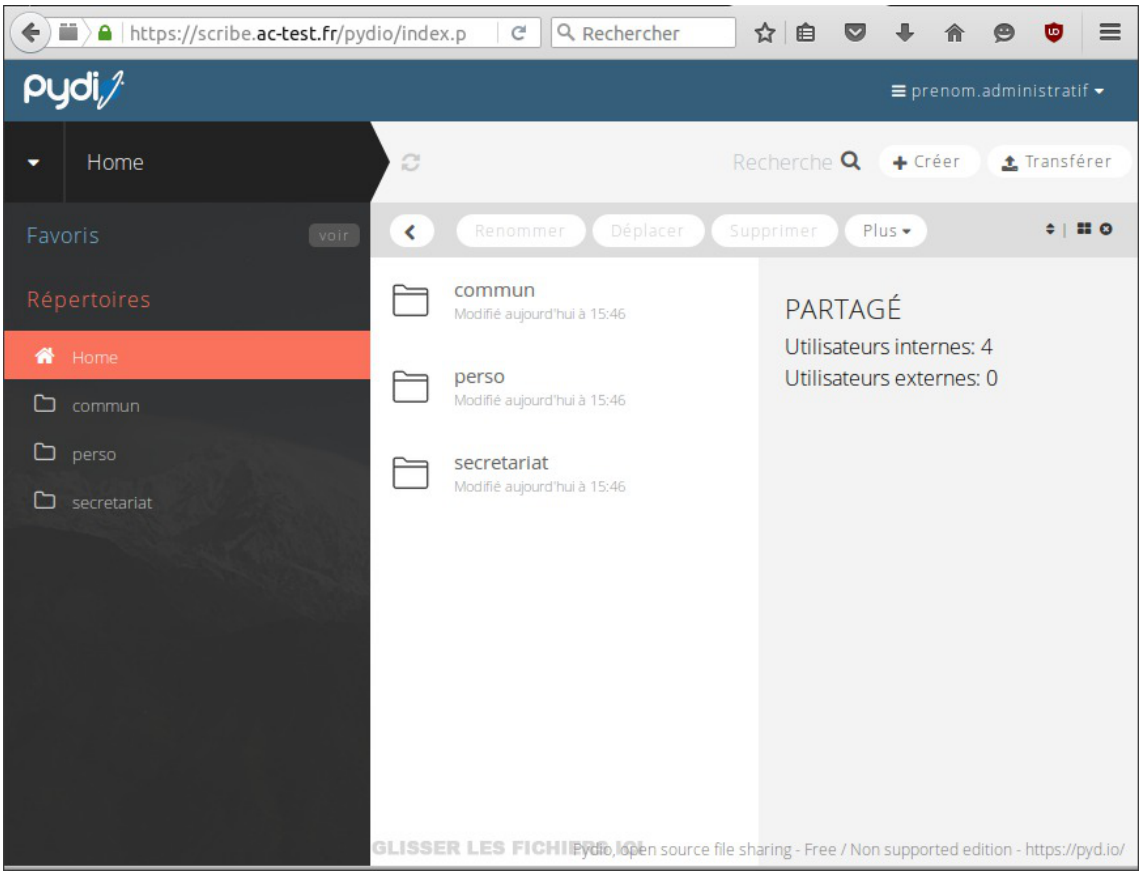
- des partages des groupes, des équipes pédagogiques et des matières dont il est membre ;
- du partage `professeurs`.



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Spécifiquement, un personnel administratif dispose :

- des partages des groupes et des services dont il est membre.



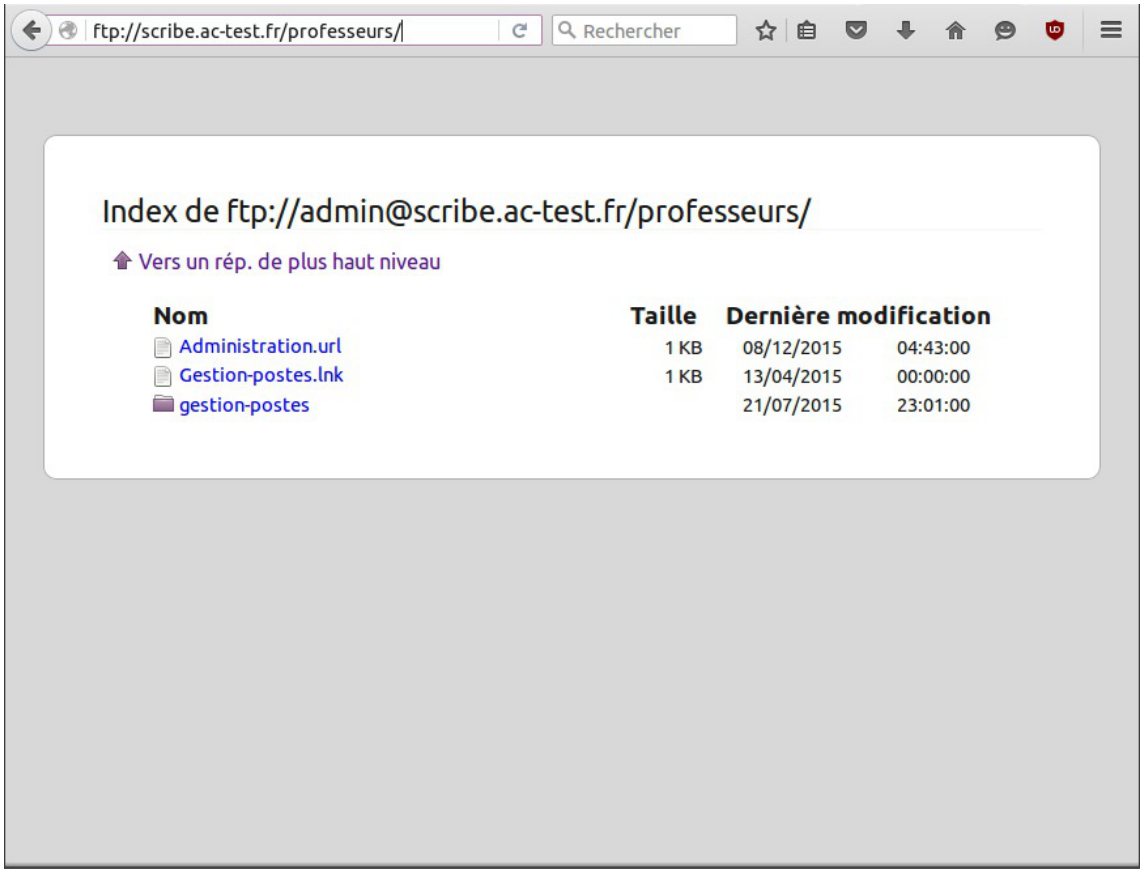
Voir aussi...

> Pydio : gestionnaire de fichiers

9.3. Partages dans le navigateur web

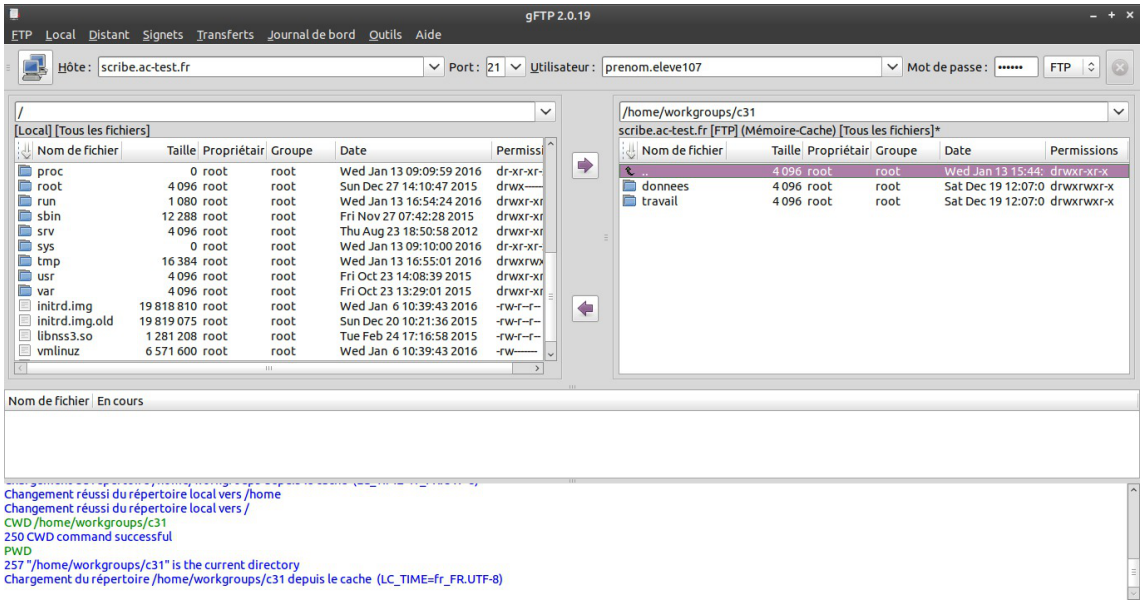
Les partages accessibles par le navigateur web sont les partages standards de l'utilisateur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



9.4. Partages via un client FTP

Les partages accessibles via un client FTP sont les partages standards de l'utilisateur.



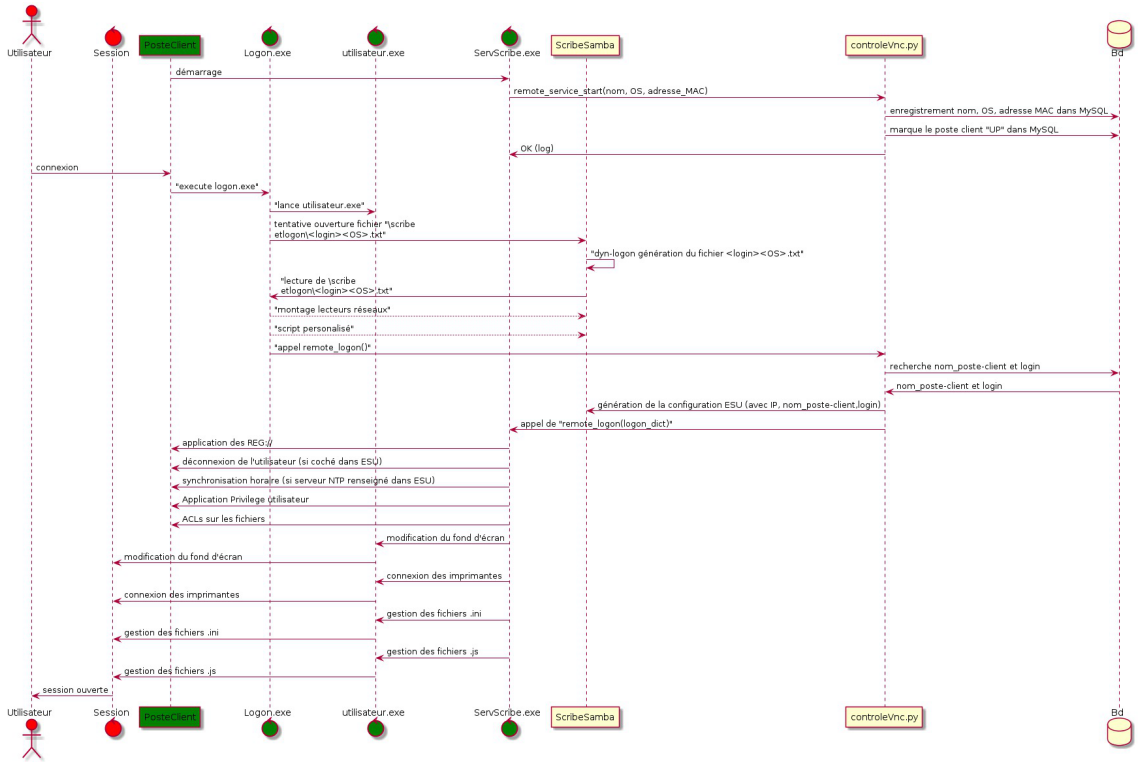
Le client gFTP affiche directement le répertoire `/home/workgroups/`, tous les répertoires partagés sont affichés mais l'utilisateur ne peut explorer les fichiers si n'en a pas le droit.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Les liens symboliques du répertoire `/home/x/utilisateur/.ftp/` sur le module en version 2.4.x ne sont pas vus comme des fichiers par le logiciel Filezilla.

Il faut saisir le chemin complet pour que cela fonctionne `/home/x/utilisateur/.ftp/nomDelaClasse`.

10. Schéma de fonctionnement du client Scribe



Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Chapitre 9

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.



1. Questions fréquentes communes aux modules

Accéder aux partitions du module depuis un Live Linux

Lorsqu'on a recours à un live CD ou USB, il n'est pas possible d'accéder directement aux partitions.

```
# mkdir /media/partition
# mount /dev/sda2 /media/partition
mount: type inconnu de système de fichiers 'LVM2_member'
```

Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
# vgscan
Reading all physical volumes. This may take a while...
Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
# vgchange -a y eolebase-vg
4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
# ll /dev/mapper/
total 0
drwxr-xr-x  2 root root     160 févr.  8 11:53 ./
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
drwxr-xr-x 19 root root    4460 févr.  8 11:53 ../
crw-------  1 root root 10, 236 févr.  8 11:53 control
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-home ->
../dm-4
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-root ->
../dm-0
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-swap_1 ->
../dm-1
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-var -> ../dm-3
```

ou

```
# lvdisplay
  --- Logical volume ---
  LV Path                /dev/eolebase-vg/swap_1
  LV Name                swap_1
  VG Name                eolebase-vg
  LV UUID                OO47WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
  LV Write Access        read/write
  LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
  LV Status              available
  # open                 2
  LV Size                1,09 GiB
  Current LE             280
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:1
[...]
```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

Ajouter de l'espace disque à un volume LVM

Sur le nouveau périphérique physique, créer une partition de type Linux LVM (8E), avec `cfdisk` par exemple.

La nouvelle partition s'appelle par exemple `/dev/sdb1` et peut être ajoutée au volume, par exemple pour agrandir `/var`.



Après avoir créé la nouvelle partition `/dev/sdb1` il peut être nécessaire de redémarrer le serveur pour la faire prendre en compte par le système.

Démonter la partition

Pour démonter la partition

```
# umount /var
```

Créer un volume physique

Créer un volume physique avec la nouvelle partition :

```
# pvcreate /dev/sdb1
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Quel est le groupe de volumes

Rechercher dans quel groupe de volumes (VG Name) se trouve le volume logique `/var` :

```
root@scribe:/dev/mapper# lvdisplay /dev/scribe-vg/var
  --- Logical volume ---
  LV Path                /dev/scribe-vg/var
  LV Name                var
  VG Name                scribe-vg
  LV UUID                N4dHMU-htpz-AhEI-x5Ld-EvpM-ZFJX-M3LbHD
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-01-16 19:17:09 +0100
  LV Status              available
  # open                 1
  LV Size                8,35 GiB
  Current LE             2138
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:3

root@scribe:/dev/mapper#
```

Ajouter ce volume physique au groupe de volumes contenant le volume logique `/var`, ici `scribe-vg` :

```
# vgextend scribe-vg /dev/sdb1
```

Agrandir le volume logique

Agrandir le volume logique correspondant à `/var` avec le nouvel espace libre :

```
# lvextend -l +100%FREE /dev/scribe-vg/var
# e2fsck -f /dev/scribe-vg/var
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM



Sur un serveur où une partition est saturée.

```
root@scribe:~# df -h
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
udev                          1,5G       0  1,5G   0% /dev
tmpfs                         301M     52M  250M  18% /run
/dev/mapper/scribe--vg-root   9,1G    2,6G  6,0G  30% /
tmpfs                         1,5G     28K  1,5G   1% /dev/shm
tmpfs                         5,0M       0  5,0M   0% /run/lock
tmpfs                         1,5G       0  1,5G   0% /sys/fs/cgroup
/dev/sda1                     687M    107M  531M  17% /boot
/dev/mapper/scribe--vg-tmp    1,8G    3,4M  1,7G   1% /tmp
/dev/mapper/scribe--vg-var    8,1G      8G  0,1G  99% /var
/dev/mapper/scribe--vg-home    18G    149M   18G   1% /home
tmpfs                         301M       0  301M   0% /run/user/0
root@scribe:~#
```

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.

Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Pour démonter le périphérique :

```
root@scribe:~# umount /home
```

Si le périphérique est occupé, la commande `lsof` renvoie les programmes utilisant la partition :

```
# lsof | grep home
```

Il faut alors arrêter les services concernés puis démonter la partition.

Vérifier le support

Pour vérifier le support, lancer la commande :

```
# fsck -f /dev/mapper/scribe--vg-home
```

Diminuer la taille de la première partition

Réduire le système de fichiers :

```
# resize2fs -p /dev/scribe-vg/home 1G
```

Réduire la partition logique :

```
# lvresize -L-1G /dev/scribe-vg/home
```

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/home
```

Vérifier l'espace libéré

Pour vérifier que l'espace a bien été libéré il faut utiliser la commande `vgdisplay` :

```
# vgdisplay
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  6
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       10060 / 39,30 GiB
  Free  PE / Size       0 / 0
  VG UUID               hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3

root@scribe:~#
```

La ligne `Free PE / Size` affiche l'espace libre.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Agrandir la taille de la deuxième partition

Les agrandissements peuvent se faire à chaud, ce qui est recommandé si la partition contient les commandes.

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/var
```

Agrandir la partition logique :

```
# lvresize -L+1G /dev/scribe-vg/var
```

Étendre le système de fichiers (sans option le système de fichiers prend toute la place possible) :

```
# resize2fs  /dev/scribe-vg/var
```

Remonter le périphérique

Procéder au montage du périphérique avec la commande `mount` :

```
# mount /var/home
```



Pensez à redémarrer les services qui ont précédemment été arrêtés.

CAS Authentication failed !

Le message ***`CAS Authentication failed ! You were not authenticated.`*** *(ou* ***`Authentification CAS infructueuse ! Vous n'avez pas été authentifié(e).`*** *)* peut apparaître si des modifications ont été faites dans l'interface de configuration.



Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

```
# reconfigure
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Vous avez ajouté un nom DNS alternatif ou une adresse IP alternative sur le serveur

Il faut ajouter le nom alternatif ou l'adresse IP alternative dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet `Certifs-ssl` en mode expert il faut remplir les champs `Nom DNS alternatif du serveur` et/ou l'adresse `IP alternative du serveur`.

Le bouton `+` permet d'ajouter autant d'alternatives que vous voulez. Il faut ensuite `Valider le groupe` et enregistrer la configuration.

L'opération doit être suivie de la reconfiguration du module, cela va régénérer le certificat `/etc/ssl/certs/eole.crt`

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

`# /usr/share/creole/gen_certif.py -f` ou `# /usr/share/creole/gen_certif.py -f nom_du_certificat` pour la régénération d'un certificat en particulier.

```
# reconfigure
```

Attention, les adresses suivantes ne sont pas définies comme sujet du certificat...

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

à jour).

`# reconfigure`

`# /usr/share/creole/gen certif.py -f` ou `# /usr/share/creole/gen certif.py -f nom du certificat` pour la régénération d'un certificat en particulier.

`# reconfigure`

Une erreur se produit lors de l'instanciation ou d'un reconfigure : "starting firewall : [...] Erreur à la génération des règles eole-firewall !! non appliquées !"

Le message suivant apparaît à l'instance ou au reconfigure après changement de valeurs dans l'interface de configuration du module :

`* starting firewall : bastion (modèle XXX) Erreur à la génération des règles eole-firewall !!`

`non appliquées !`

Vérifier la configuration des autorisations d'accès à SSH et à l'EAD sur les interfaces réseau

Cette erreur provient certainement du masque des variables d'autorisation d'accès à SSH sur l'une des interfaces réseau.

Pour autoriser une seule IP, par exemple `192.168.1.10`, le masque doit être `255.255.255.255` pour autoriser une IP particulière et non 255.255.255.0

Vérifier l'ensemble des autorisations pour l'accès SSH et pour l'accès à l'EAD.

Pour appliquer les changements il faut reconfigurer le module :

`# reconfigure`

La connexion SSH renvoie Permission denied (publickey)

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant : `Permission denied (publickey).`

Gestion des mises à jour

Pour connaître la date et l'heure des mises à jour du système il est possible de passer par l'EAD ou par un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

```
python -c "from creole import maj; print maj.get_maj_day()"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

Activation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly add
```

ou :

```
python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly del
```

ou :

```
python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

Le mot de passe par défaut ne fonctionne pas

Suite à une nouvelle installation le mot de passe par défaut ne fonctionne pas.

Le mot de passe à saisir comprend les dollars devant et derrière : `$eole&123456$`

Échec de la connexion sécurisée

Le navigateur affiche :

```
Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à IP:Port.

Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :

Votre certificat contient le même numéro de série qu'un autre certificat émis par l'autorité de certification. Veuillez vous procurer un nouveau certificat avec un numéro de série unique.

(Code d'erreur : sec error reused issuer and serial)
```

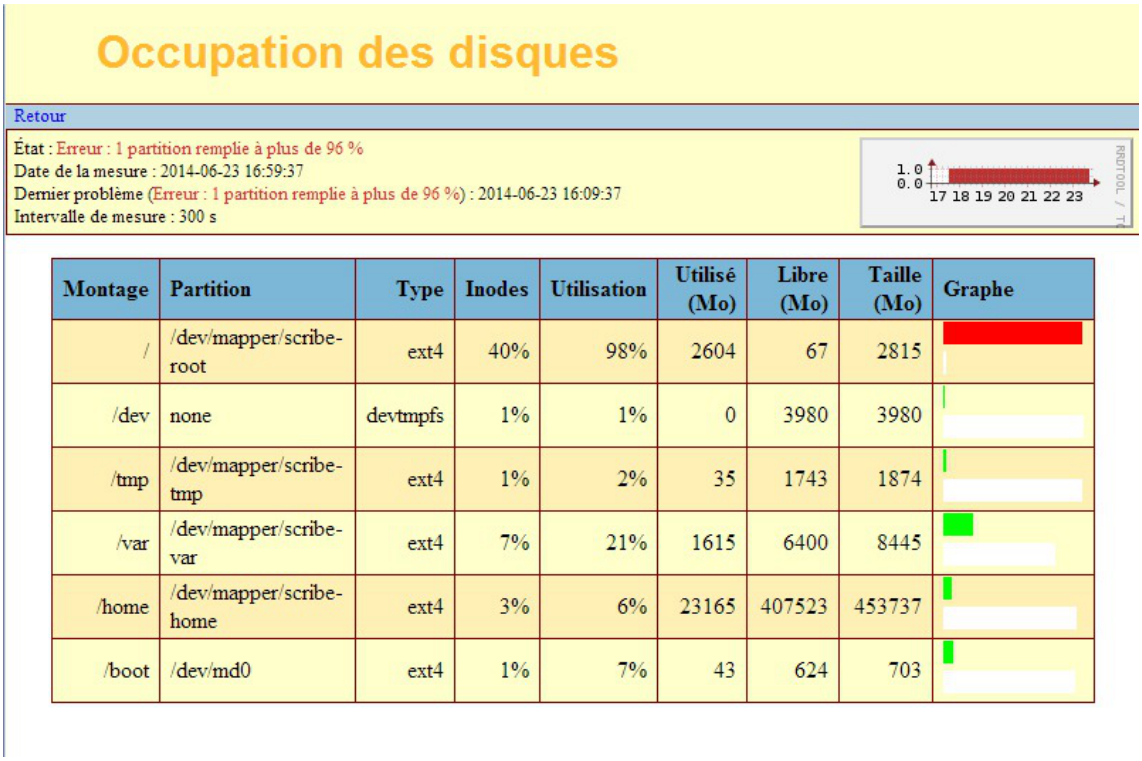
Les paramètres constituant un certificat ont été modifiés récemment

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une régénération des certificats a eu lieu.

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

Partition saturée

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

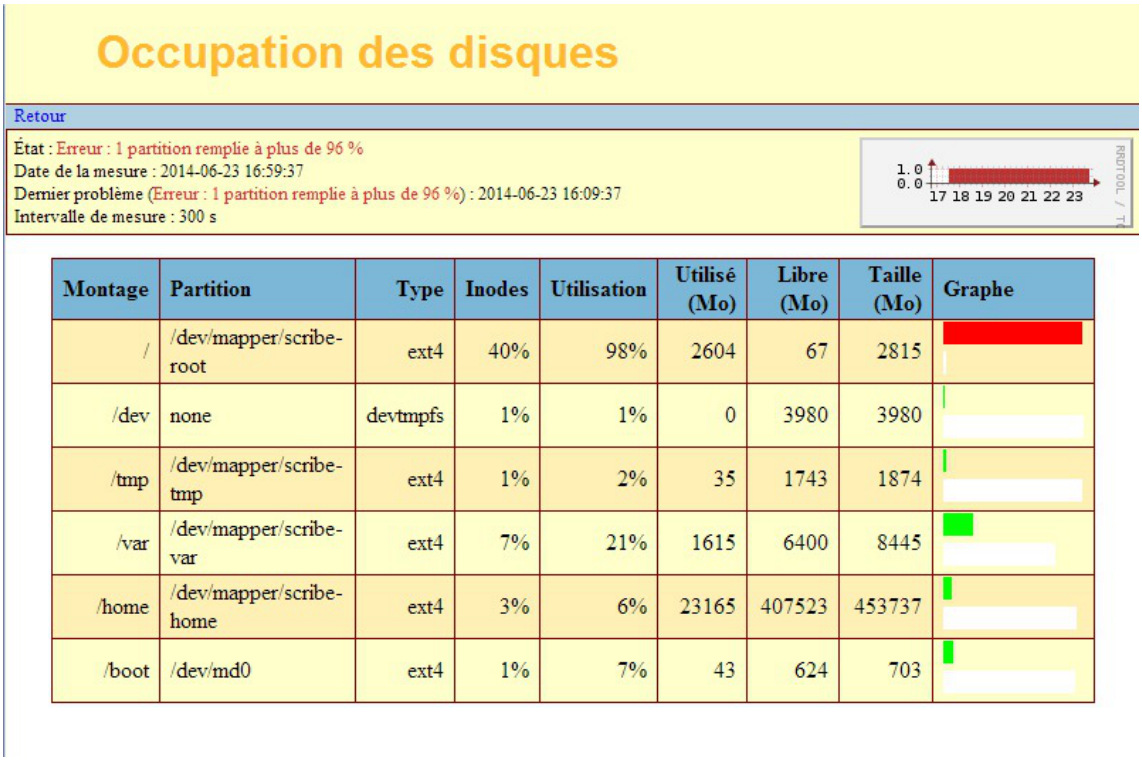
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- le manque de place disponible ;
- le manque d'inodes disponibles.

La cause de la saturation apparaît dans la page Occupation des disques, soit les inodes soit l'utilisation sont à un pourcentage élevé. La résolution du problème est différente selon le cas.

Partition / saturée



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

1.0
0.0
17 18 19 20 21 22 23
RRDTOOL / T

Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Si la partition racine est saturée sans raison apparente et que le taux d'inodes est correct, le montage d'un répertoire avant copie a peut être échoué. La conséquence est que la copie c'est faite sur la partition racine et non sur le montage. Cela peut être le cas, par exemple, de la sauvegarde.



Il faut donc vérifier le contenu et la place occupée par les répertoires (points de montage) `/mnt`, `/mnt/sauvegardes` et `/media` :

Si le répertoire `/mnt/sauvegardes` n'est pas monté il doit être vide :

```
root@scribe:/mnt/sauvegardes# ls -la
total 8 drwxr-xr-x 2 root root 4096 mai 25 11:29 ./ drwxr-xr-x 26 root root 4096 sept. 9 21:07 ../
root@scribe:/mnt/sauvegardes#
```

Normalement le répertoire `/media` ne contient que des sous-dossiers pour le montage des partitions et ou des périphériques.

Pour vérifier l'espace occupé par ces différents répertoires :

```
root@scribe:/# du -h --max-depth=1 /media /mnt/
4,0K /media 4,0K /mnt/
```



Dans certains cas particuliers, la taille allouée à la partition `/` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM[p. 892]).

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. 892]).

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.

Liste d'arguments trop longue

La commande `# rm -rf /var/<rep>/*` renvoie `Liste d'arguments trop longue`.



Préférez l'utilisation d'une autre commande :

```
# find /var/<rep>/* -type f -name "*" -print0 | xargs -0 rm
```

Le démarrage reste figé à l'étape de vérification des disques

Le serveur est virtualisé avec une solution basée sur l'émulateur qemu.



Seul l'affichage est figé, la machine démarre en fait normalement et est certainement accessible par SSH. Cela vient du support de la carte graphique. Il faut forcer la carte graphique à utiliser une autre carte graphique que celle par défaut (cirrus).

Sous Proxmox, indiquez carte `VGA standard` à la place de `par défaut`.

Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.



Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :

1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet `Eoleflask`.
2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.

Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

```
https://<adresse_serveur>:7000/genconfig/
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.



Un fichier `config.eole.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.

S'il existe une différence entre `config.eol` et `config.eole.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Impossible de trouver la base des matériels maintenue par EOLE

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Changer le disque dur du serveur

Il est possible entre autre de faire une image avec le logiciel Clonezilla.



L'UUID[p.904] ayant naturellement changé il faut démarrer en utilisant un LiveCD et éditer l'UUID dans `/etc/fstab` du serveur.

Sources supplémentaires pour apt

Il est possible d'ajouter des sources supplémentaires pour le logiciel apt.



Pour que la solution soit pérenne il faut ajouter dans le répertoire `/etc/apt/sources.list.d/` la description de la nouvelle source dans un fichier portant l'extension `.list`



Par exemple pour avoir à disposition `SCENARIserveur` sur un module EOLE il faut ajouter le fichier `scenari.list` dans le répertoire `/etc/apt/sources.list.d/` avec le contenu suivante :

```
#scenari ppa
deb https://download.scenari.org/deb precise main
```

Il faut ensuite mettre la liste des paquets disponibles à jour avec la commande `apt-get update`.

Dysfonctionnement des agents suite à un changement d'architecture

En allant sur la page des statistiques de surveillance d'un serveur (EAD ou Application Zéphir), j'obtiens

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

un message du type `rrdtool.error: This RRD was created on another architecture`

Ce problème peut survenir en cas de réinstallation des données d'un serveur 32 bits sur un serveur 64 bits (ou inversement).



Une solution consiste à supprimer les fichiers de statistiques :

- Statistiques propres au serveur Zéphir

  Concerne les statistiques de Zéphir lui-même, pour les statistiques des serveurs clients, l'erreur doit être corrigée sur le client (voir cas suivant).

  ```
  # service zephir stop
  # rm -rf /var/lib/zephir/data/0/*
  # service zephir start
  ```

- Sur un module EOLE autre que Zéphir

  ```
  # service z_stats stop
  # rm -rf /usr/share/zephir/monitor/data/*
  # rm -rf /usr/share/zephir/monitor/stats/*
  # service z_stats start
  ```



Si perdre les statistiques pose problème, il est possible de convertir les fichiers `.rrd` avec l'outil rrdtool.

Depuis l'ancien serveur, pour convertir les fichiers RRD vers des fichiers XML avec la commande `dump` :

```
# rrdtool dump stats.rrd > stats.xml
```

Après les avoir transférés sur le nouveau serveur il faut les convertir en RRD avec la commande `restore` :

```
# rrdtool restore -f stats.xml stats.rrd
```

Le serveur peut maintenant lire le fichier. Vous pouvez le tester avec la commande `info` :

```
# rrdtool info stats.rrd
```

Attention, il y a un (ou plusieurs) fichier par agent.

Exemple sur un serveur Zéphir :

```
root@zephir:~# ls -l /var/lib/zephir/data/0/*/*.rrd -rw-r--r-- 1 root root 11464 août 31 14:51 /var/lib/zephir/data/0/bastion/status.rrd -rw-r--r-- 1 root root 17032 août 31 15:27 /var/lib/zephir/data/0/bilan/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/debsums/status.rrd -rw-r--r-- 1 root root 1000 août 31 14:51 /var/lib/zephir/data/0/diag/status.rrd -rw-r--r-- 1 root root 13576 août 31 15:26 /var/lib/zephir/data/0/diskspace/status.rrd
[…]
```

Si vous voulez convertir un répertoire entier en XML, utilisez ce petit script bash :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# for f in *.rrd; do rrdtool dump ${f} > ${f}.xml; done
```

Source : http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite

Comment débloquer les message en file d'attente ?

Un nombre de messages apparaissent comme étant *Frozen* dans le retour de la commande `diagnose`.

```
*** Messagerie
. Courrier SMTP => Ok
. File d'attente => 1 message(s)
. Messages "Frozen" => 1 message(s)
```

Une solution consiste à récupérer les identifiants des messages :

```
root@scribe:~# exim4 -bp
10h 2.5K 1abJaX-00036S-Bu <> *** frozen ***
touser@ac-test.fr
```

Il est ensuite possible de récupérer les journaux spécifiques message par message :

```
root@scribe:~# exim4 -Mvl 1abJaX-00036S-Bu
2016-03-03 04:06:05 Received from <> R=1abJaX-00036L-8j U=Debian-exim P=local S=2525
2016-03-03 04:06:05 SMTP error from remote mail server after RCPT TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
2016-03-03 04:06:05 touser@ac-test.fr R=satellite_route T=remote_smtp: SMTP error from remote mail server after RCPT TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr [192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address rejected: Access denied
*** Frozen (delivery error message)
```

Dans cet exemple, le message d'erreur est `Recipient address rejected: Access denied`, l'expéditeur n'est pas autorisé à transiter par la passerelle configurée dans l'interface de configuration du module.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
root@eole:~# rm /etc/eole/extra/schedule/config.eol
rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

Le proxy empêche les mises à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le blocage de certaines mises à jour aussi, la déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon.

```
root@scribe:~# Maj-Auto
Mise à jour le lundi 20 mars 2017 11:47:52
*** scribe 2.6.1 ***

Maj-Auto - (VERSION CANDIDATE) - Augmenter le niveau de mise à jour peut empêcher de revenir au niveau de mise à jour stable.
Voulez-vous continuer ? [oui/non]
[non] : oui
pyeole.pkg - Pas de configuration du miroir Ubuntu avec eole.ac-dijon.fr qui semble inaccessible : Impossible d'obtenir la version pour le dépôt : http://eole.ac-dijon.fr/ubuntu/dists/xenial/main/binary-amd64/Release
pyeole.pkg - Pas de configuration du miroir Ubuntu avec ftp.crihan.fr qui semble inaccessible : Impossible d'obtenir la version pour le dépôt : http://ftp.crihan.fr/ubuntu/dists/xenial/main/binary-amd64/Release
Maj-Auto - Impossible de configurer les sources APT pour Ubuntu
```

La déclaration du proxy s'effectue dans l'onglet `Général` de l'interface de configuration du module, passer `Utiliser un serveur mandataire (proxy) pour accéder à Internet` à `oui` et paramétrer l'adresse du proxy dans le champ `Nom ou adresse IP du serveur proxy`.

Pour effectuer les mises à jour d'un module qui n'est pas encore instancié, il faut configurer manuellement la variable d'environnement :

```
# export http_proxy=http://<adresseProxy>:<portProxy>
# Maj-Auto
```

Comment lister les services gérés par CreoleService

Il peut être utile de lister les services qui sont gérés par CreoleService.

Une astuce consiste à utiliser la commande `CreoleGet .containers.services|grep \.name=`

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
root@eolebase:~# CreoleGet .containers.services|grep \.name=
service0.name="networking"
service1.name="cron"
service10.name="exim4"
service11.name="eoleflask"
service12.name="nginx"
service13.name="ead3"
service14.name="genconfig"
service15.name="bastion"
service16.name="z_stats"
service2.name="rng-tools"
service3.name="ntp"
service4.name="nut-server"
service5.name="salt-api"
service6.name="salt-master"
service7.name="salt-minion"
service8.name="ead-server"
service9.name="ead-web"
root@eolebase:~#
```

Résoudre des dysfonctionnements liés à l'EAD

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation du fichier journal `/var/log/ead/ead-server.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```
service ead-server stop
cd /tmp
export PYTHONPATH=/usr/share
twistd -noy /usr/share/ead2/backend/eadserver.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

Si c'est le service `ead-web` qui est en erreur et que le fichier journal `/var/log/ead/ead-web.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```
service ead-web stop
cd /tmp
export PYTHONPATH=/usr/share
twistd -noy /usr/share/ead2/frontend/frontend.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

2. Questions fréquentes propres au module Amon

Vider le cache du proxy

Vider le répertoire cache de Squid

Il faut arrêter le service Squid, supprimer les fichiers, re-générer l'arborescence du cache et redémarrer le service.

```
# service squid3 stop
# rm -rf $(CreoleGet cache_dir)/*
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# squid3 -f /etc/squid3/squid.conf -z -N
# service squid3 start
```

Vider le répertoire cache de la seconde instance de Squid

Il faut arrêter le second service Squid, supprimer les fichiers, re-générer l'arborescence du cache et redémarrer le service.

```
# service squid3-2 stop
# rm -rf $(CreoleGet cache_dir_2)/*
# squid3 -f /etc/squid3/squid2.conf -z -N
# service squid3-2 start
```

Problèmes avec le protocole HTTPS

La règle de pare-feu par défaut redirige le trafic Internet directement vers le proxy local.

C'est le mécanisme de proxy transparent.

Cette méthode ne permet toutefois pas de laisser passer le flux chiffré (HTTPS) par ce même mécanisme.

Pour accéder aux sites en HTTPS, il est nécessaire de configurer le proxy sur les postes clients (par exemple : avec ESU sur le module Scribe).

L'option `Destinations non redirigées sur le proxy` disponible en mode expert dans l'onglet `Interface-1` permet, à l'inverse, de déclarer des exceptions.

Lenteur lors de la navigation web

Un filtrage web e2guardian est en place et la navigation web est très lente.

Dans les logs apparaissent des erreurs Squid à répétition (`TCP_DENIED/407`) :

```
Mar  01  10:36:01  amon  (squid):  1363253761.503  51  192.168.10.10 TCP_DENIED/407 4006 GET http://linuxfr.org/ - NONE/- text/html
```

Augmenter le nombre de processus e2guardian maximum dans le filtre

Avant d'augmenter le nombre de processus, on peut vérifier la valeur configurée dans l'interface de configuration du module. Celle-ci est fixée à `256` par défaut et se trouve dans l'onglet `Filtrage web` en mode expert.

Une commande rudimentaire permet de se rendre compte du nombre de processus effectivement exécutés sur le serveur mais elle ne permet pas de distinguer à quelle instance appartiennent les processus et renvoie aussi les processus qui servent a contrôler les autres processus :

```
# ps ax | grep -c guardian
```

La commande `diagnose` permet de connaître précisément le nombre de processus e2guardian exécutés par instance :

```
*** Filtre web
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
admin: test-eole.ac-dijon.fr => Ok
pedago: test-eole.ac-dijon.fr => Ok
dmz-priv: test-eole.ac-dijon.fr => Ok
. Nb instances 1 => 15/256
```

Si la commande renvoie un nombre trop proche voir supérieur à la valeur configurée dans l'interface de configuration du module, elle doit être augmentée. La valeur maximum est `8192`.



Il est fortement recommandé de ne pas dépasser la valeur maximum de 8192 processus.

3. Questions fréquentes propres au module Scribe

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`.



```
# 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. 904] 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`.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

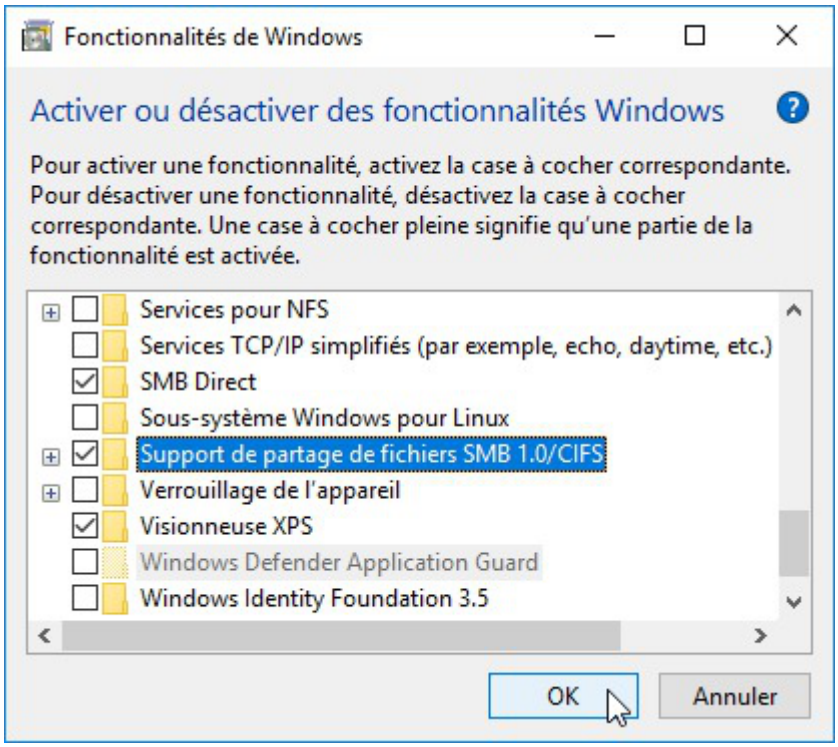
Session Windows, erreur : Une tentative d'ouverture de session a eu lieu...

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.



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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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
```

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]*
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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/
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*
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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/
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
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

`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' ~root/full-ldap-old.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 :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
# 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
```

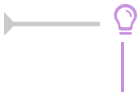


Vérifier le bon fonctionnement du service avec la commande `diagnose`.

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 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` :

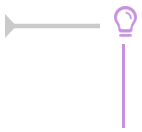
Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

```
d      n      :
cn=edu,ou=local,ou=groupes,ou=0000000A,ou=ac-test,ou=education,o=gouv,c=fr
```

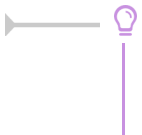
L'UAI est configuré dans l'interface de configuration du module dans l'onglet `Général`.

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.



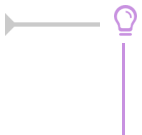
Extraire l'annuaire après arrêt du service :

Arrêt du service

```
# service slapd stop
```

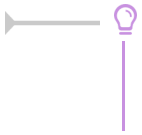
Extraction vers `~root/full-ldap-old.ldif` :

```
# 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
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.

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
  ```

- 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 Password=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
  ```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- 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 Password=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`
- 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.

Délai expiré avec un client FTP graphique

L'accès FTP se fait bien avec l'application web Pydio et en console mais impossible de se connecter avec un client graphique comme Filezilla ou gFTP. Un message de délai expiré apparaît :
`Connexion terminée par expiration du délai d'attente`

Passer le client FTP en mode actif

Les clients FTP sont par défaut configurés en mode passif. Les passer en mode actif résout le problème.

Importation : le caractère "c" s'est ajouté devant le nom d'une classe

Lors d'une importation, le caractère un "c" s'est ajouté devant le nom de la classe.

Les causes d'un renommage sont généralement les suivantes :

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

- le nom du groupe est totalement numérique (ex : `301` pour 3eme1) ;
- il existe une homonymie au niveau des groupes (ex : niveau et classe dénommés `6g`).

4. Questions fréquentes propres à la sauvegarde

La sauvegarde programmée est en échec

Relancer les services

Il faut en premier lieu enlever le verrou :

```
# baculaconfig.py --unlock
```

Si tout n'est pas passé au vert dans l'EAD, il faut relancer les services :

```
# service bacula-director stop
# service bacula-sd stop
# service bacula-fd stop
# service bacula-director start
# service bacula-sd start
# service bacula-fd start
```

Modification de la configuration de Bacula 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 Bacula.

Ré-initialisation de la base Bacula

```
# bacularegen.sh
Le catalogue Bacula a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non]
[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 Bacula.

Ré-initialisation de la base Bacula

```
# bacularegen.sh
Le catalogue Bacula 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)

Supprimer le verrou de sauvegarde

Il faut utiliser la commande suivante :

```
# baculaconfig.py --unlock
```

Paramètres de la commande baculaconfig.py

Pour afficher la liste des paramètres de la commande `baculaconfig.py` :

```
# baculaconfig.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`.

```
# baculamount.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 *bacula* et le groupe *tape* propriétaires du point de montage

```
# baculamount.py -t -o
Test OK
```

Monter le support

```
# baculamount.py --mount
Montage OK
```

Démontage du support

```
# baculamount.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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

> 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 Bacula : `bconsole`.

Voici un aperçu des manipulations à réaliser :

```
# bconsole
(pour lancer la console de bacula)
*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 `baculamount.py`.

```
# baculamount.py -t
Test de montage OK
```

```
# baculamount.py -t
Echec du test de montage :
point de montage : OK
montage : OK
permissions : Erreur
```

Options de montage du support de sauvegarde

Le fichier `/etc/eole/bacula.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/bacula.conf` a une syntaxe du type fichier INI[p.891] : clé = valeur.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



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 smbfs -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 smbfs -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 :

  - `/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 `baculamount.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 -tsmbfs //<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/bacula.conf` et mettre le contenu suivant :

```
DISTANT_LOGIN_MOUNT='/bin/mount -t smbfs -o username={0},password={1},ip={2},uid={3},noexec,nosuid,nodev,sec=nt
//{4}/{5} {6}'
```


Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

5. Questions fréquentes propres à Envole

Boucle infinie de redirection dans le navigateur

Vous essayez de vous connecter à une application web fraîchement installée et le navigateur affiche "Firefox a détecté que le serveur redirige la demande pour cette adresse d'une manière qui n'aboutira pas".

Tester avec une autre application

Afin de s'assurer que le problème n'est pas généralisé, il est conseillé de tester l'accès HTTP à une autre application web.

Reconfiguration du module

Si seule cette application provoque une redirection infinie c'est que le module n'a probablement pas été reconfiguré après l'installation de la nouvelle application web :

```
# reconfigure
```

Le portail affiche un message d'indisponibilité

Le portail affiche le message "Votre portail est momentanément indisponible, veuillez contacter votre administrateur" et pourtant aucune reconfiguration n'est en cours.

Lancer un diagnose et un reconfigure

Relancer la reconfiguration du module peut solutionner le problème d'accès :

```
# reconfigure
```

Un diagnose peut aussi vous en dire plus :

```
# diagnose
```

Le script de reconfiguration a peut être rencontré un problème

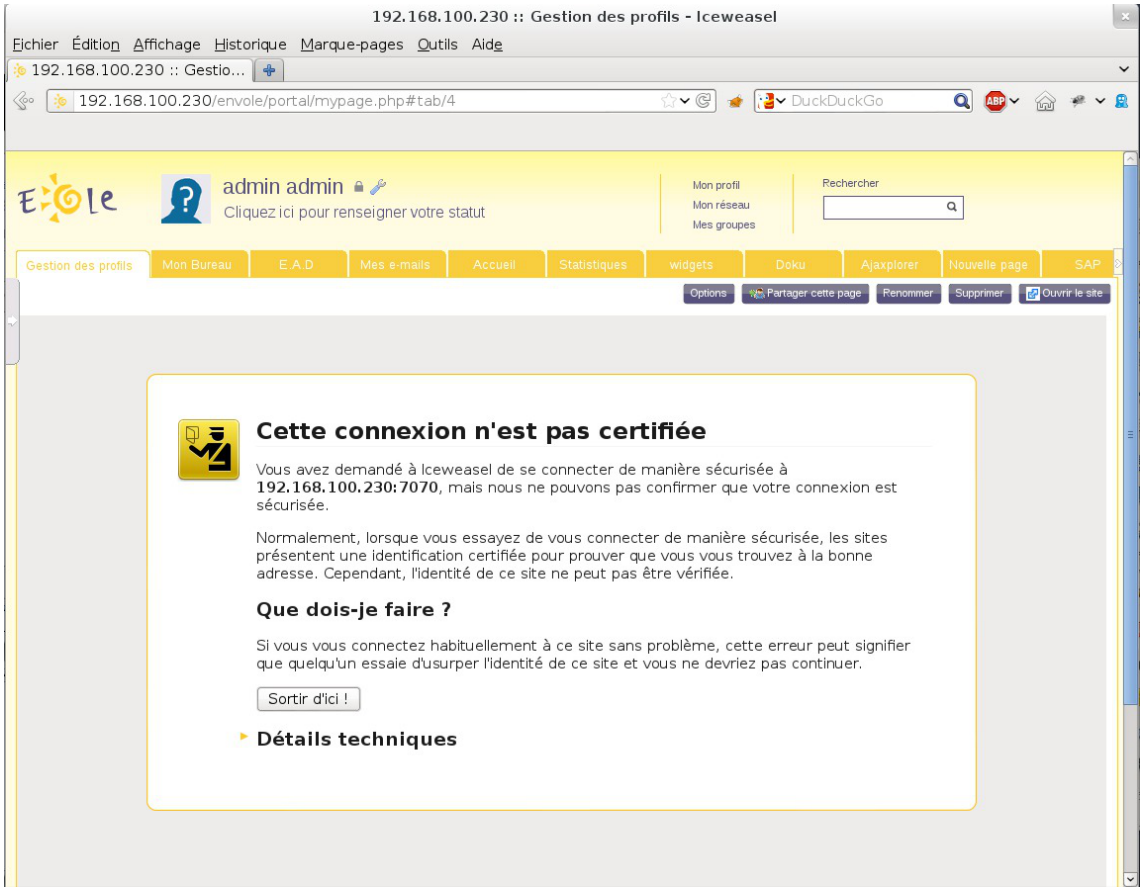
Il faut essayer de le lancer à la main et voir où il s'arrête si c'est le cas :

```
# /usr/share/eole/posteservice/10-posh
```

Impossible d'accepter le certificat à l'intérieur du portail Envole

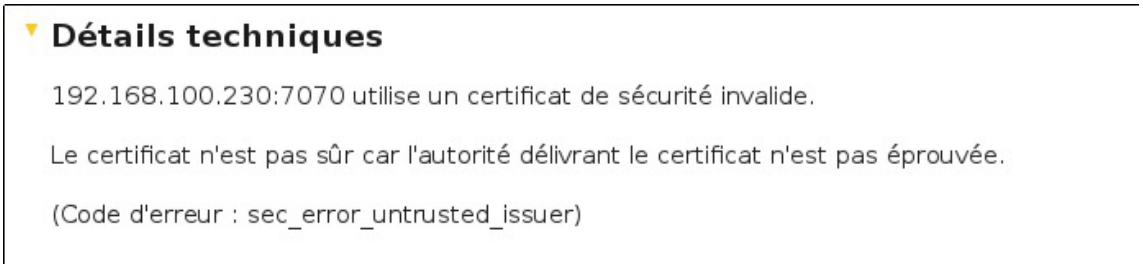
Lors du premier accès au portail il faut accepter les différents certificats. Lorsqu'on est connecté au portail, on arrive sur l'onglet Gestion des profils qui lui aussi nécessite la validation du certificat.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



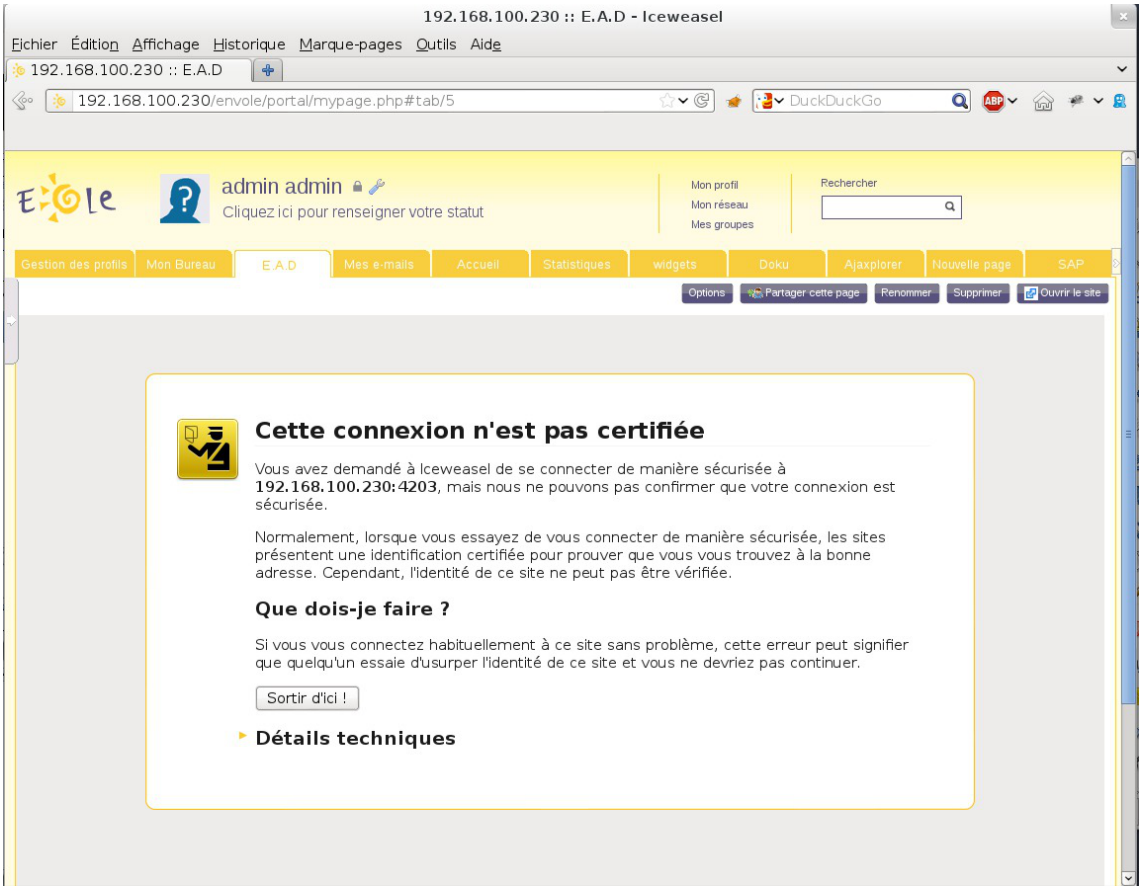
Vue du portail lors d'une première connexion

Malheureusement il n'est pas possible de valider le certificat dans la frame du portail.



Le problème sera identique pour l'onglet EAD du portail.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)



Vue de l'onglet EAD du portail lors d'une première connexion

Une des solutions consiste à ouvrir la page dans une nouvelle fenêtre en cliquant sur le bouton `Ouvrir le site`.



Une fois validé le certificat il faut fermer l'onglet, et rafraîchir l'onglet qui affiche le portail à l'aide des touches `Ctrl + r`

Les deux certificats à valider se trouvent aux adresses :

`https://<adresse serveur>:7070`

et

`https://<adresse serveur>:4203`

Le webmail renvoie une erreur IMAP

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Lors de la consultation des courriels l'utilisateur obtient le message l'utilisateur se connecte et obtient le message d'erreur `Connexion interrompue par le serveur IMAP` avec SquirrelMail ou le message `IMAP LOGIN FAILED` avec Roundcube.

L'utilisateur n'a pas de boîte locale.

Peut être que l'utilisateur n'a pas de boîte locale de déclarée.

Mais si l'utilisateur a bien une adresse locale, vous pouvez vérifier si sa boîte a bien été créée dans le répertoire `/home/mail/`.

Normalement, **envoyer un courriel à l'utilisateur suffit à créer les répertoires** associés à sa messagerie.

Si ça n'est pas le cas, une analyse des journaux d'Exim[p.889] s'impose :

`/var/log/rsyslog/local/exim/exim.info.log`

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.
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
AGRIATES *= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires*	De responsabilité partagée entre les collectivités locales et les académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications Intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements. RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE. http://www.igc.education.fr/agriates/agriates.htm

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements. RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes. RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement. RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.
ANSSI *= Agence nationale de la sécurité des systèmes d'information*	Service à compétence nationale, l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale. Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Source : https://www.cert.ssi.gouv.fr/a-propos/
Anti-spoofing *= Anti-usurpation d'adresse IP*	L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.
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.
ARV *= Administration de Réseaux Virtuels*	ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan. http://www.strongswan.org/
Backbone.js	Backbone est une bibliothèque JavaScript avec une interface RESTful JSON et est basée sur le modèle-vue-contrôleur (MVC). Cette bibliothèque est connu pour être légère, comme sa seule dépendance avec la bibliothèque JavaScript Underscore.js. Elle est conçu pour développer des applications web d'une seule page et permet de maintenir les différentes parties d'applications Web (par exemple, les clients multiples et le serveur) synchronisée. Backbone a été créé par Jeremy Ashkenas, qui est également connu pour CoffeeScript.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	http://backbonejs.org/
Balise méta	Information sur la nature et le contenu d'une page web, ajoutée dans l'en-tête de la page HTML.
bash *= Bourne-Again shell*	Bash est un interpréteur en ligne de commande de type script. C'est le shell Unix du projet GNU. Fondé sur le Bourne shell, Bash lui apporte de nombreuses améliorations, provenant notamment du Korn shell et du C shell. Bash est un logiciel libre publié sous licence publique générale GNU. Il est l'interprète par défaut sur de nombreux Unix libres, notamment sur les systèmes GNU/Linux. C'est aussi le shell par défaut de Mac OS X et il a été porté sous Microsoft Windows par le projet Cygwin. Source Wikipédia : http://fr.wikipedia.org/wiki/Bourne-Again shell
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.
BE1D *= Base Élèves 1er Degré*	L'application informatique "Base élèves premier degré" permet la gestion administrative et pédagogique des élèves de la maternelle au C.M.2 dans les écoles publiques ou privées. Elle facilite la répartition des élèves dans les classes et le suivi des parcours scolaires et améliore le pilotage académique et national. http://www.education.gouv.fr/cid24413/base-eleves-premier-degre.html En 2017 l'application BE1D fait l'objet d'une refonte complète et devient ONDE (Outil Numérique pour la Direction d'École). http://eduscol.education.fr/cid113087/refonte-de-l-application-base-elev
BIND	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet. http://www.isc.org/downloads/bind/

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Berkeley Internet Name Domain	
BIOS *= Basic Input Output System*	Le BIOS est un ensemble de fonctions contenu dans une mémoire morte (ROM) de la carte mère d'un ordinateur. Cette mémoire permet à l'ordinateur d'effectuer des opérations élémentaires lors de sa mise sous tension. Le BIOS comprend entre autres : • un logiciel nécessaire à l'amorçage de l'ordinateur ; • le prise en charge bas niveau des communications avec les périphériques ; • des outils de diagnostic.
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.
CGI *= Common Gateway Interface*	La Common Gateway Interface (littéralement « Interface de passerelle commune »), généralement abrégée CGI, est une interface utilisée par les serveurs HTTP. Elle a été normalisée par la RFC 38751. Au lieu d'envoyer le contenu d'un fichier (fichier HTML, image), le serveur HTTP exécute un programme, puis retourne le contenu généré. CGI est le standard industriel qui indique comment transmettre la requête du serveur HTTP au programme, et comment récupérer la réponse générée. Un exemple classique de paramètre est la chaîne de caractères contenant les termes recherchés auprès d'un moteur de recherche. Source : http://fr.wikipedia.org/wiki/Common_Gateway_Interface
CIDR *= Classless Inter-Domain Routing*	La notation CIDR permet de diminuer la taille de la table de routage contenue dans les routeurs. Elle donne le numéro du réseau suivi par une barre oblique (/) et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0). Source : http://fr.wikipedia.org/wiki/Sous-réseau
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

CMS *= Content Management System*	Un système de gestion de contenu (SGC) est une famille de logiciels destinés à la conception et à la mise à jour dynamique de sites Web ou d'applications multimédia. Ils partagent les fonctionnalités suivantes : • ils permettent à plusieurs individus de travailler sur un même document ; • ils fournissent une chaîne de publication (workflow) offrant par exemple la possibilité de mettre en ligne le contenu des documents ; • ils permettent de séparer les opérations de gestion de la forme et du contenu ; • ils permettent de structurer le contenu (utilisation de FAQ, de documents, de blogs, de forums de discussion, etc.) ; • ils permettent de hiérarchiser les utilisateurs et de leur attribuer des rôles et des permissions (utilisateur anonyme, administrateur, contributeur, etc.). Les SGC ne doivent pas être confondus avec les systèmes de gestion électronique des documents (GED) qui permettent de réaliser la gestion de contenu dans l'entreprise.
Cntlm	Cntlm proxy d'authentification NTLM rapide écrit en C. Il s'intercale entre le poste client et le proxy. Il oblige l'utilisateur à renseigner son identifiant/mot de passe dans une fenêtre surgissante (popup). Il ouvre une socket en écoute et gère la transmission de chaque requête au proxy parent. Si une connexion au proxy parent est créée à nouveau et authentifiée, la connexion précédente est mise en cache et est réutilisée pour une plus grande efficacité. Cntlm intègre également la redirection transparente de port TCP/IP. Il existe de nombreuses fonctions avancées telles que le support de NTLMv2, la protection de mot de passe, le hachage de mot de passe,etc. Il est peu gourmand en terme de ressources. http://cntlm.sourceforge.net/
Conteneur *= LXC*	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
CPU *= Central Processing Unit*	Le CPU , ou en français UCT pour Unité Centrale de Traitement, désigne le ou les microprocesseurs d'un ordinateur. C'est lui qui exécute les programmes informatiques.
CreoleService	`CreoleService` est un nouvel outil qui vient remplacer

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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. Exemple : `CreoleService -c fichier smbd restart`
CRL	Acronyme : Certificate Revocation List Une CRL ou Liste de Certificats Révoqués (LCR) est une liste, datée et signée par une Autorité de Certification, des numéros de série des certificats révoqués (mis en opposition) et non expirés, mise à jour périodiquement.
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.
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.
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)
DNS *= Domain Name System*	Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP. Source : http://fr.wikipedia.org/wiki/Dns
Durée de rétention	La durée de rétention désigne le temps de conservation des sauvegardes avant leur effacement.
e2guardian	e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie. Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian. http://e2guardian.org
EAD *= EOLE ADmin*	L'EAD est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse `https://<adresse_module>:4200`. L'authentification peut être locale et/ou au travers d'EoleSSO (authentification unique). L'EAD est composé de deux parties : • un serveur de commandes (service ead-server), présent et actif sur tous les modules ; • une interface web (service ead-web), présent et actif sur tous les modules. Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, ...) ne disposent que de la version de base qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...). Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.
ELF *= Executable and Linkable Format*	ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé
Envole	Envole est un Espace Numérique Personnel pour l'Éducation. Il propose une interface de type portail Web 2.0 qui permet l'interaction entre un utilisateur et son environnement numérique résultant de l'utilisation de services hétérogènes. Il centralise dans une seule interface l'ensemble des applications de l'utilisateur : mail, agenda, dossier personnel, B2I, blog, gestion de notes, gestion des absences, etc ...

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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/
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.
Espace Numérique Personnel *= ENP, E.N.P*	Système d'intégration de service réseaux/Web permettant la constitution de bouquets de services intégrés personnalisables par l'utilisateur. Il permet de mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Etablissement (PIE) ou un Espace Numérique de Travail (ENT).
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/
FAI	Le FAI est un organisme (une entreprise ou une association) qui met à disposition une connexion au réseau informatique nommé Internet.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Fournisseur d'Accès à Internet	
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.
Filtrage syntaxique	Système de pondération détectant des mots interdits dans une page et lui assignant un score en fonction de la gravité et du nombre de mots détectés. Le proxy bloquera les pages dont le score dépasse un certain seuil.
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/
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 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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

HTTP *= HyperText Transfer Protocol - protocole de transfert hypertexte*	HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (le S signifiant sécurisé) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS. HTTP est un protocole de la couche application. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).
ICMP *= Internet Control Message Protocol*	Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
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.
INE *= Identifiant National Élève*	L'INE est l'identifiant attribué à chaque élève par le Ministère de l'Éducation nationale. Cet identifiant unique a vocation à faciliter la gestion du système éducatif et à permettre le suivi statistique des élèves, des étudiants et des apprentis. Source : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000
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`.
iptables	iptables est un logiciel libre grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu dans l'espace

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	noyau composé par des modules Netfilter. Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.
IPv6 *= Internet Protocol version 6*	L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4. Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.
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)
L'expérience à tâtons	Ne pouvant établir avec certitude qui de l'équipe a introduit ce type d'expérience dans la documentation du module Amon en version 2.2, l'équipe dans son intégralité revendique la paternité du concept.
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
Liste blanche	Une liste blanche est une liste d'adresse web autorisées par le proxy.
Liste noire	Une liste noire est un document rassemblant les noms d'entités concrètes ou virtuelles jugés indésirables. Dans le contexte informatique une liste noire est une liste d'adresses web indésirables qui seront bloquées par le proxy.
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	UNIX.
LXC *= Linux Containers*	LXC, contraction de l'anglais Linux Containers, est un système de virtualisation au niveau système d'exploitation utilisé pour faire fonctionner de multiples environnements Linux isolés les uns des autres sur un seul et même système hôte. Le conteneur LXC n'est pas une machine virtuelle mais uniquement un environnement virtualisé qui dispose de ses propres processus et de son propre réseau (isolés du système physique hôte).
man in the middle *= homme du milieu*	L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. Source Wikipédia : http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
Marionette	Marionette simplifie le code applicatif Backbone grâce à des vues robustes et des solutions d'architecture. http://marionettejs.com/
MTA *= Message Transfert Agent*	Message (ou Mail) Transfert Agent. Agent de transfert de message (ou de courrier), qui s'occupe de l'acheminement des messages.
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 Access Server*	Un Network Access Server (NAS), ici un switch, fonctionne comme un client RADIUS. Au sein d'un réseau, le premier équipement qui prend en charge un client (machine ou utilisateur) est un équipement d'accès (switch, point d'accès Wifi). Ces équipements jouent un rôle crucial car ce sont eux qui détectent la présence d'un équipement qui essaye de rejoindre le réseau. Ils interviennent donc dans le processus d'authentification. Dans la terminologie RADIUS, ces équipements

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	d'accès sont appelés NAS (Network Access Server), ou clients Radius : ce sont ces équipements qui interagissent avec le serveur RADIUS en utilisant le protocole du même nom. Ils devront d'ailleurs être configurés pour cela (ils doivent connaître l'adresse IP du serveur Radius). Source : http://juboite.hd.free.fr/doku.php?id=tuto:radius:freeradius
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.
NetBIOS	NetBIOS est une architecture réseau et non un protocole réseau. C'est un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau. Ce service sert à associer un nom d'ordinateur à une adresse IP. NetBIOS tant à disparaître au profit des noms DNS. Le nom NetBIOS d'une machine est de type alphanumérique, excepté le premier caractère qui doit être de type alphabétique. Il doit comprendre entre 2 et 15 caractères.
NFS *= Network File System*	NFS est est un protocole développé par Sun Microsystems qui permet à un ordinateur d'accéder à des fichiers via un réseau. Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Des implémentations existent pour Macintosh et Microsoft Windows. NFS est compatible avec IPv6 sur la plupart des systèmes.
Nginx *= Engine-x*	Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. 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.
NIS *= Network Information Service*	Network Information Service nommé aussi Yellow Pages est un protocole client serveur développé par Sun permettant la centralisation d'informations sur un réseau UNIX. Son but est de distribuer sur un réseau les informations contenues dans des fichiers de configuration contenant par exemple les noms d'hôte (/etc/hosts), les comptes utilisateurs (/etc/passwd), etc.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Un serveur NIS stocke et distribue donc les informations administratives du réseau, qui se comporte ainsi comme un ensemble cohérent de comptes utilisateurs, groupes, machines, etc. Source Wikipédia : http://fr.wikipedia.org/wiki/Network_Information_Service
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`.
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
ODI *= Oracle Data Integrator*	ODI - Ex Sunopsis est un logiciel propriétaire de Oracle Corporation développé en java pour réaliser des tâches de type ETL/EAI. Les développements sont centralisés dans un référentiel stocké sur une base de données. Le référentiel stocke également l'ensemble des métadonnées permettant une vision globale du système d'information ainsi que des flux d'alimentation développés dans ODI.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Le principal objectif d'ODI est de faciliter les développements et la maintenance par l'intermédiaire de références croisées, cet outil permet l'automatisation de l'échange entre toutes les applications du SI.
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
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
OSPF *= Open Shortest Path First*	Open Shortest Path First (OSPF) est un protocole de routage interne IP de type « à état de liens ». Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB. Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire. En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Open_Shortest_Path_First
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
pad	Un « pad » est un texte collaboratif créé à partir d'un éditeur de texte collaboratif en ligne.
PAM *= Pluggable Authentication Modules*	PAM est un mécanisme permettant d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau, permettant de ce fait de rendre indépendants du schéma les logiciels réclamant une authentification. PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. PAM permet de contrôler la manière dont les modules sont enfichés dans les programmes en modifiant un fichier de configuration. Les programmes qui donnent aux utilisateurs un accès à des privilèges doivent être capables de les authentifier. Lorsque vous vous connectez sur le système, vous indiquez votre nom et votre mot de 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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

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.
Politique de filtrage	Une politique de filtrage permet de définir une suite d'autorisation et d'interdiction dans les accès web.
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.
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.
Préfixe binaire	Les préfixes binaires (kibi-, mébi-, gibi-, tébi-, pébi- et exbi-) sont souvent utilisés lorsqu'on a affaire à de grandes quantités d'octets. Ils sont dérivés, tout en étant différents, des préfixes du système international (kilo-, méga-, giga- et ainsi de suite). La raison d'être de ces préfixes binaires est d'éviter la confusion de valeur avec les préfixes du système international. http://fr.wikipedia.org/wiki/Préfixe_binaire
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.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

Proxy sibling *= proxy frère*	Hiérarchiquement, un cache interrogé peut être un de niveau supérieur (parent) ou de niveau égal (frère ou sibling). Les serveurs parents sont d'ordinaire plus proches du serveur hébergeant l'objet recherché que les serveurs fils. Si un serveur fils ne peut trouver l'objet, la requête est en général relayée vers un serveur de cache parent qui va rapporter, mémoriser (mettre en cache) et finalement transmettre la requête au demandeur. Les serveurs frères (siblings) sont des serveurs de cache d'un niveau hiérarchique égal, dont le but est de répartir la charge. http://fr.wikipedia.org/wiki/Internet_Cache_Protocol
PUA *= Potentially Unwanted Applications*	Applications potentiellement indésirables.
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
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
Relai SMTP	Le relai SMTP est un service qui se charge de router des requêtes SMTP vers un serveur SMTP, tandis que le serveur s'occupe de la gestion du courrier électronique (stockage, réception et envoi).
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 l'opération inverse de la sauvegarde.
RIP *= Routing Information Protocol*	RIP, protocole d'information de routage, est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé. Il permet à chaque routeur de communiquer aux routeurs voisins la métrique, c'est-à-dire la distance qui les sépare d'un réseau IP déterminé quant

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	au nombre de sauts ou « hops » en anglais.Pour chaque réseau IP connu, chaque routeur conserve l'adresse du routeur voisin dont la métrique est la plus petite. Ces meilleures routes sont diffusées toutes les 30 secondes. Source Wikipédia : http://fr.wikipedia.org/wiki/Routing_Information_Protocol
RNE *= UAI*	Depuis 1978, chaque établissement scolaire (écoles, collèges, lycées, CFA, enseignement supérieur, public ou privé) possède un code unique dans le répertoire national des établissements, aussi appelé RNE. En 1996, le « RNE » a changé de nom et s'intitule désormais « UAI » pour Unité Administrative Immatriculée qui concerne 135 000 établissements. Chaque établissement scolaire bénéficie d'un code UAI (ex-RNE) composé de 7 chiffres et d'une lettre (par exemple 0951099D) : • 3 premiers chiffres (095) qui correspondent au département (par exemple 012 pour l'Aveyron, 095 pour le Val-d'Oise, 974 pour la Réunion...) ; • 4 chiffres (1099) qui permettent d'identifier un établissement de façon unique dans le département ; • 1 lettre (D) qui sert de checksum (ou somme de contrôle) pour vérifier la bonne saisie du code. Cette dernière lettre est calculée ainsi : • on prend le nombre composé par les 7 premiers chiffres (exemple : 0951099) ; • on divise ce nombre par 23 et on garde le reste (exemple : reste de (0951099/23) = 3) ; • on prend ensuite les lettres de l'alphabet auxquelles on a enlevé les I, O et Q soient 23 lettres (a,b,c,d,e,f,g,h,j,k,l,m,n,p,r,s,t,u,v,w,x,y,z) ; • la lettre choisie est celle de la position reste + 1 (exemple : position 3+1=4, soit la lettre D). Source : http://blog.juliendelmas.com/?qu-est-ce-que-le-code-rne-ou-uai
Round-robin *= tourniquet*	Round-robin (RR) est un algorithme d'ordonnancement courant dans les systèmes d'exploitation. Ce dernier attribue des tranches de temps à chaque processus en proportion égale, sans accorder de priorité aux processus. Source Wikipédia : http://fr.wikipedia.org/wiki/Round-robin_(informatique)
Samba	Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= SaMBa : Server Message Block	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.
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 à l'utilisateur final. http://olivier.sessink.nl/scannedonly/
SDET *= Schéma Directeur des Espaces Numériques de Travail*	Le Schéma Directeur des Espaces Numériques de Travail (SDET) regroupe les grandes orientations de l'éducation nationale pour ses espaces numériques de travail. Il permet de définir les services attendus et leurs préconisations techniques. Pour plus d'informations consultez la page : http://eduscol.education.fr/pid25719/schema-directeur-des-ent-sdet.htm
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/
SIECLE anciennement Sconet *= Système d'information pour les élèves en collèges et lycée et pour les établissements*	SIECLE est une application informatique de gestion des élèves, mise à disposition des établissements scolaires du second degré en France et accessible depuis leurs locaux par un simple navigateur via un réseau sécurisé (appelé réseau AGRIATES). Il remplace depuis janvier 2012 l'application Sconet (Scolarité sur le Net).
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	SMTP est un protocole de communication utilisé pour transférer le

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= Simple Mail Transfer Protocol	courrier électronique vers les serveurs de messagerie électronique.
Squid	Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.
SSH *= Secure Shell*	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
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.
Swap *= Verbe échanger*	En informatique le swap sert à étendre la mémoire utilisable par un système d'exploitation, par un fichier d'échange ou une partition dédiée ; c'est aussi une instruction de certains processeurs et une fonction de certains langages de programmation qui permet l'échange de deux variables.
Sympa *= SYstème de Multi-Postage Automatique*	Sympa est un gestionnaire de listes de diffusion hautement configurable. Il peut gérer de grosses listes et comprend une interface web complète.

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	Sympa est multilingue et peut interopérer avec un annuaire LDAP ou un SGBD pour définir des listes de diffusion dynamiques. Le développement et la diffusion de Sympa sont contrôlés par RENATER. http://www.sympa.org
TCP *= Transmission Control Protocol*	TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport qui travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.
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.
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
Type MIME	Un type MIME est une information permettant de connaitre le format d'un document sans se baser sur l'extension.
UAC	UAC, contrôle du compte de l'utilisateur en français est un mécanisme

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

= User Account Control	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.
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`
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
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
Web 2.0 *= Web participatif*	L'expression « Web 2.0 » désigne l'ensemble des technologies et des usages du World Wide Web qui ont suivi la forme initiale du web, en particulier les interfaces permettant aux internautes ayant peu de connaissances techniques de s'approprier les nouvelles

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	fonctionnalités du web et ainsi d'interagir de façon simple à la fois avec le contenu et la structure des pages et aussi entre eux, créant ainsi notamment le Web social.
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). Cette fonction possède deux arguments associés : • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL
WPKG	WPKG est un logiciel de déploiement, de mise à jour et de suppression automatisés des paquetages pour Windows. Il peut être utilisé pour pousser/tirer des paquetages logiciels tels que des Services Packs, des hotfix, ou des programmes d'installation depuis un serveur central (par exemple Samba ou Active Directory). Il peut être lancé en tant que service, afin d'installer des logiciels en tâche de fond, sans interaction avec l'utilisateur. Configuré comme tel, il peut fonctionner même si l'utilisateur qui ouvre la session ne bénéficie pas de privilèges administrateur. WPKG peut installer des paquetages MSI, Installshield, Packagesfortheweb, Inno Setup, Nullsoft, ainsi que tous les autres installateurs de programme et aussi des scripts. Source Wikipédia : http://fr.wikipedia.org/wiki/Wpkg
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

Documentation sous licence Creative Commons by-sa - EOLE (http://eole.orion.education.fr)

	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. 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)