

Installation et mise en œuvre du module Horus

EOLE 2.5.2



EOLE 2.5.2

Version : révision : Avril 2016

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 suggérerait 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 Horus | 8 |
| 1. Qu'est ce que le module Horus ? | 8 |
| 2. À qui s'adresse ce module ? | 10 |
| 3. Les services Horus | 10 |
| 4. Structure des conteneurs | 11 |
| 5. Pré-requis | 11 |
| 6. Les différences entre les versions 2.4 et 2.5 | 12 |
| 7. Errata 2.5.n | 15 |
| Chapitre 2 - Fonctionnement du module Horus | 16 |
| Chapitre 3 - Installation du module Horus | 18 |
| Chapitre 4 - Configuration du module Horus | 19 |
| 1. Configuration en mode basique | 20 |
| 1.1. Onglet Général | 20 |
| 1.2. Onglet Services | 22 |
| 1.3. Onglet Interface-0 | 23 |
| 1.4. Onglet Directeur bacula | 25 |
| 1.5. Onglet Dhcp : Configuration du serveur DHCP | 25 |
| 1.6. Onglet Samba : Configuration du contrôleur de domaine | 27 |
| 1.7. Onglet Messagerie | 28 |
| 2. Configuration en mode normal | 30 |
| 2.1. Onglet Général | 31 |
| 2.2. Onglet Services | 33 |
| 2.3. Onglet Interface-0 | 34 |
| 2.4. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs | 38 |
| 2.5. Onglet Clamav : Configuration de l'anti-virus | 39 |
| 2.6. Onglet Directeur bareos | 41 |
| 2.7. Onglet Stockage bareos | 44 |
| 2.8. Onglet Annuaire | 44 |
| 2.9. Onglet Dhcp : Configuration du serveur DHCP | 45 |
| 2.10. Onglet Esu : Configuration du proxy ESU | 47 |
| 2.11. Onglet Samba : Configuration du contrôleur de domaine | 48 |
| 2.12. Onglet Onduleur | 51 |
| 2.13. Onglet Applications web : Configuration des applications web | 57 |
| 2.14. Onglet Eole sso : Configuration du service SSO pour l'authentification unique | 58 |
| 2.15. Onglet Messagerie | 62 |
| 3. Configuration en mode expert | 64 |
| 3.1. Onglet Général | 65 |
| 3.2. Onglet Services | 71 |
| 3.3. Onglet Système | 72 |
| 3.4. Onglet Sshd : Gestion SSH avancée | 74 |
| 3.5. Onglet Logs : Gestion des logs centralisés | 74 |
| 3.6. Onglet Interface-0 | 76 |
| 3.7. Onglet Interface-n | 80 |
| 3.8. Onglet Réseau avancé | 85 |
| 3.9. Onglet Certificats ssl : gestion des certificats SSL | 89 |
| 3.10. Onglet Eoledb : Gestion des bases de données | 91 |
| 3.11. Onglet Mots de passe : Politique de mot de passe pour les utilisateurs | 92 |

| | |
|---|-----|
| 3.12. Onglet Clamav : Configuration de l'anti-virus | 93 |
| 3.13. Onglet Directeur bareos | 96 |
| 3.14. Onglet Annuaire | 99 |
| 3.15. Onglet Dhcp : Configuration du serveur DHCP | 100 |
| 3.16. Onglet Tftp : Configuration d'un serveur PXE/TFTP | 103 |
| 3.17. Onglet Esu : Configuration du proxy ESU | 104 |
| 3.18. Onglet Samba : Configuration du contrôleur de domaine | 105 |
| 3.19. Onglet Nscd | 112 |
| 3.20. Onglet Onduleur | 112 |
| 3.21. Onglet Applications web : Configuration des applications web | 118 |
| 3.22. Onglet Apache : Configuration avancée du serveur web | 119 |
| 3.23. Onglet Eole sso : Configuration du service SSO pour l'authentification unique | 121 |
| 3.24. Onglet Ead-web : EAD et proxy inverse | 127 |
| 3.25. Onglet Mysql : Configuration du serveur MySQL | 127 |
| 3.26. Onglet Openldap : Configuration du serveur LDAP local | 128 |
| 3.27. Onglet Cups : Configuration du serveur d'impression | 129 |
| 3.28. Onglet Proftpd : Configuration du serveur FTP | 131 |
| 3.29. Onglet Messagerie | 134 |
| 3.30. Onglet Eoleflask | 139 |
| 4. Prise en charge d'applications supplémentaires | 140 |
| 4.1. Téléchargement et mise en place | 141 |
| 4.2. Configuration Apache | 142 |
| 4.3. Configuration MySQL | 143 |
| 4.4. Configuration du logiciel | 144 |
| 5. EoleSSO | 145 |
| 5.1. Présentation du produit EoleSSO | 145 |
| 5.2. Onglet Eole sso : Configuration du service SSO pour l'authentification unique | 147 |
| 5.3. Protocoles supportés | 152 |
| 5.3.1. Compatibilité CAS | 152 |
| 5.3.2. Compatibilité SAML2 | 153 |
| 5.3.3. Compatibilité RSA Securid | 154 |
| 5.4. Gestion des attributs des utilisateurs | 155 |
| 5.4.1. Ajout d'attributs calculés | 155 |
| 5.4.2. Filtrage des données par application | 157 |
| 5.4.3. Définition de filtres d'attributs | 158 |
| 5.5. Fédération avec une entité partenaire | 159 |
| 5.5.1. Déclaration d'un serveur parent | 160 |
| 5.5.2. Fédération SAML : Gestion des Associations | 161 |
| 5.5.3. Fédération SAML : Gestion des méta-données | 165 |
| 5.5.4. Fédération SAML : Accès aux ressources | 166 |
| 5.5.5. Gestion des sources d'authentification multiples | 168 |
| 5.6. Personnalisation de la mire SSO | 172 |
| 5.7. Annexes | 174 |
| 5.7.1. Résumé des fichiers et liens | 174 |
| 5.7.2. Astuces d'exploitation | 175 |
| 5.7.3. Exemple de Fédération avec RSA/FIM | 176 |
| 5.7.4. Fédération entre 2 serveurs EoleSSO | 177 |
| 5.7.5. Mise en place de l'authentification OTP | 179 |
| 5.7.6. Application de redirection : Eole-dispatcher | 180 |
| 6. Activation et configuration de Bareos | 184 |
| 7. Gestion des bases de données avec EoleDB | 189 |

| | |
|--|------------|
| Chapitre 5 - Instanciation du module | 197 |
| Chapitre 6 - Administration du module Horus | 198 |
| 1. Fonctionnalités de l'EAD propres au module Horus | 198 |
| 1.1. Gestion des comptes Horus | 198 |
| 1.1.1. Gestion des groupes | 199 |
| 1.1.2. Gestion des utilisateurs | 200 |
| 1.1.3. Gestion des partages | 203 |
| 1.1.4. Suppression des comptes de machine | 204 |
| 1.2. Les ACLs | 205 |
| 1.3. Gestion des connexions | 206 |
| 1.4. Quotas disque | 206 |
| 1.5. Observation des virus | 208 |
| 1.6. Scripts administratifs | 208 |
| 1.7. Extraction AAF | 209 |
| 1.8. Réserveation d'adresse IP dans l'EAD | 210 |
| 2. Gestion des utilisateurs sur le module Horus | 210 |
| 3. Les sauvegardes | 213 |
| 3.1. Généralités sur la sauvegarde | 213 |
| 3.1.1. Sauvegarde totale | 213 |
| 3.1.2. Sauvegarde incrémentale | 213 |
| 3.1.3. Sauvegarde différentielle | 214 |
| 3.1.4. Des outils de sauvegarde | 214 |
| 3.2. La sauvegarde EOLE | 215 |
| 3.2.1. Le vocabulaire Bareos | 215 |
| 3.2.2. Architecture de Bareos | 217 |
| 3.2.3. Configuration des sauvegardes | 219 |
| 3.2.4. Programmation des sauvegardes | 231 |
| 3.3. La restauration des sauvegardes EOLE | 233 |
| 3.3.1. Restauration complète | 233 |
| 3.3.2. Restauration partielle | 236 |
| 3.4. Ajouter des données à sauvegarder | 239 |
| 3.5. Réinitialisation de la sauvegarde | 240 |
| 3.6. bareos-webui : outil d'administration pour Bareos | 240 |
| 3.7. Diagnostic, rapport et résolution de problème | 244 |
| 3.7.1. Outils de diagnostic et rapport | 244 |
| 3.7.2. Base de donnée sqlite de Bareos irrécupérable | 246 |
| 3.8. Annexes | 249 |
| 3.8.1. Autres outils d'administration pour Bareos | 249 |
| 3.8.2. Quelques références | 250 |
| 3.8.3. Un répertoire partagé comme supports de sauvegarde | 251 |
| 4. Les imprimantes | 255 |
| 4.1. L'interface simplifiée | 255 |
| 4.2. L'interface de gestion CUPS | 256 |
| 4.2.1. Création de l'imprimante | 256 |
| 4.2.2. Choix du pilote | 260 |
| 4.2.3. Quotas d'impression | 265 |
| 4.3. Gestion des imprimantes sous Windows | 265 |
| 4.4. Questions fréquentes | 266 |
| 5. Compatibilité entre GFC et le module Horus | 266 |
| 6. Mise en place des sondes EQOS | 266 |

| | |
|--|------------|
| 7. Les clients Windows | 267 |
| 7.1. Installation et configuration des clients Windows | 267 |
| 7.1.1. Principe | 267 |
| 7.1.2. Configuration réseau | 268 |
| 7.1.3. Intégration et installation du client Horus manuelle | 268 |
| 7.1.4. Intégration et installation du client Horus automatique | 274 |
| 7.1.5. Mise à jour du client Horus | 277 |
| 7.1.6. Désinstallation du client Horus | 278 |
| 7.2. Administration des clients Windows | 279 |
| 7.2.1. Scripts personnalisés | 280 |
| 7.2.2. Les profils utilisateurs | 281 |
| 7.2.3. Gestion des configurations clientes avec ESU | 287 |
| 7.3. Déploiement d'applications pour Windows avec WPKG | 297 |
| 7.3.1. Installation et configuration | 298 |
| 7.3.2. Les packages WPKG | 302 |
| 7.3.3. Journalisation des actions WPKG | 306 |
| 7.3.4. WPKG scripts de pre et post installation | 309 |
| 7.3.5. WPKG logiciels avec traitement particulier | 313 |
| 7.3.6. Quelques références | 313 |
| 8. Les clients FTP | 314 |
| 9. Les applications web sur le module Horus | 317 |
| 9.1. L'authentification unique avec EoleSSO | 317 |
| 9.2. Applications pré-installées | 318 |
| 9.2.1. phpMyAdmin : gestionnaire de base de données MySQL | 319 |
| 9.3. Prise en charge d'applications supplémentaires | 320 |
| 9.3.1. Téléchargement et mise en place | 321 |
| 9.3.2. Configuration Apache | 322 |
| 9.3.3. Configuration MySQL | 323 |
| 9.3.4. Configuration du logiciel | 324 |
| 10. Réplication LDAP | 325 |
| Chapitre 7 - Compléments techniques | 328 |
| 1. Les services utilisés sur le module Horus | 328 |
| 1.1. eole-annuaire | 328 |
| 1.2. eole-exim | 328 |
| 1.3. eole-antivirus | 329 |
| 1.4. eole-dhcp | 330 |
| 1.5. eole-fichier-primaire | 331 |
| 1.6. eole-cups | 331 |
| 1.7. eole-proftpd | 332 |
| 1.8. eole-mysql | 332 |
| 1.9. eole-web | 333 |
| 1.10. eole-interbase | 334 |
| 2. Ports utilisés sur le module Horus | 334 |
| 3. L'annuaire LDAP du module Horus | 335 |
| 3.1. Arborescence de l'annuaire | 336 |
| 3.2. Utilisateurs spéciaux | 337 |
| 3.3. Entrée ordinateur du domaine | 338 |
| 3.4. Entrée partage | 338 |
| 4. La gestion du SID | 339 |

| | |
|---|-----|
| Chapitre 8 - Questions fréquentes | 341 |
| 1. Questions fréquentes communes aux modules | 341 |
| 2. Questions fréquentes propres au module Horus | 351 |
| 3. Questions fréquentes propres à la sauvegarde | 356 |
| Glossaire | 361 |

Chapitre 1

Introduction au module Horus

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

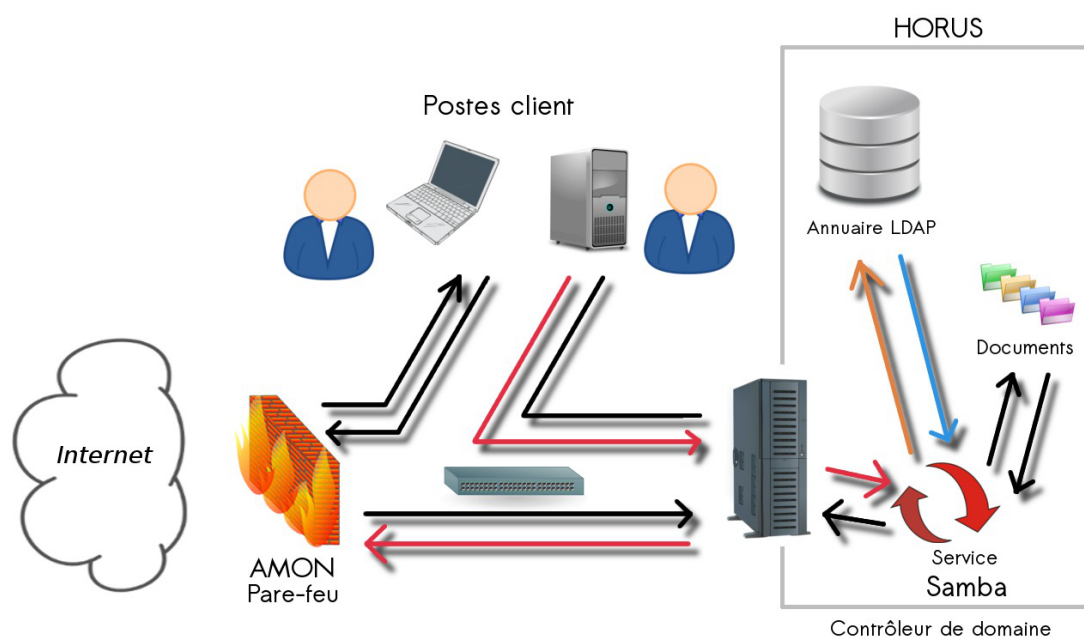
Il est également utilisable dans n'importe quelle autre structure nécessitant un contrôleur de domaine.

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

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

Le contrôleur de domaine permet donc :

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



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

1. Qu'est ce que le module Horus ?

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

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

Il peut également se substituer à un contrôleur de domaine NT^[p.362], pour l'authentification des utilisateurs, l'exécution des scripts de connexion, la gestion des droits sur les partages.

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

Les applications nationales ainsi que toutes les fonctionnalités de partage de fichiers et de gestion des utilisateurs de clients Windows sont intégrées sur le module Horus. Le module Horus est doté d'une base de données InterBase^[p.366]. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP^[p.363] pour l'attribution dynamique d'adresse IP.

Depuis plusieurs années, les applications nationales utilisées en Établissement Public Local d'Enseignement^[p.363] (EPL) sont qualifiées pour fonctionner sur le module Horus :

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



Les applications nationales sont décrites à l'adresse suivante :

<http://www.esen.education.fr/fr/ressources-par-type/outils-pour-agir/le-film-annuel-des-person>

Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL^[p.361] ;
- quotas disque ;
- partage d'imprimantes ;
- gestion des comptes utilisateurs et des accès ;
- exécution d'applications utilisateur.

Annuaire :

- l'annuaire est initialisé à partir d'importation de comptes (AAF^[p.361], CSV^[p.362], ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- un service de messagerie instantanée (standard XMPP^[p.373]) ;

Serveur web :

- une authentification centralisée ;
- des applications.

Gestion avancée des utilisateurs et des postes clients :

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

2. À qui s'adresse ce module ?

Le module Horus s'adresse principalement aux réseaux administratifs d'un établissement scolaire. Il peut toutefois être utilisé partout où il est nécessaire d'avoir un serveur de fichiers.

3. Les services Horus

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

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

Services communs à tous les modules

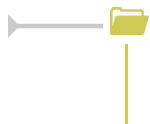
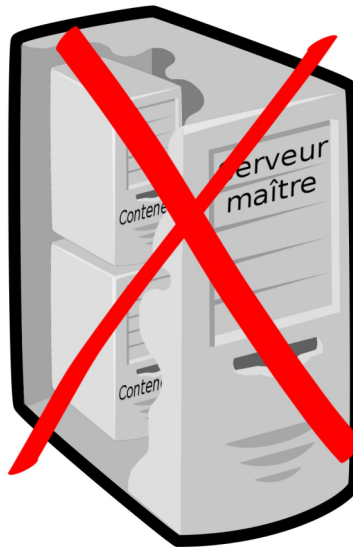
- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;
- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO*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

Services spécifiques au module Horus

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseau ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL^[p.361] ;
- *CUPS* : serveur d'impression ;
- *InterBase* : système de gestion de base de données utilisé pour les anciennes applications nationales ;
- *MySQL* : système de gestion de base de données utilisé pour les nouvelles applications nationales ;
- *Bacula* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller les partages du serveur et les échanges FTP ;
- *dhcpc3-server* : serveur DHCP.

4. Structure des conteneurs

Le module Horus s'installe par défaut en mode non conteneur^[p.362].



La mise en œuvre du mode conteneur pour ce module est possible mais ne fait pas l'objet d'une procédure de qualification.

5. Pré-requis

Les ressources de ce module sont fortement dépendantes du nombre d'utilisateurs.

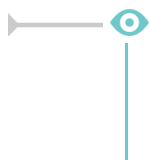
Les CPU doivent être de préférence en 64 bits.

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

Le module fonctionne avec une seule carte réseau.

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

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



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

6. Les différences entre les versions 2.4 et 2.5

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.

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.364] ;
- Backbone.js^[p.361] et Marionette^[p.366] ;
- Tiramisu^[p.371].

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.371].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML^[p.372] Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

Mode conteneur

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

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

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

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

Changement dans le PATH des commandes

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

Répertoire d'installation du logiciel nginx

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

Suppression de la base matériels

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

Logiciel de sauvegarde

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

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

ClamAV

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

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.

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.

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.

7. Errata 2.5.n

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

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



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



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

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

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

Chapitre 2

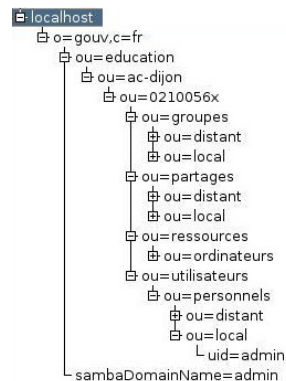
Fonctionnement du module Horus

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

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

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

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



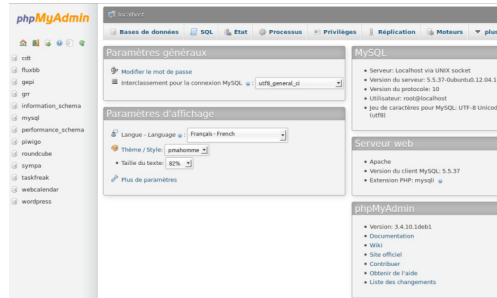
Une importation massive de comptes peut être réalisée depuis les formats AAF et Texte.

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

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

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

L'authentification unique est assurée par le service EoleSSO.

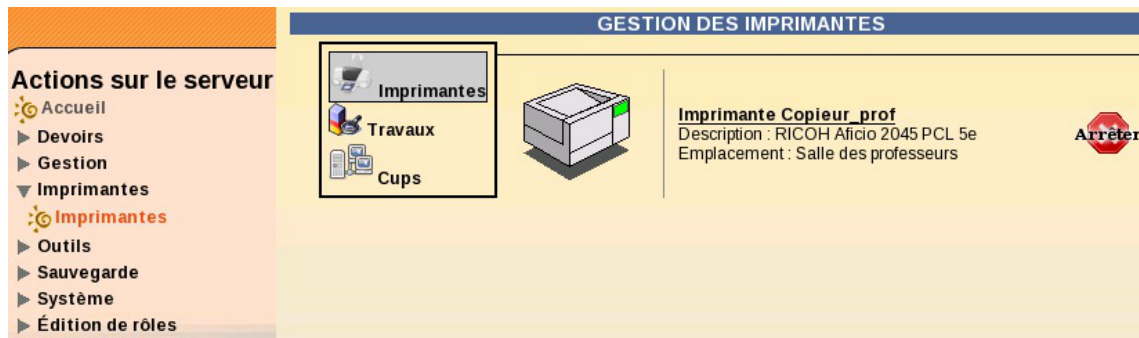


Édition de tables avec phpMyAdmin

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

Le serveur d'impression permet :

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



Interface simplifiée de gestion des imprimantes (EAD)

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

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

Chapitre 3

Installation du module Horus

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.

Après l'installation du module Horus, la mise à jour n'est pas obligatoire mais fortement recommandée.

Mise à jour

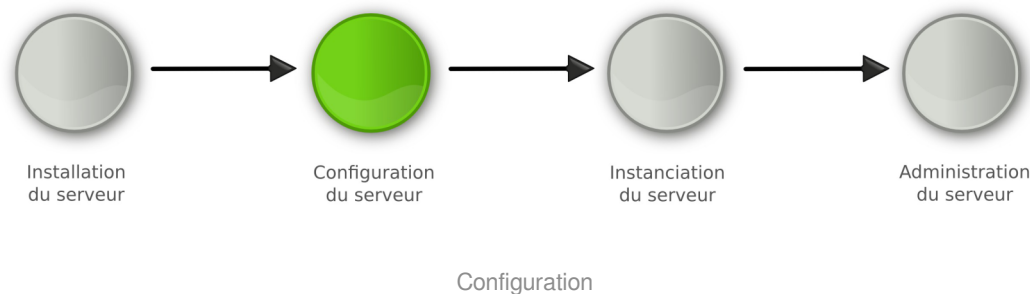
Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto` .

💡 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.

Chapitre 4

Configuration du module Horus



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.370], e2guardian^[p.363], etc.

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

Cela se traduit par des erreurs de timeout^[p.371] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Gunicorn^[p.365].



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

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

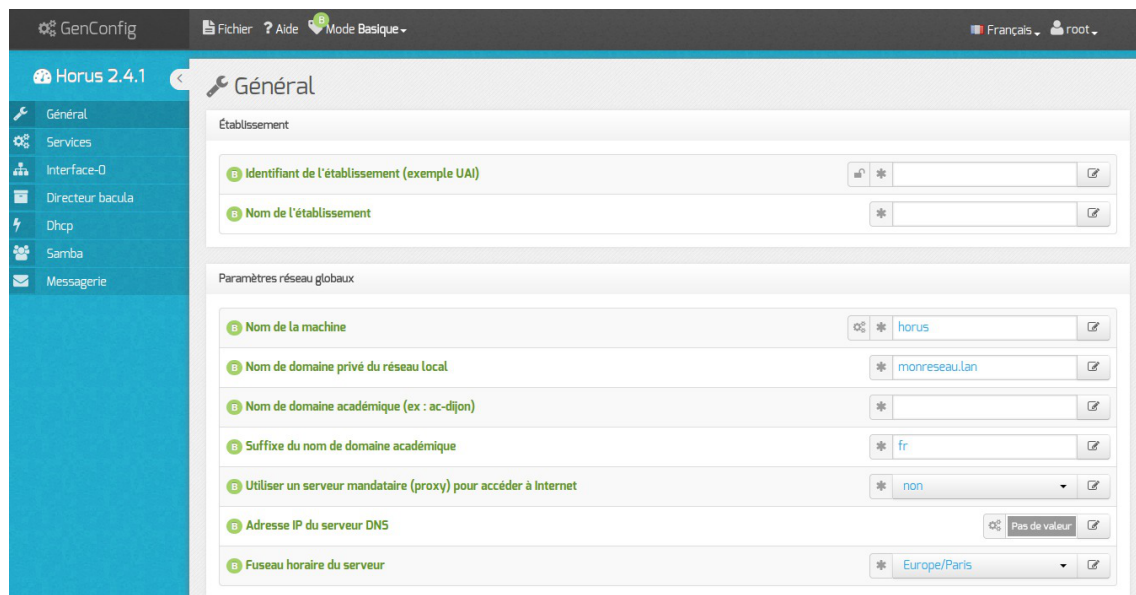
```
# CreoleService eoleflask restart
```

1. Configuration en mode basique

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

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

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



Vue générale de l'interface de configuration du module

1.1. Onglet Général

Présentation des différents paramètres de l'onglet Général.

Informations sur l'établissement

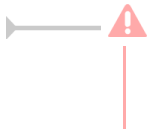
| Établissement | |
|---|--------------------|
| Identifiant de l'établissement (exemple UAI) | 🔒 * 0000G12345 |
| Nom de l'établissement | * MonEtablissement |

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.366] 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

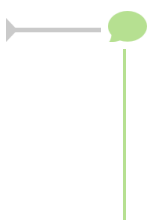
| Paramètres réseau globaux | |
|--|-----------------|
| Nom de la machine | * harpocrate |
| Nom de domaine privé du réseau local | * monreseau.lan |
| Nom de domaine académique (ex : ac-dijon) | * ac-dijon |
| Suffixe du nom de domaine académique | * fr |

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.

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.

| | |
|---|--------|
| Utiliser un serveur mandataire (proxy) pour accéder à Internet | * oui |
| Nom ou adresse IP du serveur proxy | * |
| Port du serveur proxy | * 3128 |

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

| | |
|----------------------------------|-------------------------------------|
| Adresse IP du serveur DNS | 192.168.232.2 192.168.122.1 8.8.8.8 |
| Fuseau horaire du serveur | Europe/Paris |

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.363].

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

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 onglet de configuration propre au service.

Services

Configuration

| | |
|--------------------------------|-------|
| Activer le serveur DHCP | * non |
|--------------------------------|-------|

Vue de l'onglet Services

En mode basique seul le service DHCP est activable.

1.3. Onglet Interface-0

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

Vue de l'onglet Interface-n

Configuration de l'interface

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

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH

B Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) * oui

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.370] 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.

Administration distante sur l'interface

B Autoriser les connexions ssh oui

B Adresse IP réseau autorisée pour les connexions ssh

B Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

B Masque du sous réseau pour les connexions ssh * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions ssh

B Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) oui

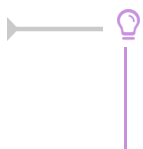
B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

B Masque du sous réseau pour administrer le serveur * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

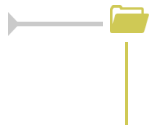
Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour...`



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

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

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



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

1.4. Onglet Directeur bacula



Vue de l'onglet Directeur Bacula

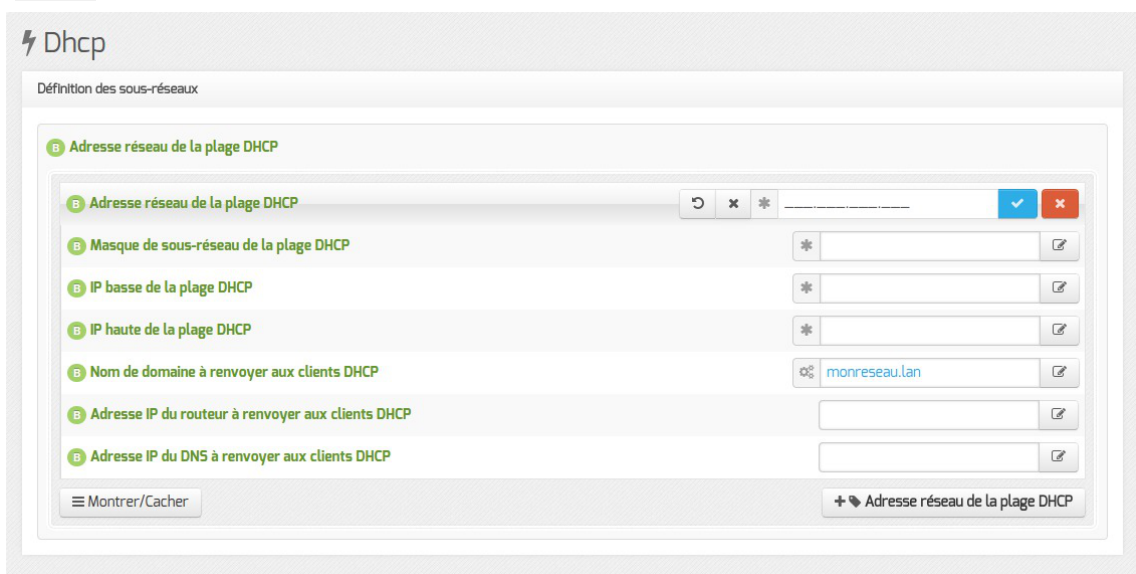
Le nom du directeur est une information importante, il est utilisé en interne dans le logiciel mais, surtout, il est nécessaire pour configurer un client Bacula ou pour joindre le serveur de stockage depuis un autre module.

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.

1.5. 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.



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

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.

The screenshot shows a configuration window titled "Définition des sous-réseaux". It contains a list of DHCP configuration parameters:

- Adresse réseau de la plage DHCP**: 192.168.0.0
- Masque de sous-réseau de la plage DHCP**: 255.255.255.0
- IP basse de la plage DHCP**: 192.168.0.50
- IP haute de la plage DHCP**: 192.168.0.60
- Nom de domaine à renvoyer aux clients DHCP**: monreseau.lan
- Adresse IP du routeur à renvoyer aux clients DHCP**: 192.168.232.2
- Adresse IP du DNS à renvoyer aux clients DHCP**: 192.168.232.2

At the bottom, there is a "Montrer/Cacher" button and a "+ Adresse réseau de la plage DHCP" button.

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

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.

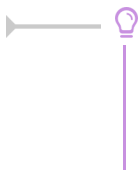
Pour la configuration de l'Adresse IP du routeur à renvoyer aux clients DHCP :

- 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.364] 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.363], 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.

1.6. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC^[p.369]) 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.).

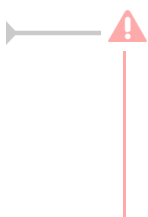
Seules deux variables sont à remplir avec attention pour obtenir un contrôleur fonctionnel.

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.367]) 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`) ;
- \$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.369] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

1.7. Onglet Messagerie

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

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

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

Serveur d'envoi/réception

The screenshot shows the 'Messagerie' configuration window. It has a title bar with a mail icon and the text 'Messagerie'. Below the title bar, there is a subtitle 'Serveur d'envoi/réception (SMTP)'. The main area contains two input fields:

- The first field is labeled 'Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)'. It contains the text 'monreseau.lan' and has a blue checkmark icon on the right.
- The second field is labeled 'Adresse électronique recevant les courriers électroniques à destination du compte root'. It contains the text 'admin@monreseau.lan' and has a small icon on the right.

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 réécrits 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

The screenshot shows the 'Relai des messages' configuration window. It has a title bar with the text 'Relai des messages'. The main area contains two input fields:

- The first field is labeled 'Router les courriels par une passerelle SMTP'. It has a dropdown menu with 'oui' selected and a blue checkmark icon on the right.
- The second field is labeled 'Passerelle SMTP'. It contains the text 'smtp.ac-dijon.fr' and has a small icon on the right.

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



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

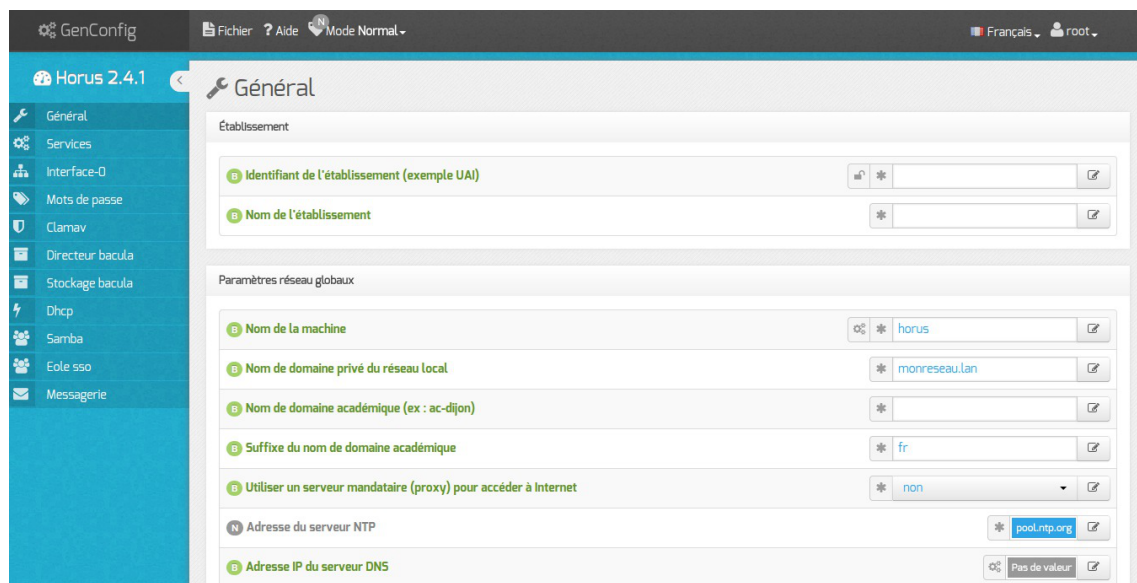
Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.

2. Configuration en mode normal

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

- Général ;
- Services ;
- Interface-0 (configuration de l'interface réseau) ;
- Mots de passe ;
- Clamav (configuration de l'anti-virus) ;
- Directeur bacula ;
- Stockage bacula ;
- Annuaire ;
- Dhcp * ;
- Esu * ;
- Samba ;
- Onduleur * ;
- Applications web * ;
- Eole-ss0 ;
- Messagerie .

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



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

Établissement

B Identifiant de l'établissement (exemple UAI)

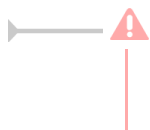
B Nom de l'établissement

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.366] 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

Paramètres réseau globaux

B Nom de la machine

B Nom de domaine privé du réseau local

B Nom de domaine académique (ex : ac-dijon)

B Suffixe du nom de domaine académique

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

Cette information est découpée en plusieurs champs :

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

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

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

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

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

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

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

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

Proxy

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

| | | |
|---|--------|--|
| Utiliser un serveur mandataire (proxy) pour accéder à Internet | * oui | |
| Nom ou adresse IP du serveur proxy | * | |
| Port du serveur proxy | * 3128 | |

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

| | | |
|----------------------------------|-------------------------------------|--|
| Adresse IP du serveur DNS | 192.168.232.2 192.168.122.1 8.8.8.8 | |
| Fuseau horaire du serveur | Europe/Paris | |

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.363].

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

NTP

A configuration field titled "Adresse du serveur NTP" with a search icon on the left and a dropdown menu on the right showing "pool.ntp.org" with a copy icon.

Une valeur par défaut est attribuée pour le serveur de temps NTP^[p.367]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

 A configuration field titled "Mise à jour" with a search icon on the left and a dropdown menu on the right showing "eole.ac-dijon.fr" and "ftp.crihan.fr" with a copy icon.

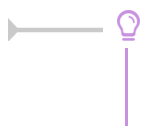
Il est possible de définir une autre adresse pour le serveur de mise à jour EOLE que celle fournie par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Voir aussi...

Les différentes mises à jour

2.2. Onglet Services

L'onglet **Services** permet d'activer et de désactiver une partie des services proposés par le module. Suivant le module installé et le mode utilisé pour la configuration la liste des services activables ou désactivables est très différente.



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

 A configuration page titled "Services" with a gear icon. Under the "Configuration" section, there is a field "Activer le serveur DHCP" with a dropdown menu set to "non" and a copy icon.

Vue de l'onglet Services

En mode basique seul le service DHCP est activable.

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

| | | |
|---|----------|---|
| Activer l'anti-virus ClamAV | * oui | ✎ |
| Activer la sauvegarde du serveur | * oui | ✎ |
| Activer le support de stockage de la sauvegarde | ⚙️ * oui | ✎ |
| Activer le serveur DHCP | * non | ✎ |
| Utiliser le logiciel ESU | * non | ✎ |
| Activer xinetd pour InterBase | * non | ✎ |
| Activer la gestion de l'onduleur NUT | * non | ✎ |
| Activer le serveur web Apache | * non | ✎ |
| Utiliser un serveur EoleSSO | * local | ✎ |
| Activer le serveur de bases de données MySQL | * oui | ✎ |
| Activer le serveur d'impression CUPS | * oui | ✎ |
| Activer l'accès FTP | * oui | ✎ |
| Activation du service horus_frontend | * non | ✎ |

Vue de l'onglet Services en mode normal

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

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

- l'anti-virus ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le logiciel ESU^[p.364] ;
- Interbase^[p.366] ;
- le serveurs web ;
- l'authentification unique SSO^[p.370] ;
- les bases de données MySQL ;
- le serveur d'impression avec CUPS ;
- l'accès FTP ;
- l'interface de gestion des utilisateurs Horus.

2.3. Onglet Interface-0

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

Vue de l'onglet Interface-n

Configuration de l'interface

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

Administration distante sur l'interface

Autoriser les connexions SSH * oui

Adresse IP réseau autorisée pour les connexions SSH

Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

Masque du sous réseau pour les connexions SSH * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH

Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) * oui

Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

Masque du sous réseau pour administrer le serveur * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.370] 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.

Administration distante sur l'interface

Autoriser les connexions ssh oui

Adresse IP réseau autorisée pour les connexions ssh

Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

Masque du sous réseau pour les connexions ssh * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions ssh

Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) oui

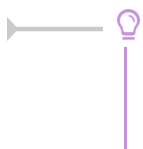
Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

Masque du sous réseau pour administrer le serveur * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

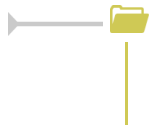
Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour...`



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

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

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



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

Configuration des alias sur l'interface

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

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

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

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

Configuration des VLAN sur l'interface

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

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

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

2.4. Onglet 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).

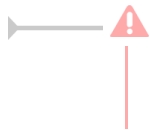
Cette contrainte sera à terme propagée à toutes les interfaces fournissant cette fonctionnalité (EAD, portail...). La longueur minimale est paramétrable de 3 à 12 caractères.

Nombre minimum de classes de caractères

Cette variable permet de choisir le nombre minimum de classes de caractères^[p.362] 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.

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

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

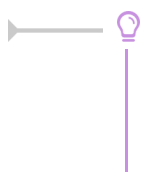
<http://www.clamav.net>

Activation de l'anti-virus

Par défaut, le service est activé sur le module et l'anti-virus est actif uniquement sur le service FTP.

Sur le module Horus il est possible d'activer l'anti-virus sur :

- le service SMB ;
- le service de messagerie.



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

Activation de l'anti-virus sur SMB

Le service, basé sur le logiciel Scannedonly^[p.369], n'est plus activé par défaut sur les modules EOLE 2.5. Il est possible de l'activer en passant la variable `Activer l'anti-virus temps réel sur SMB` à `oui` dans l'onglet **Clamav**.

La `Durée de conservation des fichiers en quarantaine` permet de fixer la durée de

quarantaine avant la purge des fichiers. Le durée fixée par défaut est de 20 jours.

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.

Activation de l'anti-virus sur FTP

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

A configuration field with a label "Activer l'anti-virus temps réel sur FTP" and a dropdown menu currently set to "oui".

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.

A configuration field with a label "Activer l'anti-virus sur la messagerie" and a dropdown menu currently set to "oui".

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://cgi.clamav.net/sendvirus.cgi>

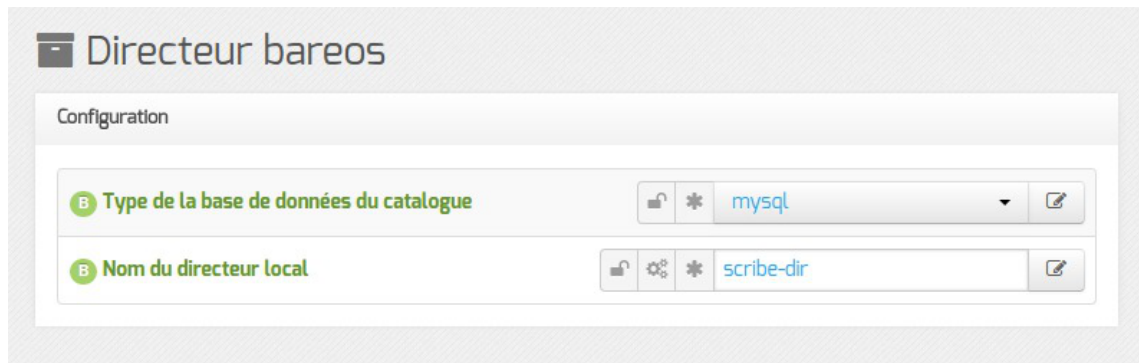
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

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.369] comme étant des faux positifs.

2.6. Onglet Directeur bareos



Vue de l'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.

Directeur bareos

Configuration

B Type de la base de donnée du catalogue * mysql

B Nom du directeur local * scribe-dir

N Période de rétention des sauvegardes complètes * 6

N Unité de valeur pour la rétention des sauvegardes complètes * months

N Période de rétention des sauvegardes différentielles * 5

N Unité de valeur pour la rétention des sauvegardes différentielles * weeks

N Période de rétention des sauvegardes incrémentales * 10

N Unité de valeur pour la rétention des sauvegardes incrémentales * days

Gestion du stockage

N Le gestionnaire du stockage est local * oui

Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention^[p.363] des différents espaces de stockage (totale, différentielle et incrémentale).

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

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



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

Pour cela, voici un exemple de configuration :

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

Avec la politique de sauvegarde suivante :

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

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



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

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

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

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

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

```
# bareosregen.sh
La régénération 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.

2.7. Onglet Stockage bareos

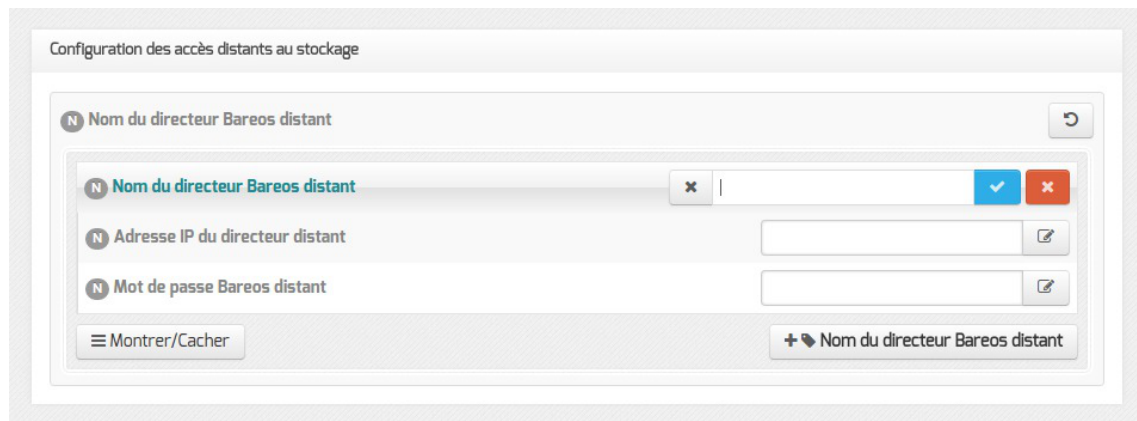
Dans l'onglet **Stockage bareos** il est possible de choisir un nom de serveur de stockage et d'autoriser des directeurs distants à se connecter au présent serveur de stockage.



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 Bacula 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

2.8. Onglet Annuaire

Sur le module Horus l'annuaire OpenLDAP est local.



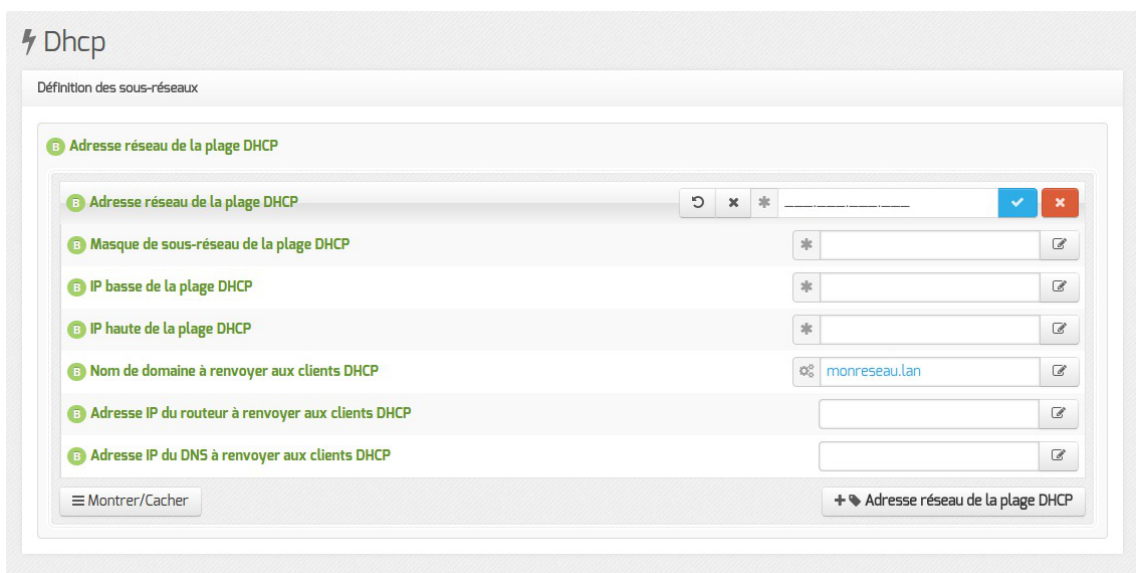
Lorsque l'annuaire est configuré comme étant local, l'onglet propose 2 paramètres :

- 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`.

2.9. 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.



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

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**.

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

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.364] 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.363], l'adresse à préciser dans le cas du mode deux cartes sera l'adresse IP du routeur et donc l'adresse IP de l'Interface-1 (eth1).



Sur le module AmonEcole, l'adresse IP du DNS à renvoyer correspond à celle renseignée

dans Adresse IP pour le proxy (adresse ip eth1 proxy link) de l'onglet Interface-1 de l'interface de configuration du module.

2.10. 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.



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

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

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

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

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



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

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

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



Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet `Interface-1` (variable : `adresse_ip_eth1_proxy_link`).



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.361] tels que sauvegardés.



Vous pouvez restaurer la base de registre de la station en appliquant des fichiers `.REG`^[p.361] tels que celui fourni par l'archive suivante : `ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip`

2.11. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC^[p.369]) 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.).

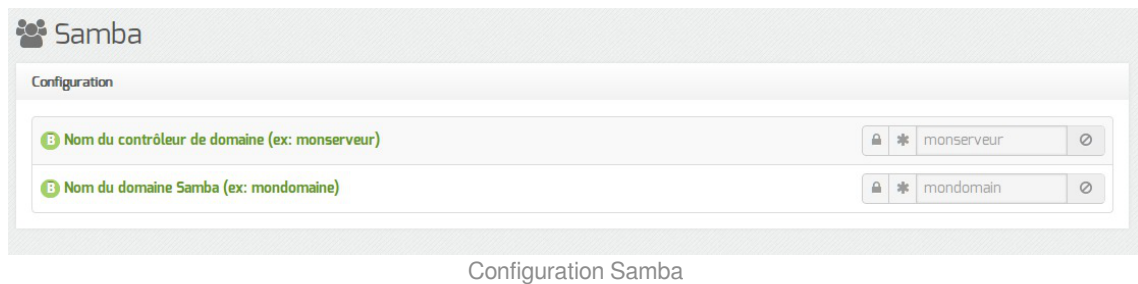
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

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.367]) 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>

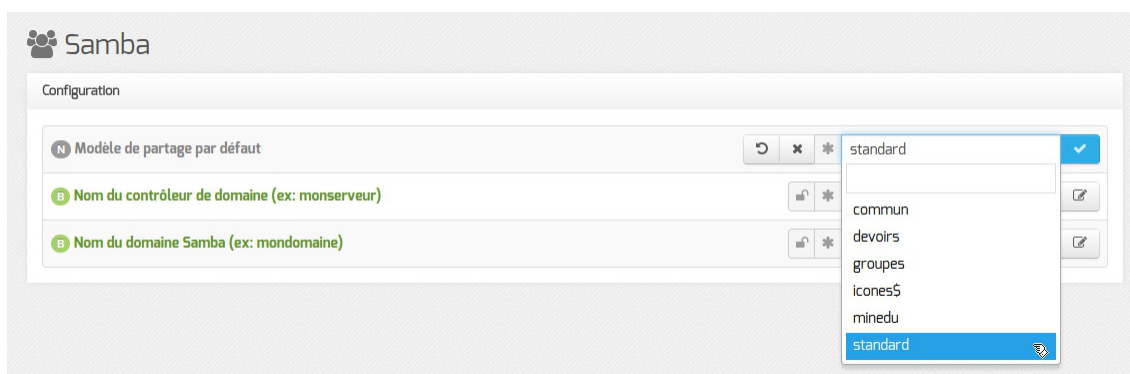
Fichiers invisibles sur les partages

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`) ;
- `$recycle.bin` : les fichiers `$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 fichiers `.scanned:*` générés par Scannedonly^[p.369] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

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.tpl`

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

Il existe déjà plusieurs modèles à disposition :

- `standard`
héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe
- `commun`
héritage des permissions, accès en écriture, accessible à tous en lecture et en écriture, accès anonyme (guest)
- `devoirs`
héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `groupes`
héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `icones$`

caché dans le voisinage réseau, accès anonyme (guest)

- `minedu`

héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe, nom de fichier et répertoire en minuscules

Anti-virus temps réel

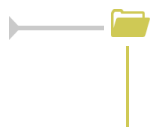
Afin de limiter la propagation des virus à travers le réseau, une surveillance anti-virus temps réel est active sur les partages.

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

2.12. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT^[p.367]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

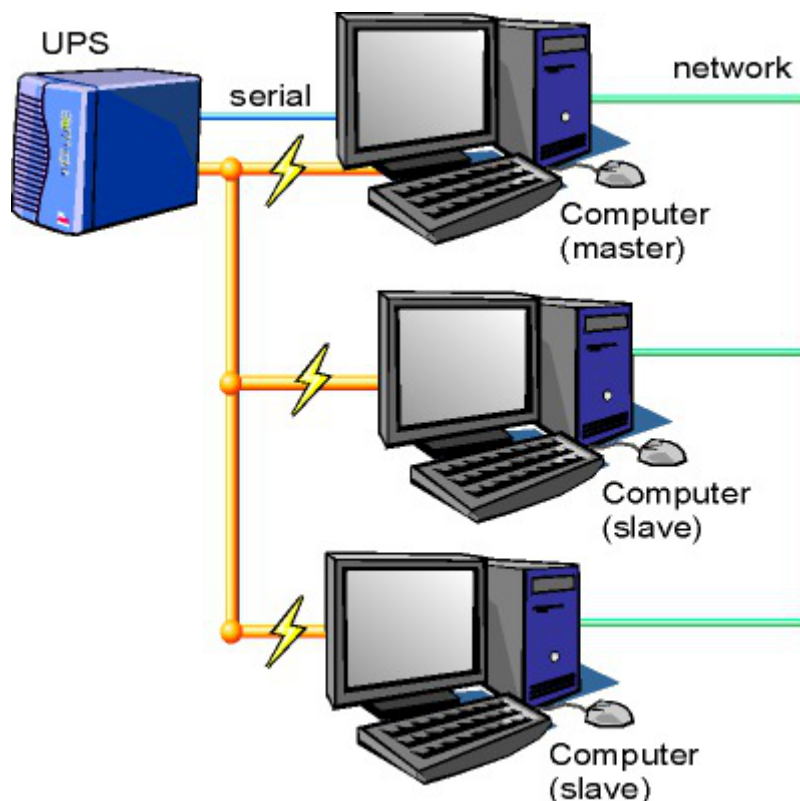


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - <http://ovanhoof.developpez.com/upsusb/>

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

<http://www.networkupstools.org/>

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

<http://www.networkupstools.org/stable-hcl.html>



Pour connaître la version de NUT qui est installée sur le module :

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

ou encore :

```
# apt-show-versions nut
```

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

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

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

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

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

Vue de l'onglet Onduleur

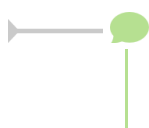
Si l'onduleur est branché directement sur le module il faut laisser la variable Configuration sur un serveur maître à oui, cliquer sur le bouton + Nom de l'onduleur et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître

Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ Nom pour l'onduleur.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante Pilote de communication de l'onduleur et éventuellement préciser le Port de communication si l'onduleur n'est pas USB.

Les champs Numéro de série de l'onduleur, Productid de l'onduleur et Upstype de l'onduleur sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.



Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost | grep <nom_variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;

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

La majorité des onduleurs USB sont détectés automatiquement.



Attention, seul le premier onduleur sera surveillé.

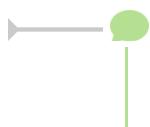
Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave à se connecter avec cet utilisateur.

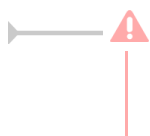
Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)



Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.



Chaque utilisateur doit avoir un nom différent.
Les noms `root` et `localmonitor` sont réservés.



Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf` ou consulter la page web suivante : <http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html>

Configurer un serveur esclave

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

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

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

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

Exemple de configuration



Sur le serveur maître :

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



Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

2.13. 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`.

The screenshot shows the 'Applications web' configuration page. It contains the following settings:

- Nom de domaine des applications web (sans http://)**: `monetab.ac-academie.fr`
- Application web par défaut (redirection)**: `/webmail`
- Le serveur web est derrière un reverse proxy**: `oui`
- Adresse IP du serveur reverse proxy**: `10.0.142.129`
- Activer phpMyAdmin (administration des bases MySQL)**: `non`

L'onglet `Applications web` permet un réglage minimum pour le fonctionnement 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.

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>/` pointerait vers `http://<adresse serveur>/webmail/`

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

L'onglet `Applications web` permet aussi d'activer/désactiver toutes les applications web EOLE installées sur le module.

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`.

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

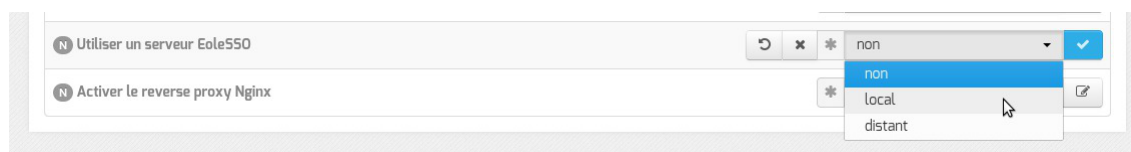
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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`.



Activation du serveur SSO dans l'interface de configuration du module

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.

The screenshot shows the 'Configuration' page for 'Eole sso'. It contains several configuration fields:

- Nom de domaine du serveur d'authentification SSO: [Empty]
- Port utilisé par le service EoleSSO: 8443
- Adresse du serveur LDAP utilisé par EoleSSO: localhost (with a dropdown menu open showing 'Adresse du serveur LDAP utilisé par EoleSSO')
- Port du serveur LDAP utilisé par EoleSSO: 389
- Chemin de recherche dans l'annuaire: o=gouv,c=fr
- Libellé à présenter aux utilisateurs en cas d'homonymes: Annuaire de amon.monreseau.lar
- Informations supplémentaires dans le cadre d'information sur les homonymes: [Empty]
- Utilisateur de lecture des comptes LDAP (nécessaire pour la fédération): cn=reader,o=gouv,c=fr
- Fichier de mot de passe de l'utilisateur de lecture: /root/.reader
- Attribut de recherche des utilisateurs: uid
- Information LDAP supplémentaires (applications): non
- Adresse du serveur SSO parent: [Empty]
- Port du serveur SSO parent: 8443
- Nom d'entité SAML du serveur eole-ssso (ou rien): [Empty]
- Gestion de l'authentification OTP (RSA SecurID): non
- Chemin du certificat SSL (ou rien): [Empty]
- Chemin de la clé privée liée au certificat SSL (ou rien): [Empty]
- Chemin de l'autorité de certification (ou rien): [Empty]
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200
- CSS par défaut du service SSO (sans le .css): [Empty]
- Cacher le formulaire lors de l'envoi des informations de fédération: non

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.

The screenshot shows the 'Configuration' page for 'Eole sso' with the following settings:

- Nom de domaine du serveur d'authentification SSO: 192.168.0.31
- Port utilisé par le service EoleSSO: 8443
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200

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.368] si disponible (*voir plus loin*).



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

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

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

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

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

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

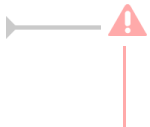
- [Utilisateur de lecture des comptes ldap](#) : renseignez son *dn* complet dans l'annuaire
- [fichier de mot de passe de l'utilisateur de lecture](#) : entrez le chemin d'un fichier où vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur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

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 essaiera 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.372] 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.370] de la société EMC (précédemment RSA).

Pour cela il faut :

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

Des champs supplémentaires apparaissent :

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

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation^[p.365] 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'autres types de serveurs compatibles avec le protocole SAML^[p.369] (version 2).

Nom d'entité SAML du serveur eole-ssso (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.168]

2.15. 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

The screenshot shows a configuration window titled 'Messagerie' with a sub-section 'Serveur d'envoi/réception (SMTP)'. It contains two input fields:

- The first field is labeled 'Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr)' and contains the value 'monreseau.lan'.
- The second field is labeled 'Adresse électronique recevant les courriers électroniques à destination du compte root' and contains the value 'admin@monreseau.lan'.

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 réécrits et envoyés à l'adresse électronique d'envoi du compte root.

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

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



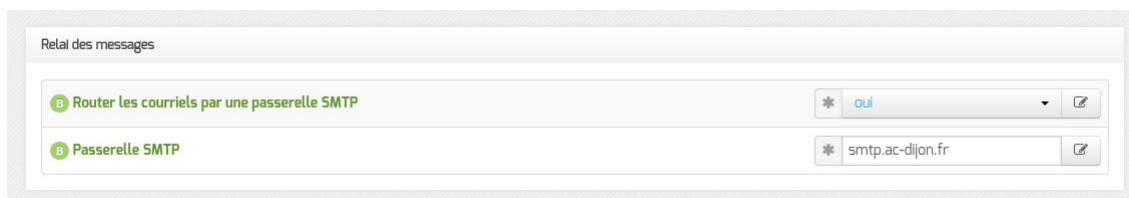
Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.

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

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

Relai des messages



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



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

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



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS^[p.371] pour l'envoi de message. Si la passerelle SMTP^[p.370] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS^[p.370] (port 25) ou non (port 465).

3. Configuration en mode expert

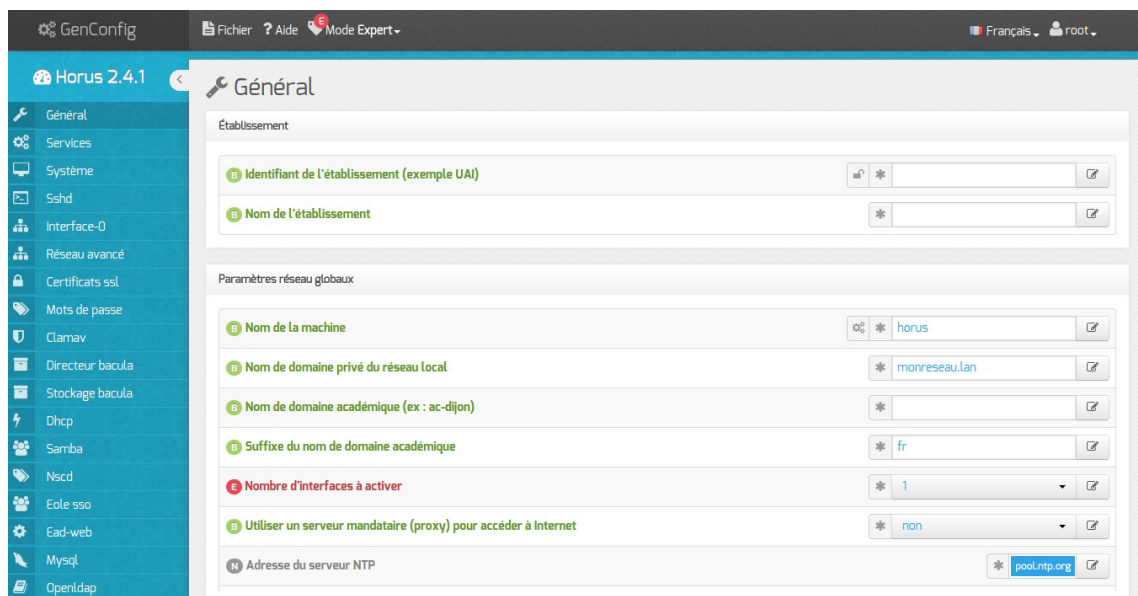
Certains onglets et certaines options ne sont disponibles qu'après avoir activé le mode expert de l'interface de configuration du module.

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

- Général ;
- Services ;
- Système ;
- Sshd ;
- Logs * ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-n (configuration de l'interface réseau) ;
- Réseau avancé ;
- Certificat ssl ;
- Eoledb ;
- Mots de passe ;
- Clamav (configuration de l'anti-virus) ;

- Directeur bacula ;
- Stockage bacula ;
- Annuaire ;
- Dhcp * ;
- Tftp * ;
- Esu * ;
- Samba ;
- Nscd ;
- Onduleur * ;
- Applications web * ;
- Apache * ;
- Eole-sso ;
- Ead-web ;
- Mysql ;
- Openldap ;
- Cups ;
- Proftpd ;
- Messagerie ;
- Eoleflask .

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



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

| Établissement | |
|---|------------------|
| B Identifiant de l'établissement (exemple UAI) | 0000G12345 |
| B Nom de l'établissement | MonEtablissement |

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.366] 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

| Paramètres réseau globaux | |
|--|---------------|
| B Nom de la machine | harpocrate |
| B Nom de domaine privé du réseau local | monreseau.lan |
| B Nom de domaine académique (ex : ac-dijon) | ac-dijon |
| B Suffixe du nom de domaine académique | 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 EOLE peut avoir de 1 à 5 cartes réseaux.

Nombre d'interfaces à activer: 1

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

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

Proxy

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

Utiliser un serveur mandataire (proxy) pour accéder à Internet: oui

Nom ou adresse IP du serveur proxy:

Port du serveur proxy: 3128

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

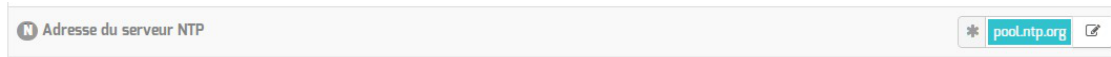
Adresse IP du serveur DNS: 192.168.232.2 192.168.122.1 8.8.8.8

Fuseau horaire du serveur: Europe/Paris

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.363].

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

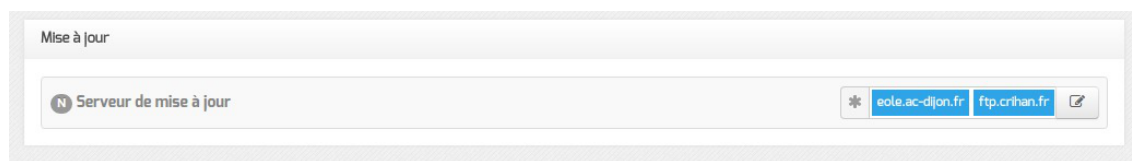
NTP



A screenshot of a configuration field titled "Adresse du serveur NTP". The field contains the text "pool.ntp.org" and has a small icon to its right.

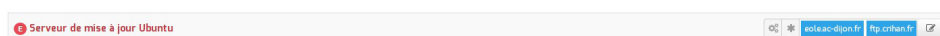
Une valeur par défaut est attribuée pour le serveur de temps NTP^[p.367]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour



A screenshot of a configuration field titled "Mise à jour". The field contains the text "eole.ac-dijon.fr ftp.crihan.fr" and has a small icon to its right.

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.

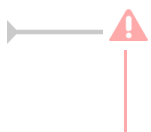


Il est possible de définir d'autres adresses pour le serveur de mise à jour Ubuntu que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Serveur de mise à jour Envole



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



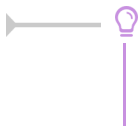
Les dépôts de paquets définis pour Envole ne sont pris en compte par les procédures de mise à jour uniquement si le serveur web apache est activé sur le module.

Voir aussi...

Les différentes mises à jour

3.2. Onglet Services

L'onglet **Services** permet d'activer et de désactiver une partie des services proposés par le module. Suivant le module installé et le mode utilisé pour la configuration la liste des services activables ou désactivables est très différente.



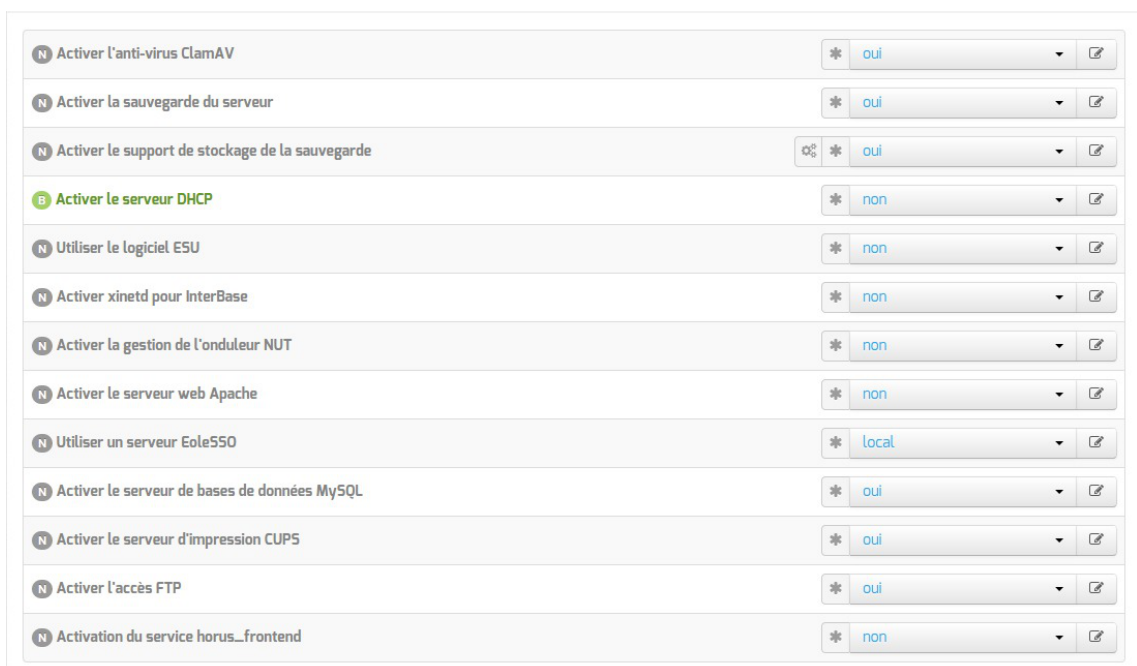
Le principe est toujours le même, l'activation d'un service va, la plupart du temps, ajouter un onglet de configuration propre au service.



Vue de l'onglet Services

En mode basique seul le service DHCP est activable.

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.

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

- l'anti-virus ;
- la sauvegarde ;
- le support de stockage de la sauvegarde ;
- le logiciel ESU^[p.364] ;

- Interbase^[p.366] ;
- le serveurs web ;
- l'authentification unique SSO^[p.370] ;
- les bases de données MySQL ;
- le serveur d'impression avec CUPS ;
- l'accès FTP ;
- l'interface de gestion des utilisateurs Horus.

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

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

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

3.3. Onglet Système

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

Paramétrage de la console

- Activer l'auto-complétion étendue sur la console : l'auto-complétion facilite l'utilisation de la ligne de commande mais peut ralentir son affichage, elle est désactivée par défaut ;
- Temps d'inactivité avant déconnexion bash : si aucune activité n'est constatée sur la console utilisateur pendant cette durée, sa session est automatiquement coupée, avec le message : `attente de données expirée : déconnexion automatique`. La valeur `0` permet de désactiver cette fonctionnalité.

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 réglée plus finement à l'aide des paramètres suivants :

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

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

➤ Les mots de passe (cf. Les mots de passe)

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

3.4. Onglet Sshd : Gestion SSH avancée



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

Ils permettent :

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



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

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

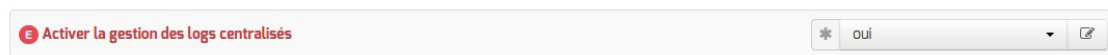


Par défaut les groupes Unix autorisés sont `root` et `adm`.

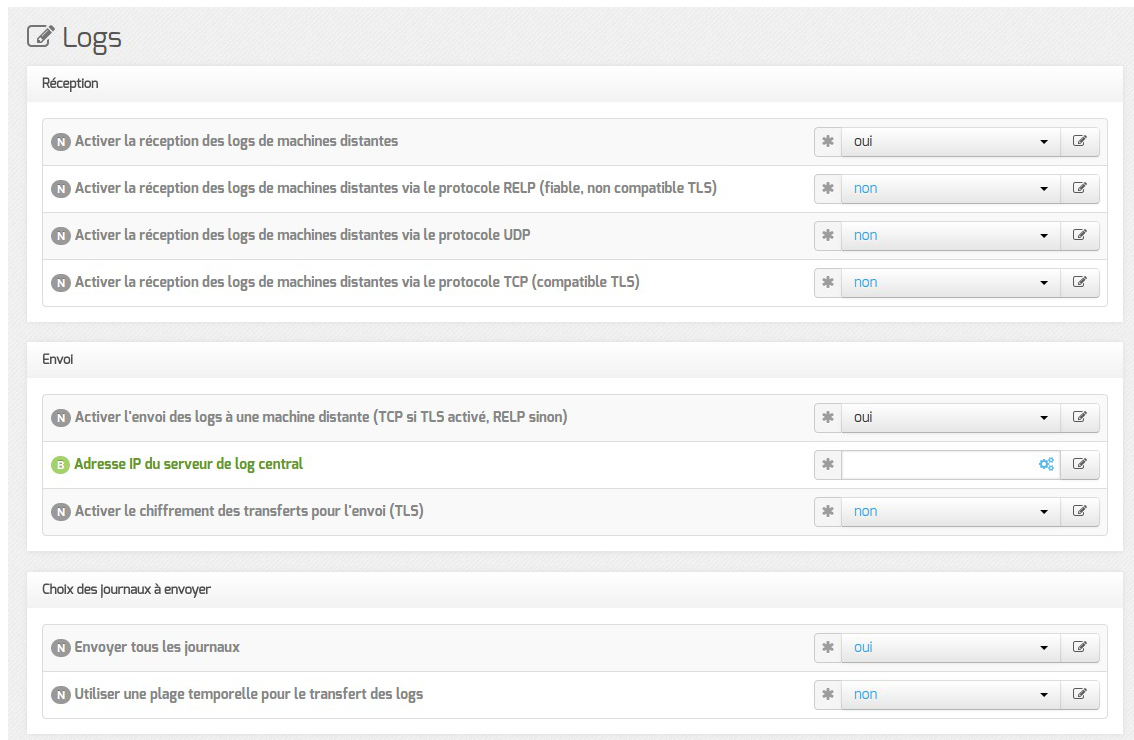
3.5. Onglet Logs : Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog^[p.373]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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



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



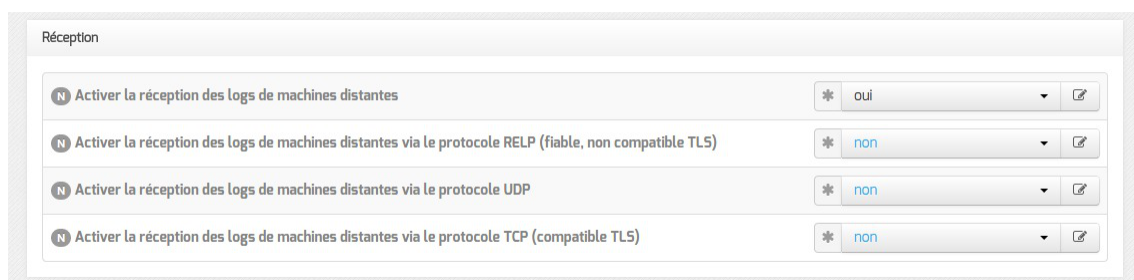
Vue de l'onglet Logs

Les options de cet onglet sont répartis en plusieurs sections :

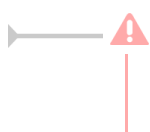
- la configuration de la réception des logs permet de spécifier les protocoles de communication entre des machines distantes émettrices identifiées par leur adresse IP et le poste configuré ;
- la configuration de l'envoi des logs permet de spécifier l'adresse de la machine distante réceptrice. Le protocole (TCP ou RELP) utilisé est contraint par l'activation ou non du chiffrement (TLS) ;
- 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 est possible de choisir jusqu'à 3 protocoles de réception : RELP, UDP et TLS over TCP.



L'activation des protocoles ouvre les ports adéquats sur le module.



Lorsque vous pouvez choisir les protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI.

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).

⚠ Lorsque vous pouvez choisir les protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI.

Choix des journaux à envoyer

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

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

3.6. Onglet Interface-0

Configuration de l'interface

Configuration de l'interface

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

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

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



Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant L'interface réseau de la zone est un bridge à oui. Il faut également saisir le nom du pont dans le champ Nom de l'interface réseau de la zone.



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

Mode de connexion pour l'interface

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

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

Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseaux, 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 100Mbps/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 10Mbps/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_\(ethernet\)](http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet)).

Administration à distance

Administration distante sur l'interface

Autoriser les connexions SSH * oui

Adresse IP réseau autorisée pour les connexions SSH

Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

Masque du sous réseau pour les connexions SSH * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH

Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) * oui

Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

Masque du sous réseau pour administrer le serveur * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.370] 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.

Administration distante sur l'interface

Autoriser les connexions ssh oui

Adresse IP réseau autorisée pour les connexions ssh

Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

Masque du sous réseau pour les connexions ssh * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions ssh

Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) oui

Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

Masque du sous réseau pour administrer le serveur * 0.0.0.0

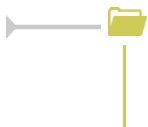
Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

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



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

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



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

Configuration des alias sur l'interface

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

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

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

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

Configuration des VLAN sur l'interface

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

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

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

3.7. Onglet Interface-n

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

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

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



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

Configuration de l'interface

Configuration de l'interface

B Adresse IP de l'interface *

B Masque de sous réseau de l'interface * 255.255.255.0

Configuration de l'interface

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

En mode expert quelques variables supplémentaires sont disponibles.

E Nom de l'interface réseau * eth0

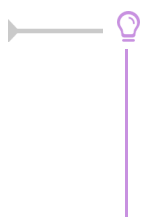
E Nom de l'interface réseau de la zone * eth0

E L'interface réseau de la zone est un bridge * non

E Mode de connexion pour l'interface *

Nom de l'interface réseau

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



Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier `/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.



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

Mode de connexion pour l'interface

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

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

Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseaux, 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 100Mbps/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 10Mbps/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_\(ethernet\)](http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet)).

Administration à distance

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

☰ Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH

B Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) * oui

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur ↻ x * 255.255.255.255 ✓

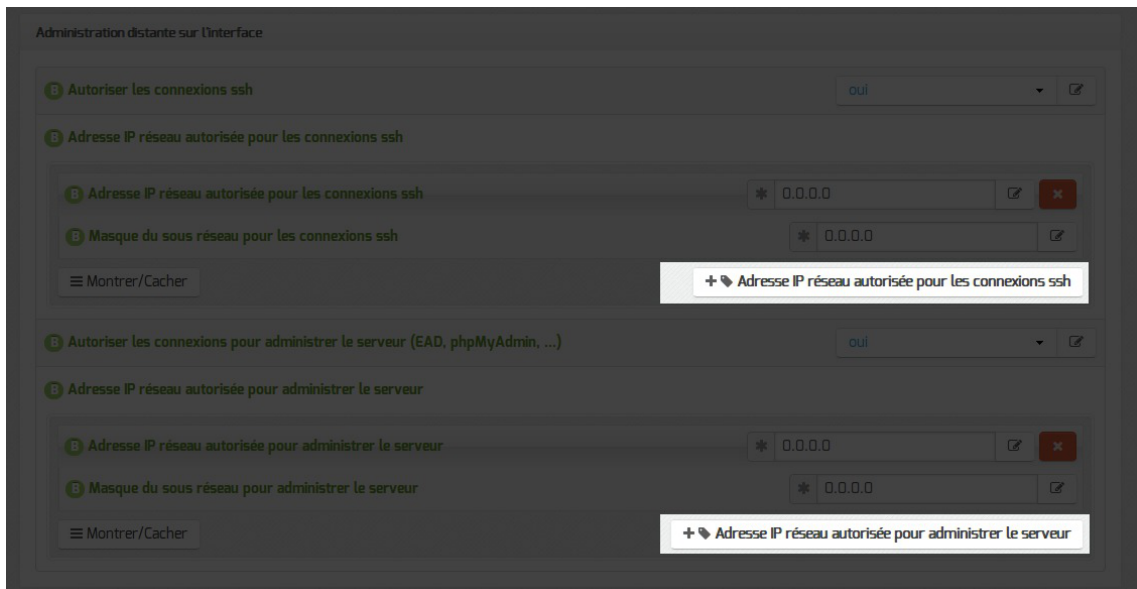
☰ Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.370] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



Le masque réseau d'une station isolée est 255.255.255.255.

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



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

Configuration des alias sur l'interface

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

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

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

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

Configuration des VLAN sur l'interface

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

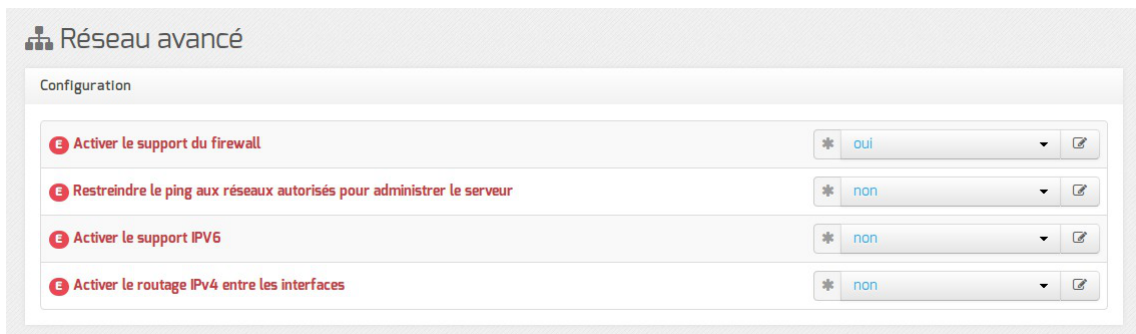
Pour cela, il faut activer son support (Activer le support des VLAN sur l'interface à oui) et ajout d'un numéro identifiant du VLAN avec le bouton + Numéro d'identifiant du VLAN) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

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

3.8. Onglet Réseau avancé

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

Configuration IP



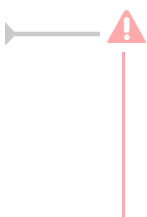
The screenshot shows the 'Réseau avancé' configuration window. It contains a 'Configuration' section with four settings, each with a red 'e' icon and a dropdown menu:

- Activer le support du firewall**: dropdown set to 'oui'
- Restreindre le ping aux réseaux autorisés pour administrer le serveur**: dropdown set to 'non'
- Activer le support IPV6**: dropdown set to 'non'
- Activer le routage IPv4 entre les interfaces**: dropdown set to 'non'

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

La valeur par défaut de la variable Restreindre le ping aux réseaux autorisés pour administrer le serveur est à oui par défaut mais cette restriction peut être levée en passant la variable à non.

Sur les modules disposant de la fonctionnalité serveur de fichiers comme Scribe et Horus, cette restriction est déjà levée puisque la variable est par défaut à non.



Il est recommandé de laisser la variable Restreindre le ping aux réseaux autorisés pour administrer le serveur à non sur les serveurs disposant de la fonctionnalité serveur de fichiers, principalement pour que les postes clients puissent fonctionner correctement.

La variable Activer le support IPV6 est par défaut à non et est utilisée pour désactiver explicitement le support de l'IPv6 dans la configuration de certains logiciels (BIND, Proftpd).

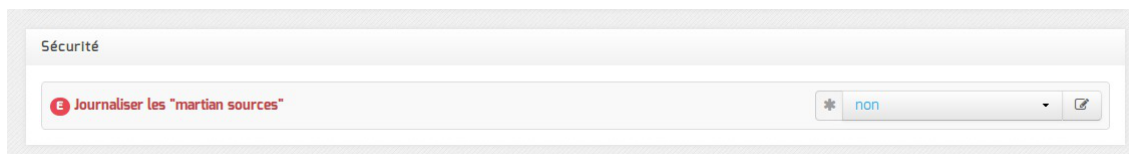
Le support de l'IPv6^[p.366] peut être activé en passant la variable Activer le support IPV6 à oui mais sa prise en charge ne se sera faite qu'au niveau du noyau.

Si la variable Activer le routage IPv4 entre les interfaces est à oui, alors le routage IPv4 est activé au niveau du noyau (`/proc/sys/net/ipv4/ip_forward` passe à 1)

L'activation du support IPv6 entraîne l'apparition de la variable : Activer le routage IPV6 entre les interfaces.

Si cette dernière est à `oui` le routage IPv6 est activé au niveau du noyau (`/proc/sys/net/ipv6/conf/all/forwarding` passe à `1`).

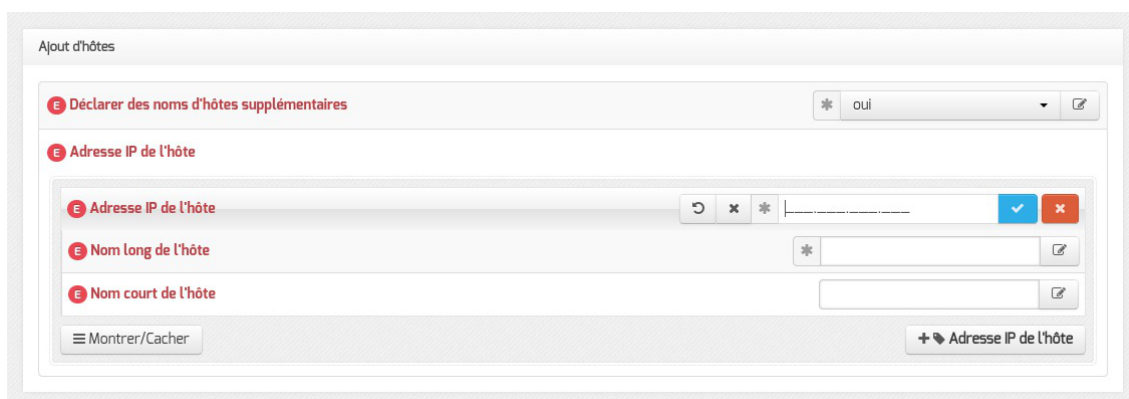
Sécurité



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

Par défaut, l'anti-spoofing^[p.361] est activé sur l'interface-0 des modules EOLE. Si plusieurs interfaces réseaux sont déclarées alors 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



En passant la variable `Déclarer des noms d'hôtes supplémentaires` à `oui` il est possible 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`.

Sur un module avec serveur DNS (module Amon), pour que le DNS puisse résoudre le nom, il faut que le suffixe DNS du nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

Si ce n'est pas le cas, il faudra déclarer un nom de domaine local supplémentaire dans l'onglet `Réseau avancé` pour permettre au serveur DNS de résoudre ce nom d'hôte.

Le champ `Nom court de l'hôte` est optionnel.

Ajout de routes statiques

Ajout de routes statiques

Ajouter des routes statiques * oui

Adresse IP ou réseau à ajouter dans la table de routage

Adresse IP ou réseau à ajouter dans la table de routage

Masque de sous réseau (mettre à 255.255.255.255 si adresse host) *

Adresse IP de la passerelle pour accéder à ce réseau *

Interface réseau reliée à la passerelle *

Autoriser ce réseau à utiliser les DNS du serveur * oui

Autoriser ce réseau à utiliser les DNS des zones forward additionnelles * oui

Montrer/Cacher

+ Adresse IP ou réseau à ajouter dans la table de routage

Ce bloc de paramètres permet d'ajouter, manuellement, des routes afin d'accéder à des adresses ou à des plages d'adresses par un chemin différent de celui par défaut (défini par le routeur par défaut).

Après avoir passé la variable `Ajouter des routes statiques` à `oui` il faut ajouter les paramètres suivants :

- `Adresse IP ou réseau à ajouter dans la table de routage` : permet de définir l'adresse de sous-réseau (ou l'adresse de l'hôte) vers lequel le routage doit s'effectuer ;
- `Masque de sous réseau` : permet de définir le masque du réseau défini ci-dessus (s'il s'agit d'une machine seule, il faut mettre l'adresse du masque à 255.255.255.255) ;
- `Adresse IP de la passerelle pour accéder à ce réseau` : permet de renseigner l'adresse de la passerelle permettant d'accéder au sous-réseau ou à l'hôte défini ci-dessus ;
- `Interface réseau reliée à la passerelle` : permet d'associer la route à une interface donnée. Ce champ, de type liste déroulante, comporte un certain nombre d'interfaces pré-définies. Il est possible d'en ajouter une en tapant son nom (par exemple : `ppp0`) ;
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Configuration du MTU

Configuration du MTU

Désactiver le path MTU discovery, le bit DF est positionné à 0 * non

Valeur du MTU pour l'interface eth0 : rien = valeur par défaut de l'interface

Valeur du MTU pour l'interface ppp0 : rien = valeur par défaut de l'interface

La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.367] (`/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.365]

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.367] 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.

Configuration de la "neighbour table"

| Paramètre | Valeur |
|---|--------|
| Neighbour table overflow stop culling limit | 128 |
| Neighbour table overflow soft limit | 512 |
| Neighbour table overflow hard limit | 1024 |

Les variables ipv4_neigh_default_gc_thresh1, ipv4_neigh_default_gc_thresh2 et ipv4_neigh_default_gc_thresh3 servent à gérer la façon dont la table ARP évolue :

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;
- **gc_thresh2** : seuil qui, s'il est dépassé depuis un certain temps (5 secondes par défaut), déclenche le recyclage des entrées de la table qui ne sont plus utilisées ;
- **gc_thresh3** : seuil au-delà duquel le recyclage est immédiatement déclenché pour contenir la taille de la table.

Test de l'accès distant

| | |
|---|-------------------------------|
| Domaine utilisé pour le test de l'accès distant | bp-eole.ac-dijon.fr google.fr |
|---|-------------------------------|

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.

3.9. Onglet Certificats ssl : gestion des certificats SSL

La gestion des certificats a été standardisée pour faciliter leur mise en œuvre. Ils sont désormais gérés par l'intermédiaire des outils Creole.

Certificats par défaut

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

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

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

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

Détermination du nom de serveur (commonName) dans le certificat

Le nom du sujet auquel le certificat s'applique est déterminé de la façon suivante (important pour éviter les avertissements dans les navigateurs) :

- si la variable `ssl_server_name` est définie dans l'interface de configuration du module (onglet `Certifs ssl -> Nom DNS du serveur`), elle est utilisée comme nom de serveur dans les certificats ;
- sinon, si un nom de domaine académique est renseigné, le nom sera : `nom_machine.numero_etab.nom_domaine_academique` (exemple : `amon_monetab.0210001A.mon_dom_acad.fr`) ;
- le cas échéant, on utilise : `nom_machine.numero_etab.debut(nom_academie).min(ssl_country_name)` (exemple : `amon_monetab.0210001A.ac-dijon.fr`).

Mise en place d'un certificat particulier

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

- Nom long du certificat SSL par défaut (server_cert) : chemin d'un certificat au format PEM à utiliser pour les services ;
- Nom long de la clé privée du certificat SSL par défaut (server_key) : chemin de la clé privée correspondante (éventuellement dans le même fichier).

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

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

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

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

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

⚠ Le répertoire `/etc/ssl/local_ca/` n'accueille que des certificats CA.

Création de nouveaux certificats

Le script `/usr/share/creole/gen_certif.py` permet de générer rapidement un nouveau certificat SSL.

🔗 Génération d'un certificat avec `gen_certif.py`

```
root@eole:~# /usr/share/creole/gen_certif.py -fc
/etc/ssl/certs/test.crt
Generation du certificat machine
* Certificat /etc/ssl/certs/test.crt généré
```

Obtention d'un certificat signé par l'IGC de l'Éducation nationale

Étapes à suivre :

1. récupérer la requête du certificat située dans le répertoire `/etc/ssl/req/` : `eole.p10` ;
2. se connecter sur l'interface web de demande des certificats et suivre la procédure ;
3. récupérer le certificat depuis l'interface (copier/coller dans un fichier) ;
4. copier le fichier dans le répertoire `/etc/ssl/certs/`.

⚠ Seuls les ISR/OSR des académies sont accrédités pour effectuer les demandes.

Certificats intermédiaires

En attendant que la prise en compte des certificats intermédiaires soit automatisée pour l'ensemble des services de base (fixme #13362 [<https://dev-eole.ac-dijon.fr/issues/13362>]), les manipulations nécessaires pour éviter des avertissements dans les navigateurs sont documentées dans la page wiki suivante : https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Gestion_certificats

3.10. Onglet Eoledb : Gestion des bases de données

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

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

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



Pour le moment, la version publiée d'EoleDB ne gère que les bases de données MySQL.

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

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

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

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

Voir aussi...

Gestion des bases de données avec EoleDB [p.189]

3.11. 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`).

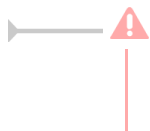
Cette contrainte sera à terme propagée à toutes les interfaces fournissant cette fonctionnalité (EAD, portail...). La longueur minimale est paramétrable de 3 à 12 caractères.

Nombre minimum de classes de caractères

Cette variable permet de choisir le nombre minimum de classes de caractères^[p.362] 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.

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

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

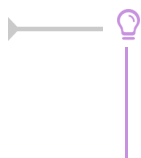
<http://www.clamav.net>

Activation de l'anti-virus

Par défaut, le service est activé sur le module et l'anti-virus est actif uniquement sur le service FTP.

Sur le module Horus il est possible d'activer l'anti-virus sur :

- le service SMB ;
- le service de messagerie.



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

| plus visible.

Activation de l'anti-virus sur SMB

Le service, basé sur le logiciel Scannedonly^[p.369], n'est plus activé par défaut sur les modules EOLE 2.5. Il est possible de l'activer en passant la variable Activer l'anti-virus temps réel sur SMB à oui dans l'onglet Clamav.

La Durée de conservation des fichiers en quarantaine permet de fixer la durée de quarantaine avant la purge des fichiers. La durée fixée par défaut est de 20 jours.

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.

Activation de l'anti-virus sur FTP

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

Activation de l'anti-virus sur la messagerie

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

Forcer l'activation du service clamd

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

À partir de la version 2.5.2 d'EOLE, il est possible de forcer l'activation du service anti-virus (clamd) en 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.

The screenshot shows the ClamAV configuration window with the following settings:

| Paramètre | Valeur |
|--|--------|
| Taille maximum pour un fichier à scanner (en Mo) | 5 |
| Quantité de données maximum à scanner pour une archive (en Mo) | 20 |
| Profondeur maximale pour le scan des archives | 12 |
| Nombre maximum de fichiers à scanner dans une archive | 5000 |
| Arrêter le démon en cas de surcharge mémoire | no |
| Détection des applications indésirables | no |
| Scan du contenu des fichiers ELF | no |
| Scan du contenu des fichiers PDF | yes |
| Scan des fichiers courriels | no |
| Détection des fichiers exécutables corrompus | no |

- 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.363] * [p.363] ;
- 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.

The screenshot shows the Freshclam configuration window with the following settings:

| Paramètre | Valeur |
|---|------------------------|
| Nom de domaine du serveur DNS de mise à jour | current.cvd.clamav.net |
| Forcer un serveur de mise à jour freshclam | non |
| Code IANA pour la mise à jour de la base de signature | fr |
| Nombre de tentatives de mise à jour par miroir | 5 |
| Nombre de mises à jour quotidiennes | 24 |

- 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 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://cgi.clamav.net/sendvirus.cgi>

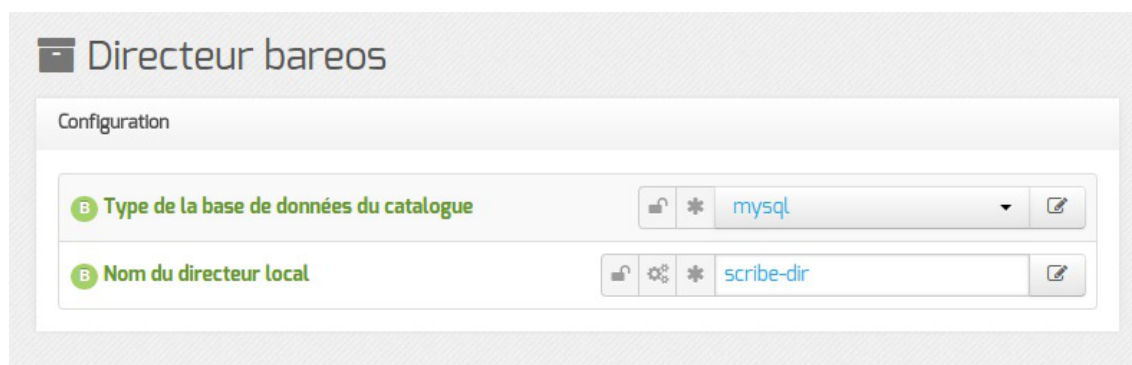
L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

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



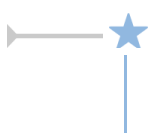
Il ne faut pas signaler des PUA^[p.369] comme étant des faux positifs.

3.13. Onglet Directeur bareos



Vue de l'onglet Directeur Bareos

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



Si le choix est laissé à l'utilisateur il est préférable d'utiliser MySQL. L'application web [bareos-webui](#) nécessite MySQL.

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

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

Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention^[p.363] des différents espaces de stockage (totale, différentielle et incrémentale).

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

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



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

Pour cela, voici un exemple de configuration :

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

Avec la politique de sauvegarde suivante :

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

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



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

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

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

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

```
# bareosregen.sh
La régénération 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 stockage.

The screenshot shows the configuration interface for the Bareos Director. It features three main configuration fields:

- Mot de passe de la base de données MySQL de la sauvegarde:** A text input field containing a long alphanumeric string, with a refresh icon and a checkmark.
- Délai alloué pour l'exécution complète d'une sauvegarde:** A numeric input field set to '0'.
- Niveau de compression des sauvegardes:** A dropdown menu set to 'GZIP6'.
- Mot de passe du directeur:** A text input field containing another long alphanumeric string, with a refresh icon.

Below the fields, the text 'Type de compression et délai alloué' is displayed.

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.

3.14. Onglet Annuaire

Sur le module Horus l'annuaire OpenLDAP est local.

The screenshot shows the 'Annuaire' configuration interface. It has a title bar with a folder icon and the text 'Annuaire'. Below the title bar, there is a 'Configuration' section with two settings:

- Port du serveur LDAP:** A numeric input field set to '389'.
- Définir le mot de passe admin de LDAP dans un fichier:** A dropdown menu set to 'oui'.

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 permettent de modifier finement le comportement de l'annuaire.

| | |
|--|--------------------------|
| Fichier de mot de passe de l'utilisateur admin | */root/writer |
| Attribut de recherche des utilisateurs | * uid |
| Filtre d'utilisateurs | * objectClass=person |
| Filtre de groupes | * objectClass=posixGroup |
| DN racine de l'arbre utilisateurs | |
| DN racine de l'arbre groupes | |
| Champ 'nom d'affichage' de l'utilisateur | * displayName |
| Champ 'mail' de l'utilisateur | * mail |
| Champ 'maildir' de l'utilisateur | * maildir |
| Champ 'fonction' de l'utilisateur | |
| Champ 'categorie' de l'utilisateur | |
| Champ 'rne' de l'utilisateur | |
| Champ 'frederne' de l'utilisateur | |
| Champ 'nom d'affichage' du groupe | * cn |

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

Voir aussi...

Onglet Openldap : Configuration du serveur LDAP local

3.15. 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.

⚡ Dhcp

Définition des sous-réseaux

B Adresse réseau de la plage DHCP

B Adresse réseau de la plage DHCP ↻ × *

B Masque de sous-réseau de la plage DHCP *

B IP basse de la plage DHCP *

B IP haute de la plage DHCP *

B Nom de domaine à renvoyer aux clients DHCP

B Adresse IP du routeur à renvoyer aux clients DHCP

B Adresse IP du DNS à renvoyer aux clients DHCP

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

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 relaying 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**.

| Définition des sous-réseaux | |
|--|-----------------|
| B Adresse réseau de la plage DHCP | * 192.168.0.0 |
| B Masque de sous-réseau de la plage DHCP | * 255.255.255.0 |
| B IP basse de la plage DHCP | * 192.168.0.50 |
| B IP haute de la plage DHCP | * 192.168.0.60 |
| B Nom de domaine à renvoyer aux clients DHCP | monreseau.lan |
| B Adresse IP du routeur à renvoyer aux clients DHCP | 192.168.232.2 |
| B Adresse IP du DNS à renvoyer aux clients DHCP | 192.168.232.2 |
| + Adresse réseau de la plage DHCP | |

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

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.364] 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.363], 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.

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

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

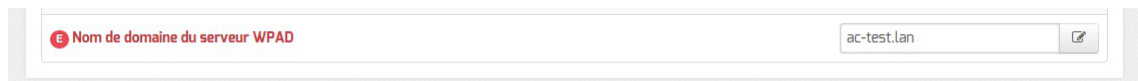
Vue de l'onglet Dhcp de l'interface de configuration du module

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).



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

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.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD

3.16. 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.

Les autres variables `Répertoire sur le serveur PXE/TFTP` et `Chemin vers le fichier de boot PXE initial` peuvent également être laissées par défaut.

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

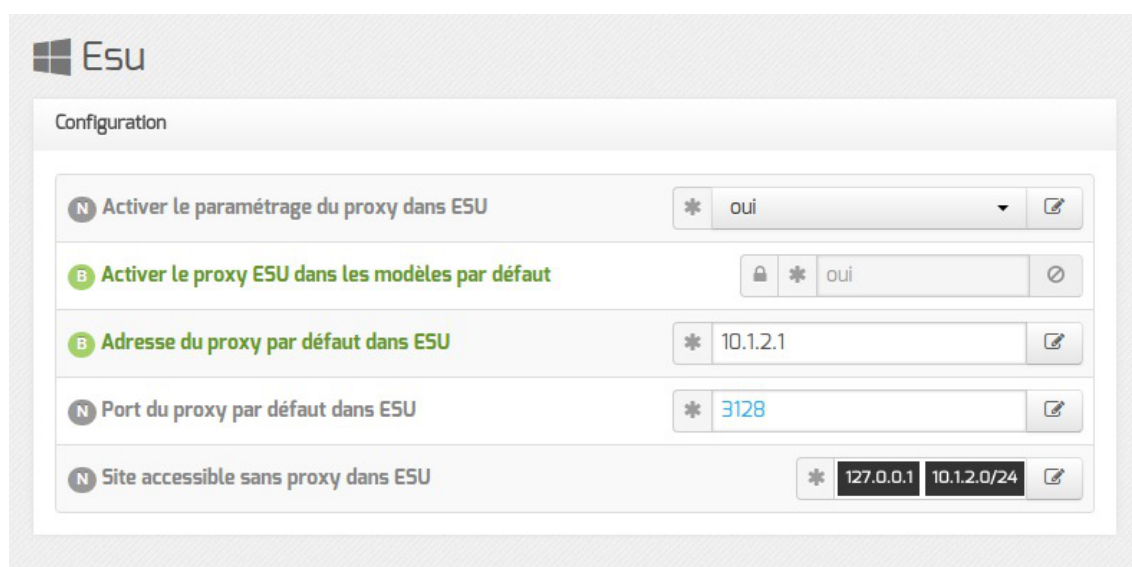
Exemple d'OSCAR^[p.368], outil de clonage édité par le CRDP de Lyon (<http://oscar.crdp-lyon.fr>) :

- Une 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

3.17. 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.



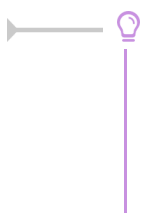
Vue de l'onglet Esu de l'interface de configuration du module

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

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

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

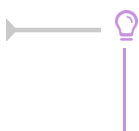
Si, à l'avenir, l'utilisateur souhaite changer le comportement du proxy il devra le faire au travers de l'interface ESU.



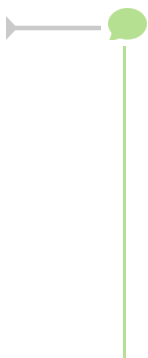
Les paramètres suivants Adresse du proxy par défaut dans ESU, Port du proxy par défaut dans ESU et Réseau par défaut sans proxy dans ESU sont modifiables à souhait et sont appliqués dans les variables ESU à chaque reconfiguration du module.

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

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



Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet Interface-1 (variable : adresse_ip_eth1_proxy_link).



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.361] tels que sauvegardés.



Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG^[p.361] tels que celui fourni par l'archive suivante :
ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

3.18. Onglet Samba : Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC^[p.369]) 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.).

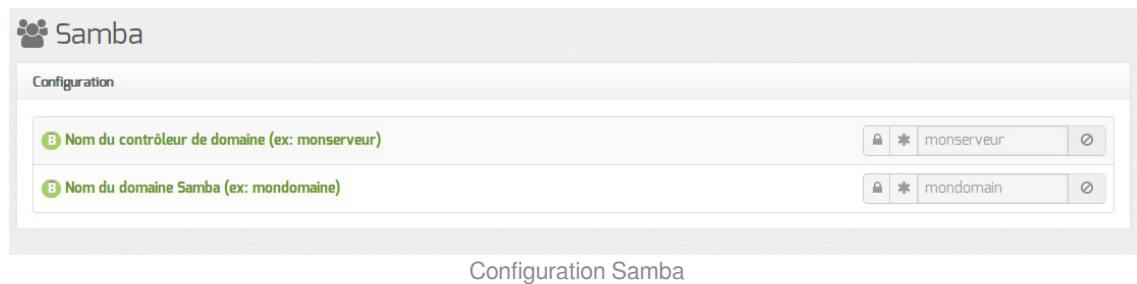
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

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.367]) 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>

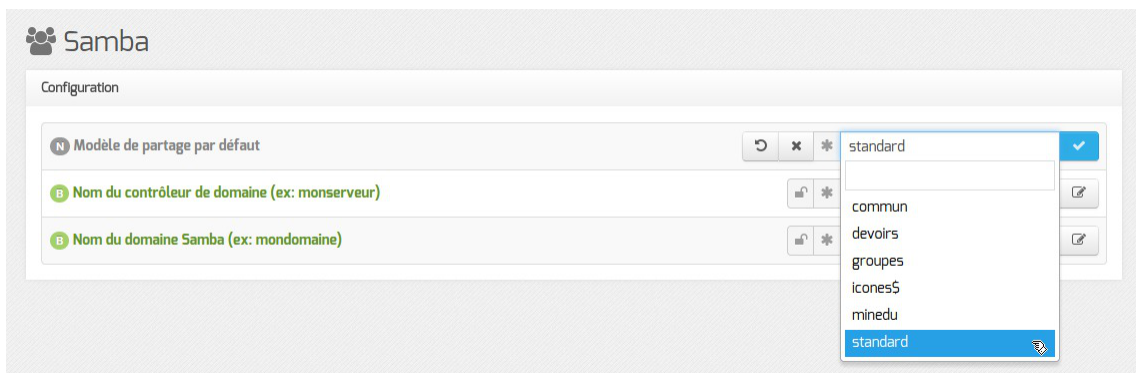
Fichiers invisibles sur les partages

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`) ;
- `$recycle.bin` : les fichiers `$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 fichiers `.scanned:*` générés par Scannedonly^[p.369] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

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.tpl`

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

Il existe déjà plusieurs modèles à disposition :

- `standard`
héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe
- `commun`
héritage des permissions, accès en écriture, accessible à tous en lecture et en écriture, accès anonyme (guest)
- `devoirs`
héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `groupes`
héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture
- `icones$`

caché dans le voisinage réseau, accès anonyme (guest)

- `minedu`

héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe, nom de fichier et répertoire en minuscules

Configuration avancée du serveur Samba

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

Âge maximal par défaut des mots de passe

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

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

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

Durée du cache des résultats de requêtes négatifs

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

Délai avant abandon pour la connexion au LDAP

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

Libellé du serveur Samba

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

Activer la corbeille Samba

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

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

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

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

La durée de conservation des fichiers supprimés est également paramétrable.



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

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

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

Activer le mode invité sur le partage

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

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

Niveau de log

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

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

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

Si la valeur de cette option est mise à 0, cela 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.

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 influencer sur les chances de Samba de remporter les élections de maître explorateur.

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

Niveau de protocole maximum supporté par le serveur

Cette variable, disponible à partir de la version 2.5.2 d'EOLE, permet de forcer l'utilisation d'un protocole. Par défaut la valeur NT1 permet d'assurer la compatibilité avec Windows 10.



Une valeur autre que NT1 ne garantit pas la compatibilité avec Windows 10.



La valeur `default` sera la valeur par défaut proposée par la version de Samba installée soit, par exemple, SMB3 pour la version 4.1.6 de Samba.

Annoncer Spoolss comme architecture x64

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

Activer des partages supplémentaires

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

Les options à saisir pour chaque partage supplémentaire sont :

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



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

Partages manuels

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

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

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

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

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

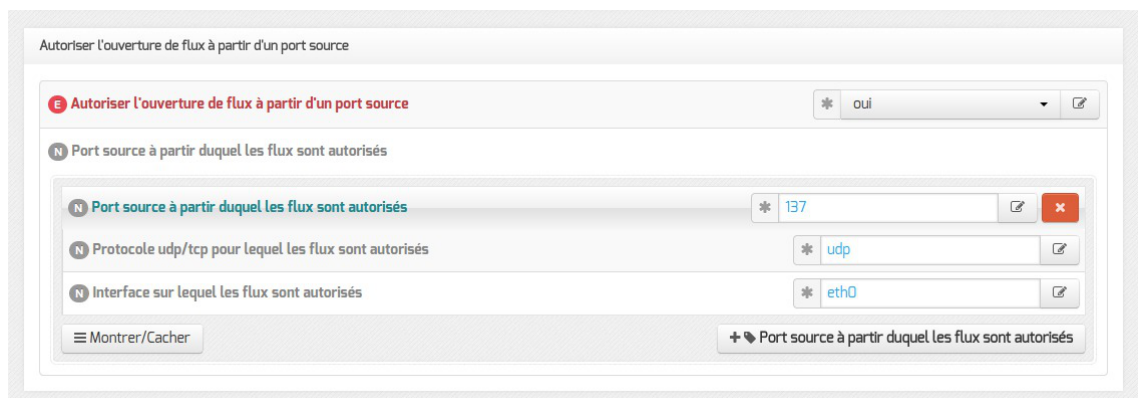
<http://manpages.ubuntu.com/manpages/precise/en/man5/smb.conf.5.html>

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

Lors de diagnostic il peut être utile d'utiliser la commande `nmblookup` pour déterminer l'adresse IP du ou des serveurs contrôleurs de domaine sur le réseau local.

Pour que l'échange puisse se faire en UDP via le port 137 il est nécessaire que le serveur EOLE puisse en autoriser l'accès.

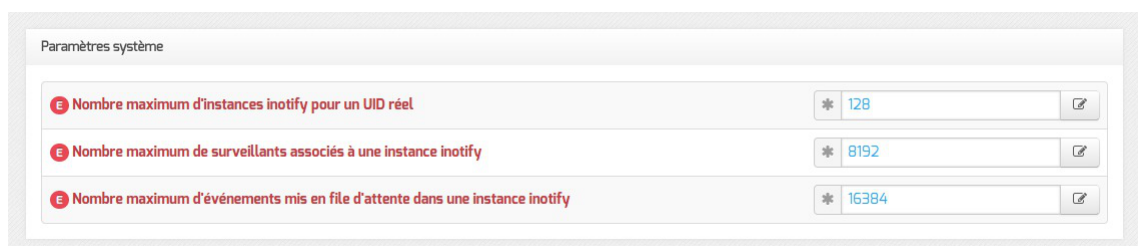
Pour activer cette fonctionnalité il faut passer Autoriser l'ouverture de flux à partir d'un port source à oui.



Les options pour le port autorisés et le protocole peuvent être laissés par défaut. Par contre il est important de choisir l'interface sur laquelle aura lieu cette autorisation.

Il est possible d'ajouter des autorisations sur plusieurs interfaces en cliquant sur le bouton `Port source à partir duquel les flux sont autorisés`.

Paramètres système



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

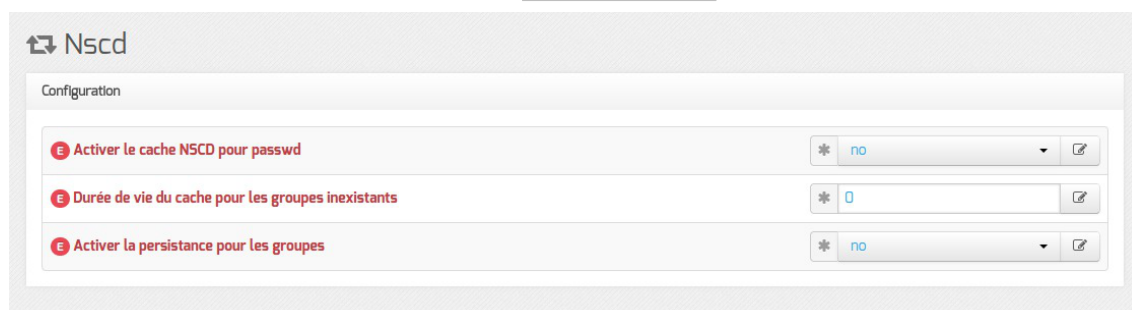
Voir aussi...

Onglet Clamav : Configuration de l'anti-virus

3.19. Onglet Nscd

NSCD^[p.367] est un démon qui fournit un cache pour limiter les requêtes vers l'annuaire LDAP.

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



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

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

3.20. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT^[p.367]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

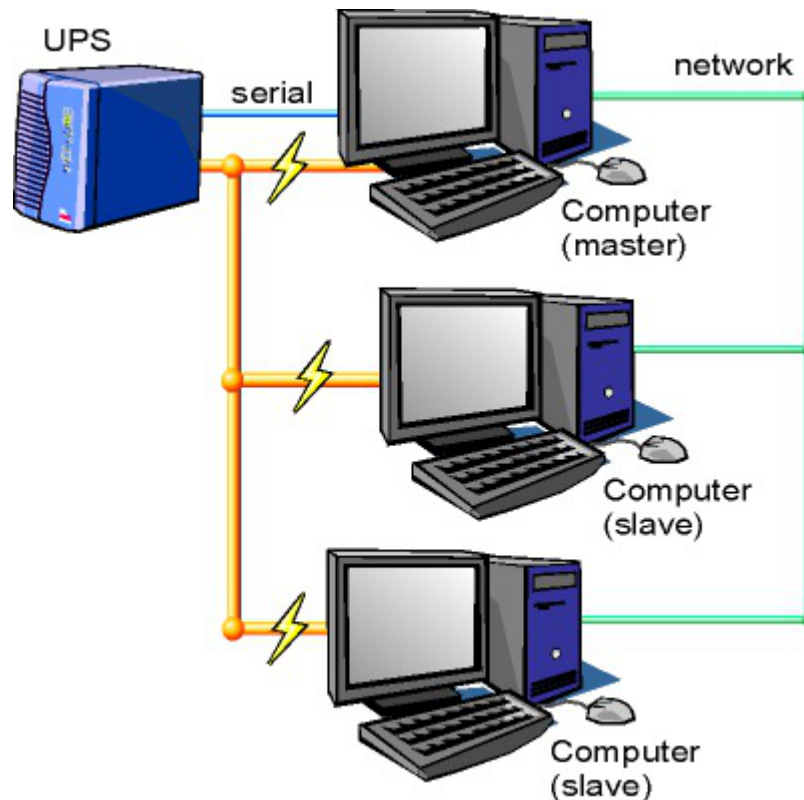


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - <http://ovanhoof.developpez.com/upsusb/>

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

<http://www.networkupstools.org/>

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

<http://www.networkupstools.org/stable-hcl.html>



Pour connaître la version de NUT qui est installée sur le module :

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

ou encore :

```
# apt-show-versions nut
```

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

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

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

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

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

Vue de l'onglet Onduleur

Si l'onduleur est branché directement sur le module il faut laisser la variable Configuration sur un serveur maître à oui, cliquer sur le bouton + Nom de l'onduleur et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître

Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ Nom pour l'onduleur.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante Pilote de communication de l'onduleur et éventuellement préciser le Port de communication si l'onduleur n'est pas USB.

Les champs Numéro de série de l'onduleur, Productid de l'onduleur et Upstype de l'onduleur sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost | grep <nom_variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;

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

La majorité des onduleurs USB sont détectés automatiquement.



Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave à se connecter avec cet utilisateur.

Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)



Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.



Chaque utilisateur doit avoir un nom différent.

Les noms `root` et `localmonitor` sont réservés.



Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf` ou consulter la page web suivante : <http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html>

Configurer un serveur esclave

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

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

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

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

Exemple de configuration



Sur le serveur maître :

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



Sur le serveur esclave :

- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

3.21. 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.

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.

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/`

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

L'onglet `Applications web` permet aussi d'activer/désactiver toutes les applications web EOLE installées sur le module.

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`.

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.

| | | |
|---|-------------------------|---|
| Activer la vérification de l'autorité de certification pour les applications web cassifiées | * non | ✎ |
| Certificat utilisé par apache | /etc/ssl/certs/eole.crt | ✎ |

3.22. 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`.

The screenshot shows the 'Apache' configuration page with two main sections: 'Applications supplémentaires' and 'Configuration PHP'. The 'Applications supplémentaires' section has a single setting 'Déclarer des applications web supplémentaires' set to 'non'. The 'Configuration PHP' section contains ten settings, each with a value and an edit icon:

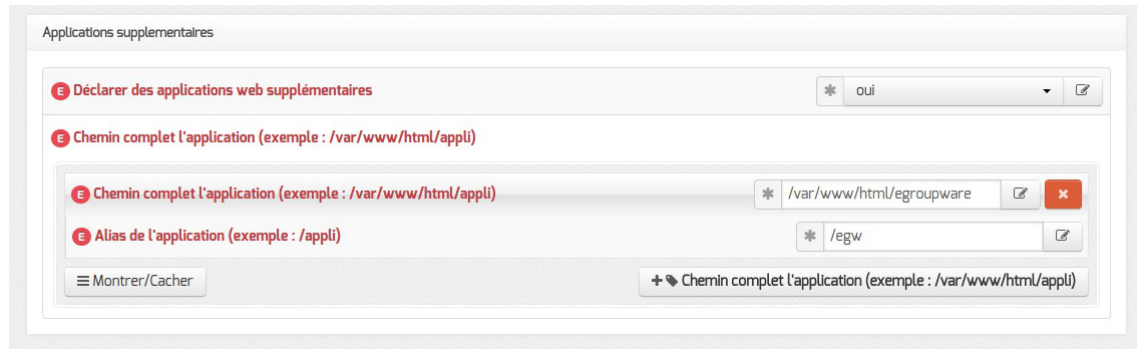
| | |
|--|------|
| Taille maximale des données reçues par la méthode POST (en Mo) | 32 |
| Taille maximale d'un fichier à charger (en Mo) | 16 |
| Temps maximal d'exécution d'un script (en secondes) | 30 |
| Durée maximale pour analyser les données d'entrée (en secondes) | 60 |
| Taille mémoire maximale qu'un script est autorisé à allouer (en Mo) | 128 |
| Affichage des erreurs à l'écran | Off |
| Durée de vie des données sur le serveur (en secondes) | 3600 |
| Permettre de lister les répertoires et leur contenu | non |
| Nombre d'octets à lire dans le fichier utilisé comme source additionnelle d'entropie | 16 |
| Activer la directive de configuration browscap | non |

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

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).
- 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 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()`.



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.140]

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

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

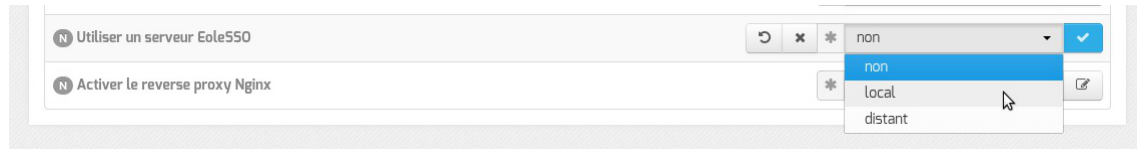
Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

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**.



Activation du serveur SSO dans l'interface de configuration du module

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-ss0` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

The screenshot shows the 'Configuration' page for 'Eole sso'. It contains several configuration fields:

- Nom de domaine du serveur d'authentification SSO: [Empty]
- Port utilisé par le service EoleSSO: 8443
- Adresse du serveur LDAP utilisé par EoleSSO: localhost
- Port du serveur LDAP utilisé par EoleSSO: 389
- Chemin de recherche dans l'annuaire: o=gouv,c=fr
- Libellé à présenter aux utilisateurs en cas d'homonymes: Annuaire de amon.monreseau.lar
- Informations supplémentaires dans le cadre d'information sur les homonymes: [Empty]
- Utilisateur de lecture des comptes LDAP (nécessaire pour la fédération): cn=reader,o=gouv,c=fr
- Fichier de mot de passe de l'utilisateur de lecture: /root/.reader
- Attribut de recherche des utilisateurs: uid
- Information LDAP supplémentaires (applications): non
- Adresse du serveur SSO parent: [Empty]
- Port du serveur SSO parent: 8443
- Nom d'entité SAML du serveur eole-ssso (ou rien): [Empty]
- Gestion de l'authentification OTP (RSA SecurID): non
- Chemin du certificat SSL (ou rien): [Empty]
- Chemin de la clé privée liée au certificat SSL (ou rien): [Empty]
- Chemin de l'autorité de certification (ou rien): [Empty]
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200
- CSS par défaut du service SSO (sans le .css): [Empty]
- Cacher le formulaire lors de l'envoi des informations de fédération: non

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.

The screenshot shows the 'Configuration' page for 'Eole sso' with the following settings:

- Nom de domaine du serveur d'authentification SSO: 192.168.0.31
- Port utilisé par le service EoleSSO: 8443
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200

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.368] si disponible (*voir plus loin*).



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

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

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

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

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

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

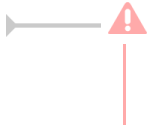
- Utilisateur de lecture des comptes ldap : renseignez son *dn* complet dans l'annuaire
- fichier de mot de passe de l'utilisateur de lecture : entrez le chemin d'un fichier où vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur `root`)

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 essaiera 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.372] 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.370] de la société EMC (précédemment RSA).

Pour cela il faut :

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

Des champs supplémentaires apparaissent :

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

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation^[p.365] 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'autres types de serveurs compatibles avec le protocole SAML^[p.369] (version 2).

Nom d'entité SAML du serveur eole-ssso (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

| | |
|--|--------|
| Ne pas répondre aux demandes CAS des applications inconnues | * non |
| Décalage de temps (en secondes) dans les messages de fédération SAML | * -300 |
| Utiliser l'authentification SSO pour l'EAD | * oui |

En mode expert 3 nouvelles variables sont disponibles :

- 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.

Voir aussi...

Gestion des sources d'authentification multiples [p.168]

3.24. 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.

3.25. 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.

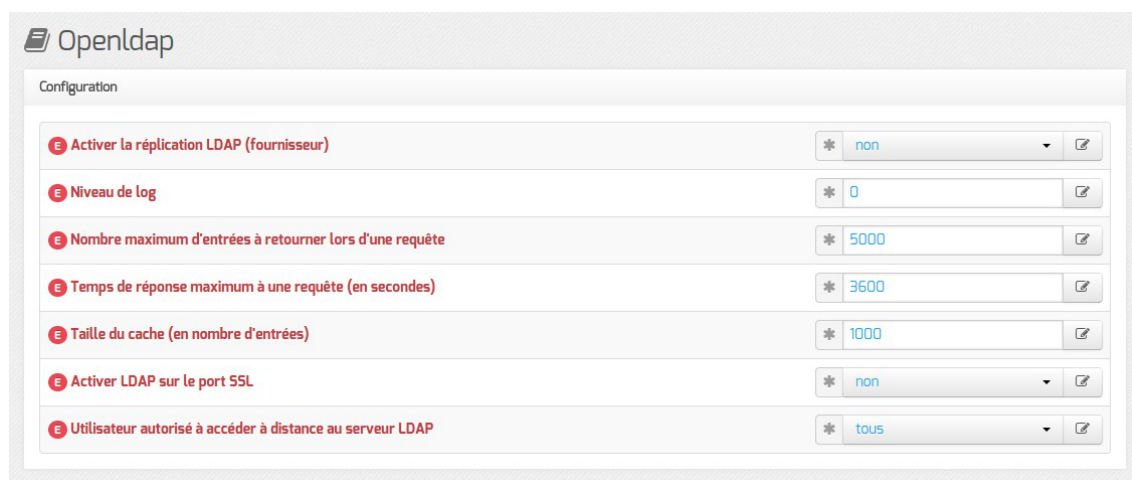


Pour plus d'informations, vous pouvez consulter les exemples de configuration fournis dans :
</usr/share/doc/mysql-server-5.5/examples/>
 ou consulter :
<http://dev.mysql.com/doc/refman/5.5/en/server-system-variables.html>

3.26. Onglet Openldap : Configuration du serveur LDAP local

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

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



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

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

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

Activer la réplication LDAP (fournisseur)

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

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

Niveau de log

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

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

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

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

La valeur par défaut est de `5000` entrées.

Temps de réponse maximum à une requête (en secondes)

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

La valeur par défaut est de `3600` secondes.

Taille du cache (en nombre d'entrées)

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

La valeur par défaut est de `1000` entrées.

Activer LDAP sur le port SSL

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

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>

3.27. 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.

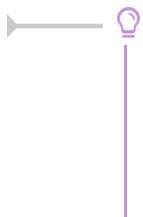
L'onglet expert **Cups** permet de configurer l'imprimante virtuelle PDF.

| Cups Configuration | |
|--|--------|
| Activation de l'imprimante virtuelle PDF | * oui |
| Nom de l'imprimante virtuelle PDF | * PDF |
| L'imprimante virtuelle PDF est partagée | * true |

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

| | |
|---|--------|
| Niveau de log | * info |
| Activer la récupération des informations des imprimantes distantes | * on |
| Nombre maximum de copies qu'un utilisateur peut effectuer pour un travail d'impression | * 100 |
| Nombre maximum de travaux simultanés | * 500 |
| Nombre maximum de clients simultanés | * 100 |
| Conserver l'historique des demandes d'impression | * Yes |
| Conserver les fichiers après impression | * No |
| Purger automatiquement l'historique des travaux | * No |
| Générer le fichier printcap | * non |
| Charger le module d'impression d'imprimante sur port parallèle (incompatible avec les conteneurs) | * non |

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



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

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

Niveau de log

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

Activer la récupération des informations des imprimantes distantes

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

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

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

Nombre maximum de travaux simultanés

Indique le nombre maximum de travaux simultanés supportés.

Nombre maximum de clients simultanés

Indique le nombre maximum de clients simultanés supportés.

Conserver l'historique des demandes d'impression

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

Conserver les fichiers après impression

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

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/precise/en/man5/cupsd.conf.5.html>

3.28. Onglet Proftpd : Configuration du serveur FTP

Le serveur FTP est activable/désactivable dans l'onglet `Services` par l'intermédiaire de l'option `Activer l'accès FTP`. Le serveur FTP est basé sur le logiciel libre ProFTPD.

<http://www.proftpd.org/>

L'onglet `Proftpd` n'apparaît en mode expert que si le service est activé.

The screenshot shows the 'Configuration' tab of the Proftpd interface. It contains a list of settings, each with a red 'E' icon, a name, a value, and an edit icon:

- Nom du serveur FTP**: [Empty text field]
- Activer le chiffrement TLS**: [non]
- Activer l'accès anonyme**: [non]
- Activer des accès FTP supplémentaires**: [non]
- Autoriser CAS en accès FTP**: [oui]
- Utiliser le fichier '/etc/ftpusers' pour interdire l'accès FTP à des comptes utilisateur**: [non]
- Nombre maximum d'utilisateurs simultanés**: [50]
- Nombre maximum de processus pour ProFTPD**: [40]
- Taille maximum du fichier récupéré (download) en Mb**: [500]
- Taille maximum du fichier déposé (upload) en Mb**: [100]
- Temps maximum d'inactivité avant déconnexion (en secondes)**: [1200]

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.

The screenshot shows two configuration items:

- Activer l'accès anonyme**: [oui]
- Chemin du répertoire anonyme**: [/home/ftp]

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.

| | |
|--|---------------------------|
| E Activer des accès FTP supplémentaires | * oui |
| E Chemin du répertoire FTP supplémentaire | * /home/commun /home/data |

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.

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 :

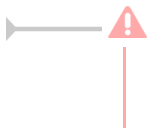
ftp://user@<adresse_serveur>/

ou

ftp://<adresse_serveur>/

Accès par une application web

Pour accéder aux fichiers par l'application web Ajaxplorer 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.

3.29. 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

Messagerie

Serveur d'envoi/réception (SMTP)

Nom de domaine de la messagerie de l'établissement (ex : monetab.ac-aca.fr) monreseau.lan

Adresse électronique recevant les courriers électroniques à destination du compte root admin@monreseau.lan

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 réécrits et envoyés à l'adresse électronique d'envoi du compte root.

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

Adresse électronique d'envoi pour le compte root

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.

Gérer la distribution pour les comptes LDAP * non

Quota des boîtes aux lettres en Mo * 20

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

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

En mode expert il est possible d'écraser l'entêtes des courriers électroniques.

La réécriture des adresses doit prendre en compte la distinction entre l'enveloppe SMTP (« MAIL FROM » et « RCPT TO ») et les en-têtes des messages (« From: », « Reply-To:», « To: », « Cc: », « Bcc: »).

Les adresses électroniques systèmes ont par défaut une des formes suivante :

- `user@%domaine_messagerie_etab` si l'expéditeur ne précise pas le nom de domaine, par exemple :

```
root@internet:~# echo "Test" | mail -s "Test mail from shell" -r root root
```
- `user@%nom_machine.%domaine_messagerie_etab` pour le maître si l'expéditeur utilise la configuration définie dans `/etc/mailname`
- `user@%conteneur.%nom_machine.%domaine_messagerie_etab` pour les conteneurs^[p-362] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

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

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

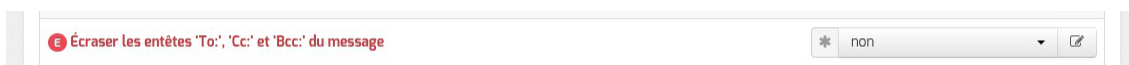
Les adresses destinataires `root@%nom_domaine_local` et `root@%domaine_messagerie_etab` sont remplacées par `%system_mail_to` si cette dernière est définie.

Les adresses expéditeurs et destinataires systèmes sont ensuite réécrites selon les tableaux suivants en fonction de variables expertes :

- `system_mail_from_for_headers` : écraser les en-têtes « From: », « Reply-To: » et « Sender: » du message, par défaut à `non`



- `system_mail_to_for_headers` : écraser les en-têtes « To: », « Cc: » et « Bcc: » du message, par défaut à `non`



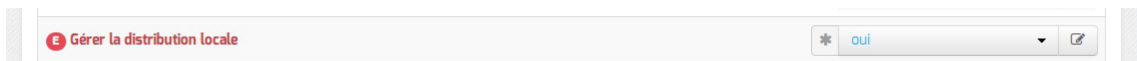
Réécriture de l'expéditeur :

| | | |
|------------|---|---|
| | <code>system_mail_from_for_headers = non</code> | <code>system_mail_from_for_headers = oui</code> |
| MAIL FROM | <code>system_mail_from</code> | <code>system_mail_from</code> |
| From : | <code>user@conteneur.machine.domaine</code> | <code>system_mail_from</code> |
| Reply-To : | <code>user@conteneur.machine.domaine</code> | <code>system_mail_from</code> |
| Sender : | <code>user@conteneur.machine.domaine</code> | <code>system_mail_from</code> |

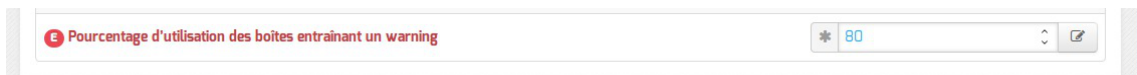
Réécriture du destinataire :

| | | |
|---------|----------------------------------|----------------------------------|
| | system_mail_to_for_headers = non | system_mail_to_for_headers = oui |
| RCPT TO | system_mail_to | system_mail_to |
| To : | user@conteneur.machine.domaine | system_mail_to |
| Cc : | user@conteneur.machine.domaine | system_mail_to |
| Bcc : | user@conteneur.machine.domaine | system_mail_to |

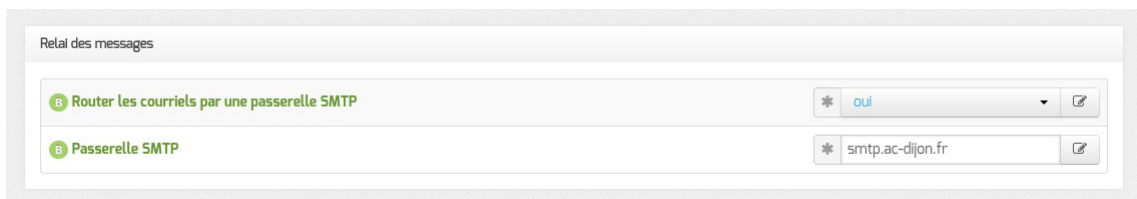
Par défaut la distribution des messages se fait en local, ce qui permet d'avoir un domaine local et un domaine privé.



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



Relai des messages



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

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



`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS^[p.371] pour l'envoi de message. Si la passerelle SMTP^[p.370] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS^[p.370] (port 25) ou non (port 465).

Par défaut le relai des messages n'est pas activé sur les modules sauf sur le module Seshat. Si la variable est passée à oui, elle active les listes d'adresses IP autorisées à utiliser ce serveur comme relai

de messagerie et la liste des noms de domaines autorisés à être relayés par ce serveur.



| | |
|---|---------------|
| Activer le relais des messages | oui |
| Activer le TLS pour les clients | oui |
| Relayer les courriers électroniques pour des plages d'adresses IPv4 | Pas de valeur |
| Relayer les courriers électroniques pour des nom de domaines | Pas de valeur |

Le TLS est activé par défaut pour les clients.

Dans la rubrique Configuration experte plusieurs paramètres peuvent être modifiés.



| | |
|---|----------------------|
| FQDN utilisé par Exim | automatique |
| Domaine utilisé pour qualifier les adresses | nom de domaine local |
| Envoyer les logs par syslog | oui |
| Dupliquer les logs dans des fichiers | non |
| Activer les règles de réécriture étendue | non |

- FQDN utilisé par Exim

Personnalisation du nom de domaine complètement qualifié utilisé par Exim dans le protocole SMTP. C'est utile pour les vérifications anti-spam des MX externes

Les valeurs possibles sont :

- automatique : laisser Exim décider ;
- nom_machine.domaine_messagerie_etab : utiliser le nom de la machine complété par le nom de domaine de la messagerie établissement ;
- nom_machine.nom_domaine_local : utiliser le nom de la machine complété par le nom de domaine local.

- Domaine utilisé pour qualifier les adresses

Nom de domaine ajouté aux adresses :

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

- Envoyer les logs à rsyslog

Permet de désactiver l'envoi des logs.

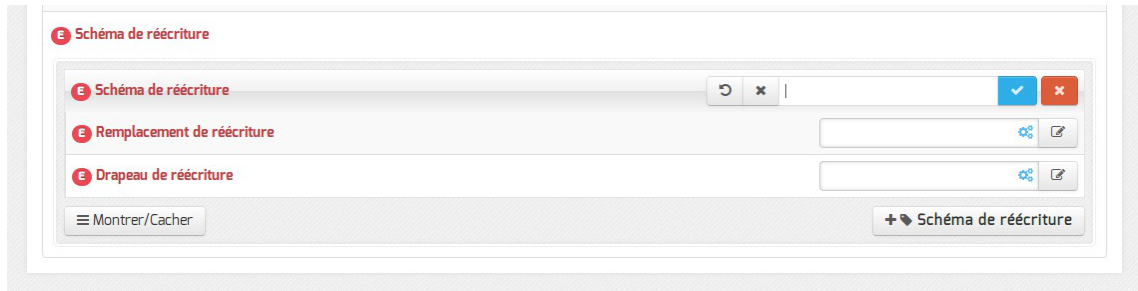
- Dupliquer les logs dans des fichiers

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

- Activer les règles de réécriture étendue

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

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

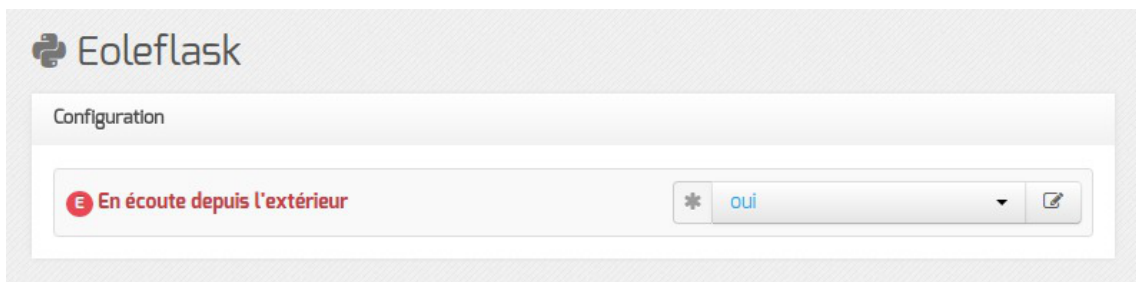


Les trois variables à saisir sont :

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

3.30. Onglet Eoleflask

Dans cet onglet se trouvent les options concernant le service Eoleflask et les options des applications reposant sur ce service.



Passer la variable `En écoute depuis l'extérieur` à `oui` permet d'accéder à l'interface de configuration du module depuis un poste client.

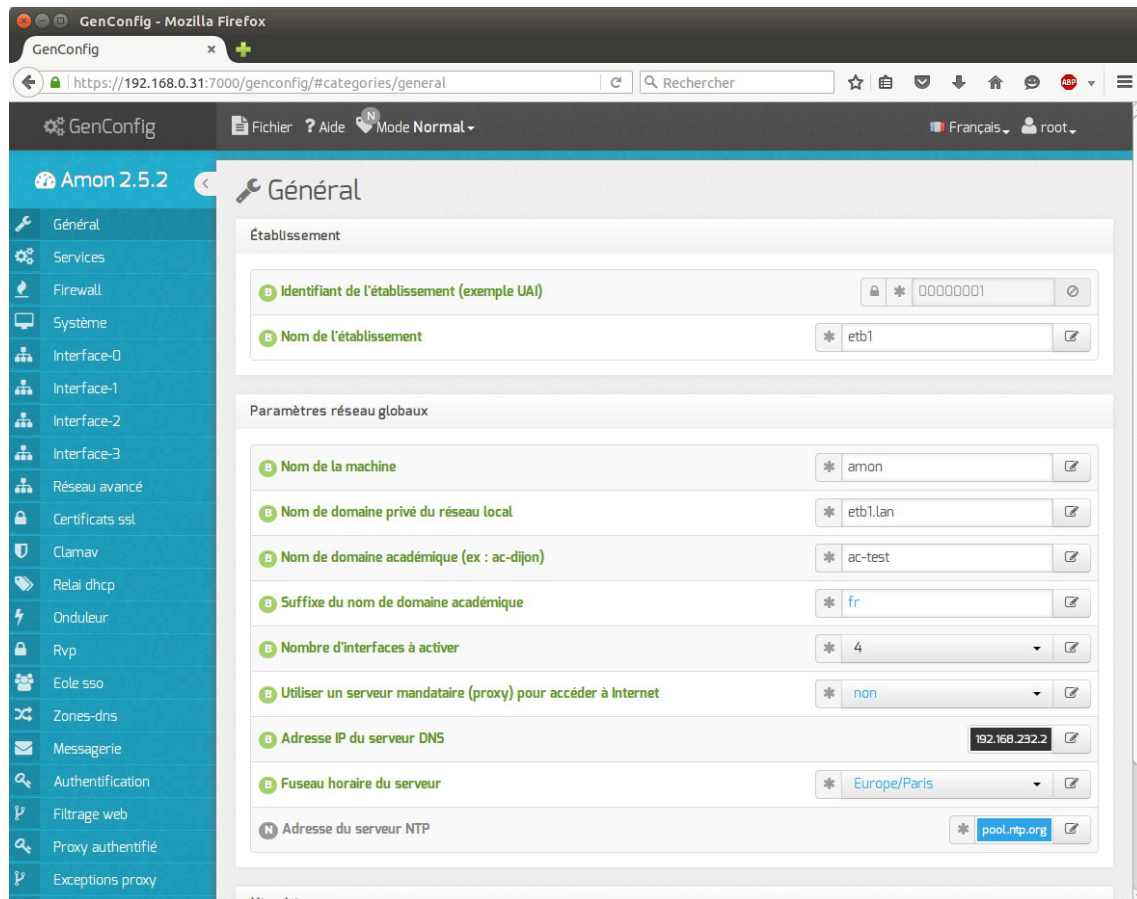
Accès distant

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

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

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

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



Vue de l'interface de configuration au travers d'un navigateur web



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

4. 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.

4.1. Téléchargement et mise en place

Installation des fichiers

Pour télécharger une archive sur le module, il faut utiliser la commande `wget` :

```
# wget https://downloads.sourceforge.net/project/egroupware/eGroupware-14.2/eGroupware-14.2
```

Il faut ensuite décompresser l'archive à l'aide de la commande `tar` (ou `unzip`, pour le format zip) :

```
# tar xzvf egroupware-epl-14.2.20150310.tar.bz2
```

Dans cet exemple, cela créera le répertoire `egroupware`

Ensuite, il faut envoyer les fichiers dans le répertoire de destination, soit :

- sur les modules Scribe ou Horus :

```
# cp -r egroupware /var/www/html/egroupware
```

- sur un module Horus dépourvu d'application web :

```
# mkdir /var/www/html
```

```
# cp -r egroupware /var/www/html/egroupware
```

- sur le module AmonEcole :

```
# cp -r egroupware /opt/lxc/reseau/rootfs/var/www/html/egroupware
```

Affectation de droits

La plupart des applications nécessitent que l'utilisateur utilisé par le service Apache (ici, l'utilisateur système : `www-data`) ait le droit d'écrire en certains endroits du disque.

Le propriétaire d'un fichier ou d'un répertoire se modifie à l'aide de la commande `chown` :

- sur les modules Scribe/Horus :

```
# chown -R www-data: /var/www/html/egroupware
```

```
# chmod 770 /var/www/html/egroupware (le temps de l'installation)
```

- sur le module AmonEcole :

```
# ssh reseau
```

```
# chown -R www-data: /var/www/html/egroupware
```

```
# chmod 770 /var/www/html/egroupware (le temps de l'installation)
```

```
# ctrl + d pour sortir du conteneur
```



Donner trop de droits à l'utilisateur `www-data` diminue la sécurité du serveur.

Consulter la documentation du logiciel pour n'attribuer que les droits nécessaires au fonctionnement de l'application.

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-imagick

- sur les modules Scribe ou Horus :

```
# apt-eole install php5-imagick
```

- sur le module AmonEcole :

```
# apt-eole install-conteneur web php5-imagick
```

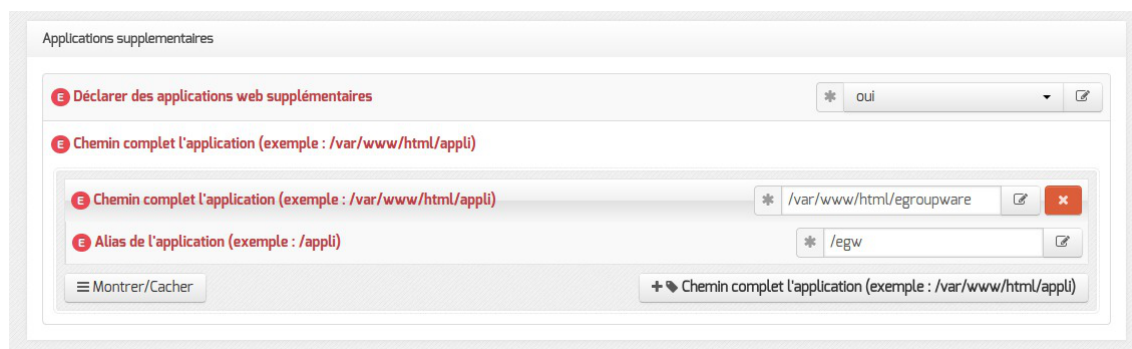
Installation manuelle de paquets (cf. Installation manuelle de paquets)

4.2. Configuration Apache

Méthode Creole

Dans l'interface de configuration du module :

- aller dans l'onglet `Apache` en mode expert ;
- indiquer le chemin complet de l'application et l'alias de l'application `/var/www/html/egroupware` ;
- indiquer le chemin de l'alias de l'application `/egw` ;



Déclaration d'une application web dans gen_config

- enregistrer la configuration et quitter ;
- lancer la commande `reconfigure` ;
- le logiciel doit répondre à l'adresse : `http://<adresse_serveur>/egw`



Le fichier de configuration apache pour cette application est `/etc/apache2/sites-available/eole`



La directive `php_admin_flag allow_url_fopen` 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-enabled/egroupware`

- sur le module AmonEcole : `/opt/lxc/reseau/rootfs/etc/apache2/sites-enabled/egroupware`

```
# 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 :

```
# a2ensite egroupware
```

- recharger la configuration d'Apache à l'aide de la commande `CreoleService`^[p.362] :

```
# CreoleService apache2 reload
```

- le logiciel doit répondre à l'adresse : `http://<adresse_serveur>/egw`

Pour obtenir une configuration apache optimale, consulter la documentation de l'application. En cas de problème, consulter le fichier de journal `/var/log/rsyslog/local/apache2/apache2.err.log`. Dans le cas d'EGroupware, il est nécessaire de supprimer le fichier `.htaccess` situé dans le répertoire racine du logiciel :

```
# rm -f /var/www/html/egroupware/.htaccess
```

La directive `php_admin_flag allow_url_fopen On` est également nécessaire au bon fonctionnement d'EGroupware.

4.3. 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`.

4.4. Configuration du logiciel

Vous pouvez maintenant utiliser le système automatique d'installation du logiciel disponible à l'adresse : `http://<adresse_serveur>/egw`

Un `/install` ou `/config` sera à ajouter au chemin en fonction de l'application à installer.



Sur le module AmonEcole, l'adresse de la base de données à mettre dans l'interface de configuration de l'application est celle du conteneur `bdd` (`192.0.2.50`) et non `localhost`.

Affectation de droits après l'utilisation du système automatique d'installation du logiciel

Changer les droits d'accès :

```
# chmod 750 /var/www/html/egroupware
```

Changer le propriétaire des fichiers :

```
# chown -R root :www-data /var/www/html/egroupware
```

Authentification CAS

Informations utiles à la configuration d'une authentification CAS :

- adresse du serveur CAS : adresse IP (ou nom DNS) de votre module EOLE
- port d'écoute par défaut du serveur CAS : 8443 (CAS EOLE)
- URI sur le serveur CAS : *rien*
- Destination après la sortie : *rien*



Par défaut EoleSSO, fournit uniquement l'identifiant de l'utilisateur. Pour chaque application, il est possible d'ajouter des filtres définissant des attributs

supplémentaires à fournir.

Pour plus d'informations, consulter la documentation EoleSSO.

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.361] 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 ^[p.337]

Définition de filtres d'attributs

5. EoleSSO

5.1. Présentation du produit EoleSSO

Description du produit

EoleSSO est un serveur d'authentification développé pour répondre à la problématique du SSO^[p.370] (authentification unique) dans différentes briques de l'architecture EOLE. Il est développé en langage Python à l'aide du framework Twisted^[p.371].

Ce produit implémente en premier lieu un serveur d'authentification compatible avec le protocole CAS^[p.361].

Une partie du protocole SAML^[p.369] 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.370] (SSO) dans EoleSSO est basée sur le protocole CAS^[p.361].

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.

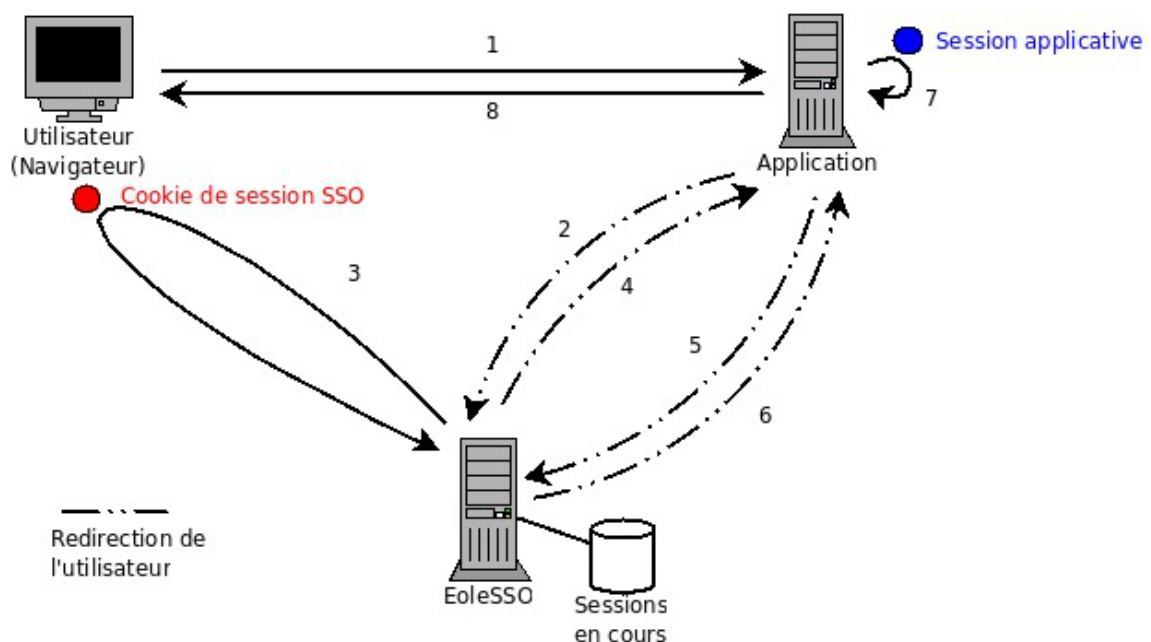
Ces tickets sont également utilisés pour mémoriser une session de fédération avec un autre système (se reporter aux chapitres traitant de la fédération d'identité).

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.

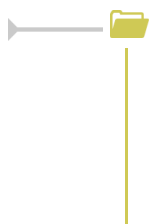
Une fois qu'une application a obtenu un ticket, elle peut utiliser de façon classique une session interne pour ne pas surcharger le serveur par des appels trop nombreux.

 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).
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>

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

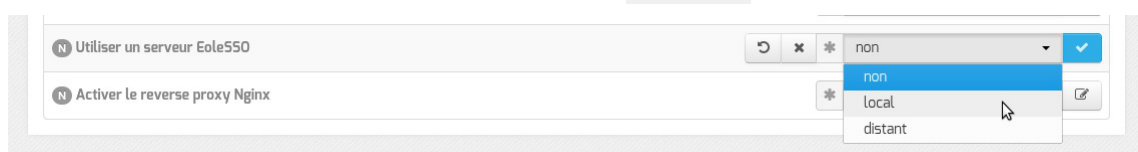
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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`.



Activation du serveur SSO dans l'interface de configuration du module

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-ssso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

The screenshot shows the 'Eole sso' configuration page. It is divided into two main sections. The top section, titled 'Configuration', contains several fields for LDAP settings, including the domain name, port (8443), and a list of LDAP servers. The first LDAP server is 'localhost' on port 389, with search path 'o=gouv,c=fr' and search attribute 'uid'. The bottom section contains SSO-related settings, such as 'Information LDAP supplémentaires (applications)' set to 'non', 'Port du serveur SSO parent' set to 8443, and 'Gestion de l'authentification OTP (RSA SecurID)' set to 'non'.

| Paramètre | Valeur |
|---|--------------------------------|
| Nom de domaine du serveur d'authentification SSO | |
| Port utilisé par le service EoleSSO | 8443 |
| Adresse du serveur LDAP utilisé par EoleSSO | localhost |
| Port du serveur LDAP utilisé par EoleSSO | 389 |
| Chemin de recherche dans l'annuaire | o=gouv,c=fr |
| Libellé à présenter aux utilisateurs en cas d'homonymes | Annuaire de amon.monreseau.lar |
| Informations supplémentaire dans le cadre d'information sur les homonymes | |
| Utilisateur de lecture des comptes LDAP (nécessaire pour la fédération) | cn=reader,o=gouv,c=fr |
| Fichier de mot de passe de l'utilisateur de lecture | /root/.reader |
| Attribut de recherche des utilisateurs | uid |
| Information LDAP supplémentaires (applications) | non |
| Adresse du serveur SSO parent | |
| Port du serveur SSO parent | 8443 |
| Nom d'entité SAML du serveur eole-ssso (ou rien) | |
| Gestion de l'authentification OTP (RSA SecurID) | non |
| Chemin du certificat SSL (ou rien) | |
| Chemin de la clé privée liée au certificat SSL (ou rien) | |
| Chemin de l'autorité de certification (ou rien) | |
| Durée de vie d'une session sur le serveur SSO (en secondes) | 7200 |
| CSS par défaut du service SSO (sans le .css) | |
| Cacher le formulaire lors de l'envoi des informations de fédération | non |

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.

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.368] si disponible (*voir plus loin*).

Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.
Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).
Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

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

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

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

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

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 essaiera 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.372] 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.370] de la société EMC (précédemment RSA).

Pour cela il faut :

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

Des champs supplémentaires apparaissent :

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

minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation^[p.365] 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'autres types de serveurs compatibles avec le protocole SAML^[p.369] (version 2).

Nom d'entité SAML du serveur eole-ssso (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/ssso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

Configuration en mode expert

| | |
|--|--------|
| Ne pas répondre aux demandes CAS des applications inconnues | * non |
| Décalage de temps (en secondes) dans les messages de fédération SAML | * -300 |
| Utiliser l'authentification SSO pour l'EAD | * oui |

En mode expert 3 nouvelles variables sont disponibles :

- 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.

Voir aussi...

Gestion des sources d'authentification multiples [p.168]

5.3. Protocoles supportés

5.3.1. Compatibilité CAS

Fonctions implémentées au niveau serveur



Le serveur EoleSSO implémente le protocole CAS^[p.361].

Vous pouvez retrouver la description de ce protocole sur le site officiel du protocole :

<http://www.apereo.org/cas/protocol>

Les version 1 et 2 du protocole sont gérées.

En plus des fonctionnalités de base décrites dans le protocole, les fonctions suivantes ont été ajoutées pour permettre une meilleure compatibilité avec des versions plus récentes (CAS 3) :

- échange de messages au format SAML 1.1 dans une enveloppe SOAP ;
- implémentation d'une déconnexion centralisée pour les sessions établies via le protocole CAS. Cette fonctionnalité peut être activée ou désactivée au niveau du serveur (active par défaut) ;
- envoi d'attributs utilisateur supplémentaires dans la réponse du serveur, avec un système de filtres suivant l'URL de destination.



Les protocoles 1 et 2 de CAS utilisent un format de messages différent. Le serveur peut être configuré pour répondre à l'un ou l'autre des formats, mais ne peut pas gérer les 2 en même temps. La version 1 du protocole est disponible pour permettre au serveur de répondre à des

clients plus anciens, mais dans ce cas les fonctionnalités du serveur seront très limitées (en particulier, le mode proxy et l'envoi d'attributs ne sont pas gérés).

Compatibilité du client

Suivant le client utilisé, certaines fonctionnalités peuvent ne pas être disponibles.

- La prise en compte des requêtes de déconnexion envoyées par le serveurs nécessitent l'utilisation d'un client récent (phpCAS version 1.1.0 ou supérieur).

Une version modifiée du client phpCAS est disponible dans les dépôts de la distribution EOLE.

5.3.2. 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.369]. 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 [\[http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf\]](http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf) publié sur le site d'OASIS.

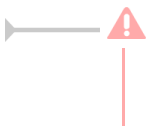
Les fonctionnalités absentes seront éventuellement implémentées dans des versions ultérieures selon les besoins.

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 incluse dans le fichier de méta-données.

Scenarii gérés :

1. En tant que fournisseur d'identité :

- émission d'une assertion d'authentification à destination d'un fournisseur de service (initié par le fournisseur d'identité ou suite à réception d'une requête authentification émise par un fournisseur de service valide) ;

- déclenchement du processus de déconnexion globale à l'initiative du fournisseur ou suite à la réception d'une requête de déconnexion valide.
2. En tant que fournisseur de service :
- création d'une session locale suite à la réception d'une assertion d'authentification d'un fournisseur d'identité (et redirection vers l'adresse spécifiée par le paramètre *relayState* si il est présent) ;
 - émission d'une requête de déconnexion en direction du fournisseur d'identité en cas de demande de déconnexion depuis une application cliente.

5.3.3. 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.370] (authentification de type One Type Password).

L'authentification est effectuée par l'intermédiaire du module PAM^[p.368] 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.368].

Il est prévu par la suite de pouvoir déléguer cette validation à un autre serveur EoleSSO (moyennant l'établissement d'un lien de fédération entre les deux serveurs).

Utilisation

Lors de la première utilisation, l'utilisateur se connecte au serveur EoleSSO avec ses identifiants habituels (authentification LDAP). Avant de valider le formulaire d'authentification, il peut cocher la case Enregistrer mon identifiant OTP. Il peut alors renseigner l'utilisateur associé à sa clé OTP sur le serveur RSA, ainsi que son code PIN et le mot de passe actuel.



Le serveur SSO ne gère pas la saisie initiale du code PIN d'un utilisateur. Dans le cas d'un nouvel utilisateur, il faudra au préalable que celui-ci se connecte sur la mire RSA pour créer son code PIN.

Le serveur EoleSSO va vérifier l'authentification LDAP, puis va valider l'authentification auprès du serveur RSA. Si les deux authentifications réussissent, il va enregistrer l'identifiant de l'utilisateur sur le serveur RSA et va l'associer à l'utilisateur LDAP.

Par la suite, lorsque l'utilisateur revient sur la page d'authentification, le système détecte qu'il s'est déjà

enregistré (après saisie de son identifiant habituel). L'utilisateur a alors la possibilité de cocher la case 'Connexion par clé OTP'. Dans ce cas, il lui suffit de saisir son code PIN et mot de passe OTP pour s'authentifier.

5.4. 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-ssso reload
```

5.4.1. Ajout d'attributs calculés

Le principe est de créer un fichier `<nom_champ>.py` dans le répertoire `/usr/share/ssso/user_infos/` :

```
def calc_info(user_info):
```

```
.....
```

```
return liste_val
```

- `user_info` est le dictionnaire des données existantes (cf. paragraphe précédent), il est passé automatiquement à la fonction par le serveur SSO ;
- `liste_val` est une liste python contenant les valeurs à associer au champ `<nom_champ>`.

Pour que ces données soient envoyées aux applications clientes du SSO, il faut les mettre dans un filtre de données (cf. paragraphes suivants)

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 cela 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 (récupérés également dans l'annuaire) ;

- une entrée `info_groups` contenant un dictionnaire dont les clés sont l'attribut `cn` des groupes présents dans `user_groups` et les valeurs sont les attributs du groupe correspondant dans l'annuaire ldap. Seuls les attributs suivants sont conservés : `sambaGroupType`, `displayName`, `cn`, `objectClass`, `gidNumber`, `mail`, `description` et `niveau`.
- une entrée `dn` contenant le DN complet de l'utilisateur (utilisé pour récupérer le RNE d'origine d'un utilisateur dans le cas d'un annuaire multi-établissements).
- les entrées `rne` et `nom_etab` qui correspondent aux informations présentes dans la configuration Creole du serveur (ou dans le fichier de configuration du serveur EoleSSO le cas échéant).



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 avec 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 ;
- `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) ;
- `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()]
```

5.4.2. 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
```

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.

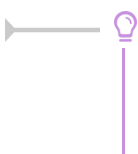
Les formats d'écriture suivants sont possibles :

- 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-ssso.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
- envoi d'un ticket PGT à un client CAS en mode proxy

5.4.3. 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/ssso/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 où 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 Authentication 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
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`

5.5. Fédération avec une entité partenaire

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO, ou vers d'autres 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.369] 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.

5.5.1. 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 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.366]), il est conseillé d'utiliser cette

solution dans le cadre d'un réseau sécurisé (par exemple, à travers un RVP). Le cas échéant, on préférera la solution proposée dans le paragraphe suivant.

5.5.2. Fédération SAML : Gestion des Associations

La solution retenue pour effectuer une fédération entre deux systèmes est l'utilisation de messages SAML^[p.369] 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 (metadata^[p.364]) 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).

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 fichiers, 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 où 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 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 réplification 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 métadatas 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`)
- `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 a 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 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.



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.

5.5.3. Fédération SAML : Gestion des méta-données

Pour permettre d'établir un lien de confiance avec une entité partenaire, le serveur EoleSSO utilise des fichiers métadonnées^[p.364] comme défini dans les standards SAML.

1. Envoi des informations du service EoleSSO à un partenaire :

- Le fichier métadonnées 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_eolessso>:8443/saml/metadata`
- Dans le cas où ils ne sont pas pris en compte depuis le fichier de métadonnées, 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 métadatas 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 métadatas 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.

5.5.4. Fédération SAML : Accès aux ressources

Activation des différents rôles dans un accord de fédération

Pour résumer, une fois les fichiers de métadatas 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.
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 Ajaxplorer (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 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**.

5.5.5. 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=....
```

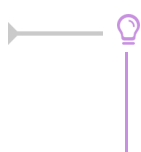
```
type_etab=....
```

```
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-ssso`, 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/utills/etabs.ini`. Cette application permet de rediriger automatiquement les utilisateurs vers les portails ENT auxquels ils ont accès (pour plus d'informations, se reporter aux annexes).

Aide au choix de la source d'authentification

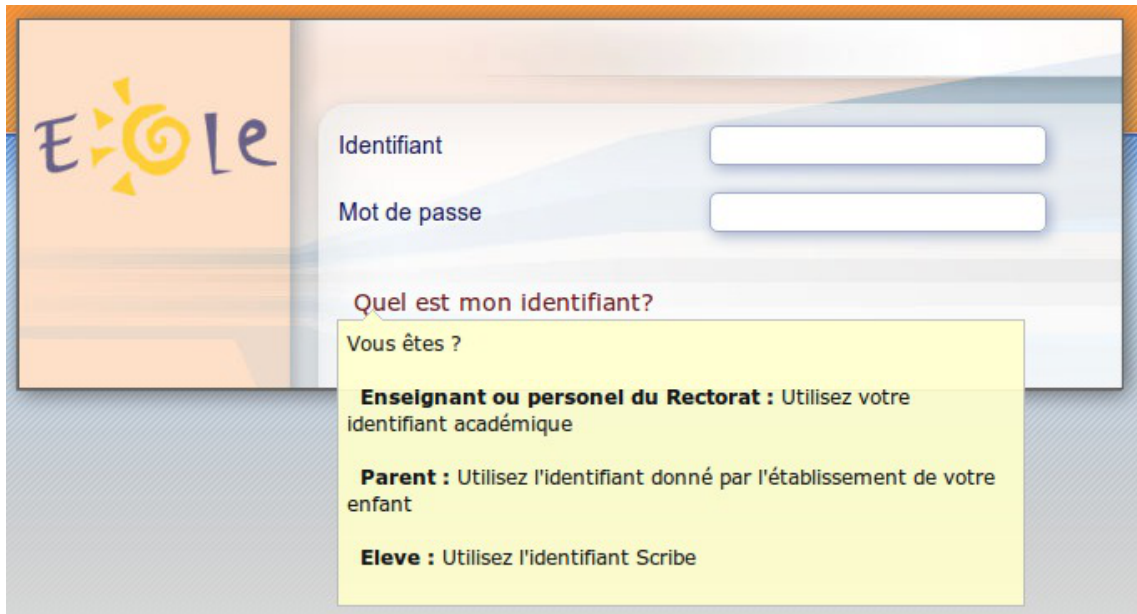
Lorsque des homonymes sont détectés, la mire d'authentification va générer la liste des choix disponibles.

Pour aider l'utilisateur dans sa décision, différentes informations sont affichées.

Si un fichier `/usr/share/sso/interface/login_help.tmpl` est présent, un lien apparaîtra sur la mire d'authentification (Quel est mon identifiant?). Un survol de ce lien avec la souris fait apparaître le contenu du fichier sous forme d'un cadre en surimpression (classes liées à `a.aide` dans la feuille de style).

Un exemple est fourni dans le fichier `/usr/share/sso/interface/login_help_example.tmpl`.

Le but de ce cadre est d'indiquer à l'utilisateur l'identifiant qu'il doit utiliser.



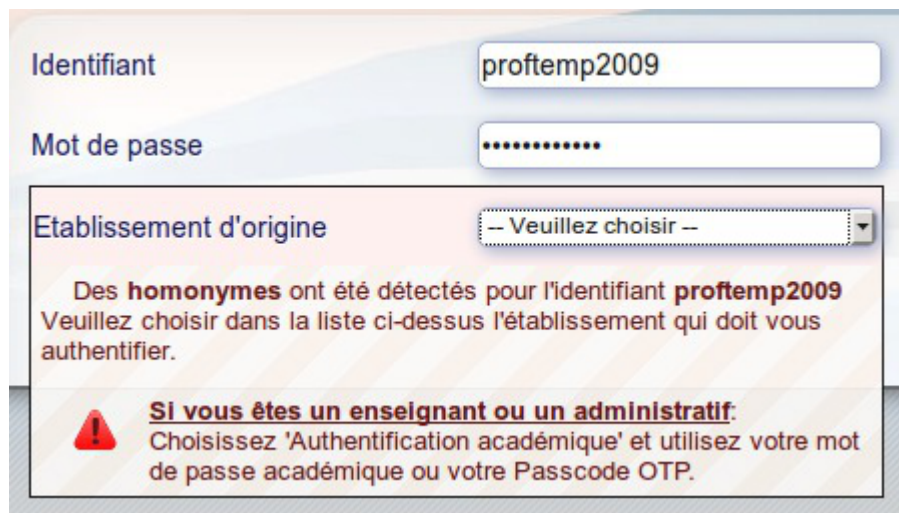
Un deuxième cadre d'information est affiché lorsque des homonymes ont été trouvés pour l'identifiant saisi par l'utilisateur (`#homonyme` et `#homonymetext` dans la feuille de style).

Le contenu de celui-ci est conditionné par les choix disponibles. Le but est d'aider à choisir parmi les sources proposées.

Le début du texte est générique et indique à l'utilisateur que plusieurs entrées sont disponibles pour l'identifiant renseigné.

Il est ensuite possible de spécifier un fichier d'information pour chaque annuaire LDAP, dont le contenu sera ajouté au cadre si l'identifiant entré y est présent (l'information doit donc être au format HTML).

Un exemple est fourni dans `/usr/share/sso/interface/personnel_acad.html`, et donne le résultat suivant :



Voir aussi...

➤ Onglet Eole sso : Configuration du service SSO pour l'authentification unique ^[p.121]

5.6. 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

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-ssso`, 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 :

```
/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).

5.7. Annexes

5.7.1. Résumé des fichiers et liens

Fichiers de configuration

Fichiers de base

- `/usr/share/sso/config.py` : fichier de configuration principal de l'application (sur un module Eole, la configuration est gérée via Creole)
- `/usr/share/sso/app_filters/*_apps.ini` : définition des applications et spécification du filtre à utiliser
- `/usr/share/sso/app_filters/*.ini` : fichiers de description des filtres d'attributs
- `/usr/share/sso/user_infos/*.py` : fonctions de calcul d'attributs supplémentaires
- `/usr/share/sso/interface/theme` : répertoire pour personnalisation de la CSS des pages d'authentification

Fichiers spécifiques au fonctionnement en mode SAML

- `/usr/share/sso/metadata/*.xml` : fichiers metadata des entités partenaires (doit contenir le certificat utilisé pour la signature des requêtes)
- `/usr/share/sso/metadata/attributes.ini` : définition des attributs requis/optionnels en tant que fournisseur de service (obsolète)
- `/usr/share/sso/attribute_sets/*.ini` : description de jeux d'attributs pour la fédération via SAML
- `/usr/share/sso/attribute_sets/associations*.ini` : fichiers de configuration des associations avec des fournisseurs d'identité

URL principales

Toutes les URL du service EoleSSO décrites ci-dessous commencent par `https://adresse_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 à vérifier (de type ST)
- `/proxyValidate?service=X&ticket=Y&pgtUrl=Z` : adresse de validation des tickets d'application CAS en mode proxy
 - `ticket` est le ticket à vérifier (de type ST ou PT) ;
- `/samlValidate` : adresse de validation des tickets CAS au format SAML 1. Les paramètres doivent être passés par méthode POST (méthode supportée par les client CAS java 3.1.X, phpCAS 1.1.0 et .NET CAS Client). Pour plus de détail sur, se reporter à la page http://en.wikipedia.org/wiki/SAML_1.1
 - `TARGET` : URL à laquelle la réponse doit être envoyée
 - Le corps de la requête doit contenir la requête SAML dans une enveloppe SOAP. Le ticket à valider est fourni comme valeur de l'élément AssertionArtifact
- `/proxy?pgt=X?targetService=Y` : adresse d'obtention d'un ticket de type proxy

URL spécifiques à SAML 2

- `/saml/metadata` : adresse de récupération des méta-données SAML du serveur (fournisseur d'identité et fournisseur de services)
- `/saml?sp_ident=X&RelayState=Y&index=Z` : adresse à utiliser pour envoyer une assertion d'authentification SAML à un fournisseur de services
 - `sp_ident` est l'identifiant de ce partenaire (ou le nom de son fichier metadata sans l'extension .xml)
 - `RelayState` est une information (URL ou autre) indiquant au partenaire où l'utilisateur doit être 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

5.7.2. Astuces d'exploitation

Journalisation du service

Le fichier de journalisation du service EoleSSO est `/var/log/eole-ssso.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 remplacez 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-ssso, 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-ssso reload
```

L'avantage de cette méthode par rapport à `CreoleService eole-ssso restart` est que les sessions des utilisateurs en cours sont conservées.

Les données suivantes sont prises en compte lors du rechargement :

- filtres d'attributs et description d'applications (situés dans `/usr/share/sso/app_filters`) ;
- jeu d'attributs et fichier de configuration d'associations (situés dans `/usr/share/sso/attribute_sets`) ;
- fichiers metadata des entités partenaires (situés dans `/usr/share/sso/metadata`) ;
- définitions d'attributs calculés (situés dans `/usr/share/sso/user_infos`).

5.7.3. Exemple de Fédération avec RSA/FIM

Préparation de la configuration FIM

Les données suivantes sont nécessaires pour configurer l'association dans FIM :

- Les méta-données du serveur EoleSSO : `wget https://<ip_serveur_sso>:8443/saml/metadata --no-check-certificate --outputfile=eolesso.xml`
- le certificat du serveur EoleSSO : `/etc/ssl/certs/eole.crt` (fichier par défaut, peut varier selon la configuration)

Si le certificat est au format PEM (c'est le cas du certificat par défaut sur un module EOLE), il faut le convertir au format DER : `openssl x509 -inform PEM -outform DER -in eole.crt -out`

`eole_der.crt`

Une fois converti, utiliser la commande `keytool` pour intégrer le certificat à un truststore du serveur RSA/FIM (ou créer un truststore spécifique à cette occasion). Sur notre serveur de test, ils sont situés dans `/appli/federation/rsa-fim-config/keystores`

Par exemple : `<chemin vers jdk>/bin/keytool -import -alias fs-ac-mon_acad-et-mon_etab-1.0 -keystore mon_truststore-trust.jks -file eole_der.crt`

Configuration du fournisseur d'identité :

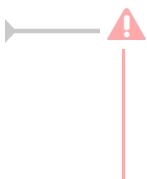
- aller dans Quick Setup -> add New Partner ;
- importer le fichier de méta-données `eolesso.xml` et donner un nom d'entité ;
- sauver dans la page suivante (association), choisir le fournisseur de service (FIM) ;
- cliquer sur l'onglet `general settings` et choisir les réglages suivants :
 - Encrypting/Signature truststores : sélectionner le truststore créé ci dessus ;
 - cocher la case `Transient Plug-in` ;
 - le greffon 'dictao cleartrust transient plugin' doit être sélectionné ;
 - attribute plugin : ajouter DictaoDumbAttributePluginRP ;
 - laisser les autres valeurs par défaut et sauver.

Configuration du serveur EoleSSO

La première étape est de récupérer le fichier de méta-données du fournisseur de service dans FIMConfig :

- Entities -> local entities -> manage existing ;
- cliquer sur le fournisseur, puis sur 'Export' dans le menu déroulant ;
- valider avec les valeurs par défaut, et copier le contenu affiché dans un fichier sur votre machine locale.

Placer ce fichier dans le répertoire `/usr/share/sso/metadata` (dans cet exemple, `fim_sp.xml`) du serveur EoleSSO et redémarrer le service.



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>`

5.7.4. Fédération entre 2 serveurs EoleSSO

Synopsis

On considère la situation suivante :

Un serveur Scribe en établissement (adresse : `Scribe_FI`) propose l'accès à des ressources protégé par un serveur Seshat (adresse : `Seshat_FS`) à travers son portail local.

Une réplication d'annuaire est en place entre les 2 serveurs (le serveur Seshat répliquant les annuaires de plusieurs établissements).

On souhaite que l'utilisateur se connecte sur le portail établissement du serveur Scribe, et accès à un application web du serveur Seshat (en saisissant une seule fois ses identifiants lors de la connexion au portail).

Pour permettre de retrouver les utilisateurs sur le fournisseur de service, on décide d'utiliser comme clé de jointure le champ FederationKey de l'annuaire de Scribe. Ce champ étant unique au niveau national, il n'y aura pas de problème



Se reporter à la partie traitant de la gestion des identifiants ENT dans la documentation Scribe pour plus d'informations sur la mise en place de l'attribut FederationKey

Configuration du fournisseur d'identité (module Scribe)

La première étape est de définir un filtre pour définir les attributs à envoyer au fournisseur de service dans l'assertion SAML.

Par défaut, le serveur EoleSSO utilise le filtre défini dans le fichier `/usr/share/sso/app_filters/saml.ini` si aucun filtre n'est spécifié pour l'adresse du fournisseur de service (pour information, cette adresse est `https://Seshat_FS:8443/saml/acs`).

Il n'y a ici rien à modifier car ce filtre envoie l'attribut FederationKey.

Configuration du fournisseur de service (Seshat)

Sur le fournisseur de service, il faut indiquer le jeu d'attributs à utiliser pour établir la correspondance entre les attributs donnés dans l'assertion SAML et les attributs présents dans l'annuaire de Seshat.

Ici aussi, la configuration par défaut convient. Si aucun jeu d'attribut n'est défini pour l'identifiant du 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-ssso` sur les 2 serveurs : `CreoleService eole-ssso 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

5.7.5. Mise en place de l'authentification OTP

Le service EoleSSO est capable de valider une authentification par clé OTP auprès d'un serveur RSA Authentication Manager (protocole SecurID).

Pour permettre ce fonctionnement, il est nécessaire d'installer sur le serveur un module PAM fourni par EMC.

Ce module est disponible à l'adresse suivante :

<http://france.emc.com/security/rsa-securid/rsa-authentication-agents/pam-7-1.htm>

La dernière version testée est la version 7.1.0.1. elle nécessite au minimum un serveur RSA Authentication Manager version 6.1 ou 7.1

Ce client n'est pas certifié pour fonctionner sur le système GNU/Linux Ubuntu, il peut être nécessaire de modifier le script d'installation présent dans l'archive pour qu'il s'exécute correctement sur un serveur EOLE (voir ci-dessous).



Adaptation du fichier `install_pam.sh` pour une installation sur un serveur EOLE :

- Remplacer les occurrences de `chmod 755` par `chmod 644` pour appliquer les permissions préconisées par la distribution.
- Rechercher la section concernant le paramétrage pour Linux (ligne 362 dans la version testée) :

```
'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_secured`)

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, vérifiez 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_secured.so` installé avec les versions 32 ou 64 bits qui peuvent être trouvées dans l'archive `sd_pam_agent.tar` du répertoire `/lnx` du répertoire d'installation de l'agent.

La librairie doit être installée dans le répertoire `/lib64/security/` dans le cas d'une version d'EOLE inférieure à 2.5.0 ou dans le répertoire `/lib/x86_64-linux-gnu/security/` dans le cas contraire.

5.7.6. Application de redirection : Eole-dispatcher

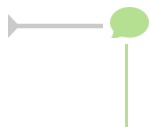
Dans le cadre de l'utilisation du module Seshat en tant que point d'entrée d'un ENT centralisé, l'application Eole-dispatcher permet de rediriger les utilisateurs vers leur établissement d'origine. Elle se base sur les informations remontées lors de la mise en place de la réplication des serveurs Scribe.

Il est prévu également pour gérer le cas de la multi-affectation pour les enseignants et les parents :

- 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 multi-affectation pour un élève ne se pose pas, puisque ce dernier ne peut pas être scolarisé dans deux établissements.

Eole-dispatcher est capable (au travers de ses filtres d'attributs) de gérer les sources d'authentification suivantes :

- LDAP Académique pour les agents de l'Éducation nationale ;
- LDAP Téléservices pour les parents et élèves ;
- LDAP local (Réplicat des serveurs Scribe) pour l'authentification des élèves et parents (si les téléservices ne sont pas déployés).



Le terme affectation est à prendre au sens large, il désigne l'appartenance d'une personne à un établissement.

Pré-requis

Cette application nécessite :

- la mise en place de la réplication LDAP des serveurs Scribe sur le serveur Seshat ;
- l'alimentation des annuaires des serveurs Scribe avec des extractions AAF **EXCLUSIVEMENT** ;
- la bonne saisie des numéros et libellés établissement sur les serveurs Scribe et Zéphir ;
- la configuration d'une fédération entre chaque serveur Scribe et le serveur Seshat (voir documentation EoleSSO au chapitre : Fédération entre 2 serveurs EoleSSO).

Installation

Le dispatcher est à installer sur le module Seshat, afin d'utiliser son portail EoleSSO comme portail unique d'authentification vers les ENT (Envole).

L'application n'est pas installée par défaut, saisissez les commandes suivantes sur le module Seshat :

```
# Query-Auto  
# apt-eole install eole-dispatcher
```

Une fois les paquets installés, il faut se rendre dans l'onglet **Application web** de l'interface de configuration du module et renseigner les paramètres suivants :

- **Portail académique (PIA)** : portail sur lequel seront redirigés les personnels académiques ;
- **Site par défaut** : adresse du site Internet dédié à l'ENT si aucun portail d'établissement n'est disponible pour l'utilisateur.

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'une 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.
```

Configuration

RNE : `id_fs`

`id_fs` est :

- soit l'identifiant du fournisseur de service (entityID tel que défini dans son fichier de méta données) ;
- soit le nom de son fichier de méta-données placé dans `/usr/share/sso/metadata/` (sans l'extension `.xml`).

Par simplicité il est possible de nommer le fichier metadata de nos entités partenaires (Serveur Scribe des établissements) par `<RNE>.xml` ; `id_fs` est alors le code RNE de l'établissement.

Libellé et adresse du portail des établissements : `URL_du_portail_Établissement`

EoleSSO, va générer automatiquement, à chaque redémarrage du service `eole-ssso`, un fichier dans `/var/www/html/edispatcher/utills/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](#) (cf. [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 s'affiche `aucun portail trouvé`

Veillez sélectionner l'établissement sur lequel vous souhaitez vous connecter.

! #1: [9741046U] 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 portail ARENA^[p.361].

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` (accessibles en externe) ;
- `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 sera proposée ou non.

Il faut donc permettre aux utilisateurs d'obtenir le bon portail en fonction de la zone où ils se trouvent.

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/utills/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/utills/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 renvoyer vers l'URL du portail académique <https://scoweb.ac-reunion.fr>.

La variable `arena` , permet de spécifier la zone ClearTrust associée au portail. Elle est 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>.

6. Activation et configuration de Bareos

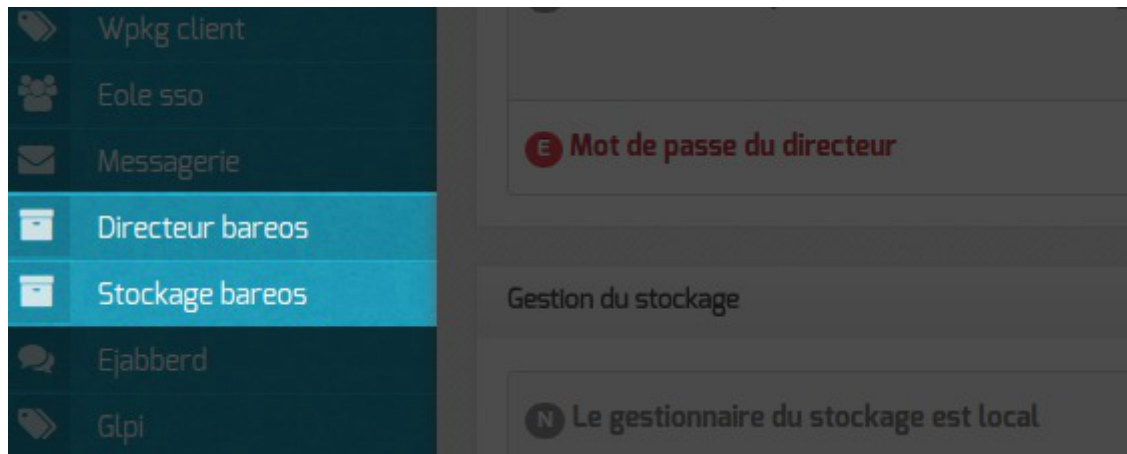
La sauvegarde du serveur et le support de stockage de la sauvegarde sont activés par défaut sur certains modules, il peuvent être activés/désactivés dans l'onglet `Services` de l'interface de configuration du module.

Two configuration rows are shown. The first row is labeled 'Activer la sauvegarde du serveur' with a dropdown menu set to 'oui'. The second row is labeled 'Activer le support de stockage de la sauvegarde' also with a dropdown menu set to 'oui'. Each row has a small icon to the right of the dropdown.

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.

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

The screenshot shows the 'Directeur bareos' configuration page. It has a title bar 'Directeur bareos' and a sub-section 'Configuration'. There are two main configuration items: 'Type de la base de données du catalogue' with a dropdown menu set to 'mysql', and 'Nom du directeur local' with a text input field containing 'scribe-dir'. Each item has a lock icon and a refresh icon.

Vue de l'onglet Directeur Bareos

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



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

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

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

Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention^[p.363] des différents espaces de stockage (totale, différentielle et incrémentale).

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

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



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

Pour cela, voici un exemple de configuration :

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

Avec la politique de sauvegarde suivante :

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

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



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

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

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

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

```
# bareosregen.sh
La régénération 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 stockage.

The screenshot shows a configuration window titled 'Vue de l'onglet Directeur Bareos'. It contains several settings:

- Mot de passe de la base de données MySQL de la sauvegarde:** A text field containing a long alphanumeric string.
- Délai alloué pour l'exécution complète d'une sauvegarde:** A numeric input field set to '0'.
- Niveau de compression des sauvegardes:** A dropdown menu set to 'GZIP6'.
- Mot de passe du directeur:** A text field containing another long alphanumeric string.

Below the settings is the label '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.

The screenshot shows a configuration window titled 'Stockage bacula'. Under the 'Configuration' section, there is a field for 'Nom du serveur de stockage' with the value 'horus-sd' entered.

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.

Configuration des accès distants au stockage

Nom du directeur Bareos distant

Nom du directeur Bareos distant

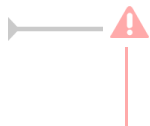
Adresse IP du directeur distant

Mot de passe Bareos distant

Montrer/Cacher

+ Nom du directeur Bareos distant

Autoriser des clients Bacula 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.240]

7. 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 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.373], 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
4 client_hosts: ['192.168.0.26']
5 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.373] 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 à 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**.


```

1 dbtype: mysql
2 dbname: taskfreak
3 dbuser: taskfreak
4 dbpass: "53nrgk>as="
5 createscript: "/usr/share/eole/db/taskfreak/gen/taskfreak-create.sql"
6 pwd_files:
7   - {file: '/var/www/html/taskfreak/include/config.php',
8     pattern: '$dbpass=',
9     owner: 'www-data:www-data',
10    mod: '600' }

```



L'option **pwd_files** accepte une liste de dictionnaires au format python.

```

1 pwd_files:
2   - {file: '/var/www/html/posh/includes/config.inc.php',
3     container: 'web',
4     pattern: 'define("__PASS", "',
5     end_pattern: ');',
6     owner: 'root:www-data',
7     mod: '660' }
8   - {file: '/usr/share/envole/eoledb/posh',
9     pattern: 'dbpassPOSH=" ',
10    owner: 'root:root',
11    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 où 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 '.

EoleDB détecte également si le caractère ; est requis en fin de ligne et l'ajoute après le **pattern**.



L'option **end_pattern** permet de maîtriser des cas non gérés par EoleDB, exemple

```
define('DBPASS': 'JeSuisUnMauvaisPassword');
pattern : "define('DBPASS': '"
end_pattern: ");",
```

Pour une application 3 modes de gestion de la base de données sont possibles et sont fonctions de la configuration :

- mode **default** : l'application utilise la configuration globale d'EoleDB ;
- mode **local** : l'application force l'utilisation d'un serveur de base de données local ;
- mode **externe** : l'application force l'utilisation d'un serveur de base de données et définit complètement la configuration.

Le mode default

Dans le mode **default**, l'application ne prend donc aucune liberté et sa configuration repose exclusivement sur la configuration d'EoleDB saisie dans l'onglet **Eoledb** de l'interface de configuration du module.



```
1 dbtype: mysql
2 dbname: taskfreak
3 dbuser: taskfreak
4 dbpass: "53nrgk>as="
5 createscript: "/usr/share/eole/db/taskfreak/gen/taskfreak-create.sql"
6 pwd_files:
7   - {file: '/var/www/html/taskfreak/include/config.php',
8     pattern: '$dbpass="',
9     owner: 'www-data:www-data',
10    mod: '600' }
```



Si le comportement d'EoleDB est changé, celui-ci impactera l'application.

Le mode local

Dans le mode **local** la configuration de l'application à utiliser un serveur de base de données local, il faut donc ajouter dans la configuration **dbhost** et **client_hosts**.

La configuration d'EoleDB saisie dans l'onglet **Eoledb** de l'interface de configuration du module est ignorée.

```

1 ---
2 dbhost: 127.0.0.1
3 dbtype: mysql
4 dbname: taskfreak
5 dbuser: taskfreak
6 dbpass: "task;Freak"
7 client_hosts: ["127.0.0.1", "localhost"]
8 createscript: "/usr/share/eole/mysql/taskfreak/gen/taskfreak-create.sql"
9 pwd_files:
10   - {file: '/var/www/html/taskfreak/include/config.php',
11     pattern: '$dbpass=',
12     owner: 'www-data:www-data',
13     mod: '600' }
```

Le mode externe

Dans le mode **externe** l'application définit 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.

```

1 ---
2 dbhost: 192.168.45.34
3 dbport: 3309
4 dbroot: adminDB
5 dbrootpwd: /root/.secrets-mydb
6 dbtype: mysql
7 dbname: taskfreak
8 dbuser: taskfreak
9 dbpass: "task;Freak"
10 client_hosts: ["127.0.0.1", "localhost", "192.168.0.14" ]
11 createscript: "/usr/share/eole/mysql/taskfreak/gen/taskfreak-create.sql"
12 pwd_files:
13   - {file: '/var/www/html/taskfreak/include/config.php',
14     pattern: '$dbpass=',
15     owner: 'www-data:www-data',
16     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` :

```
root@eolebase:~# apt-eole install eole-phpmyadmin
```

Éditer le configuration du serveur à l'aide de la commande de l'interface de configuration du serveur :

```
root@eolebase:~# gen_config
```

Dans l'onglet `t Applications web`, la variable minimum à renseigner est `Nom de domaine des applications web (sans http://)`, il est possible d'activer l'application phpMyAdmin et de la choisir comme application web par défaut.

Reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
root@eolebase:~# reconfigure
```

Vérifier dans un navigateur web que le serveur répond.

Modifier le mot de passe par défaut du compte root mysql avec la commande `mysql_pwd.py` :

```
root@eolebase:~# mysql_pwd.py
```

```
## Réinitialisation des mots de passe Mysql ##
```

```
Nouveau mot de passe root mysql : eole21
```

```
Voulez-vous que les autres mots de passe soient modifiés ? [oui/non] [non]
```

```
: non
```

```
root@eolebase:~#
```

Se connecter à MySQL avec l'utilisateur root :

```
root@eolebase:~# mysql -u root -h localhost -peole21
```

Créer un utilisateur autre que `root` (le mot de passe du compte `root` est généré à chaque `reconfigure`) et lui donner les privilèges et l'autorisation de se connecter depuis le serveur hébergeant EoleDB :

```
mysql> grant all privileges on *.* to admin@<IPServeurEoleDB> identified by "eole21";
```

```
mysql> quit
```

Pour ouvrir le port il faut faire un dictionnaire personnalisé `00_mysql.xml` à placer dans `/usr/share/eole/creole/dicos/local/`

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <creole>
3   <files>
4     <service_access service='mysql'>
5       <port>3306</port>
6       <tcpwrapper>mysqld</tcpwrapper>
7     </service_access>
8   </files>
9   <variables />
10  <constraints />
11  <help />
12 </creole>
13 <!-- vim: ts=4 sw=4 expandtab
14 -->
```

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>
```

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`.

```
1 root@scribe:~# eole_db_gen -b /var/backup/eole-db
2 TASKFREAK :
3 >>> Passwords [OK]
4 >>> Create [OK]
5 >>> Update [OK]
6 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 à 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

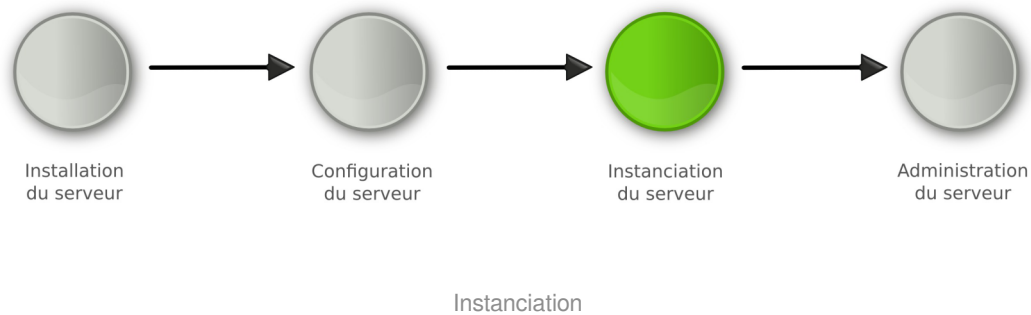
Pour connaître les différents paramètres de la commande `eole_db_gen` :

```
# eole_db_gen --help
```

Chapitre 5

Instanciation du module

La troisième des quatre phases



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` .

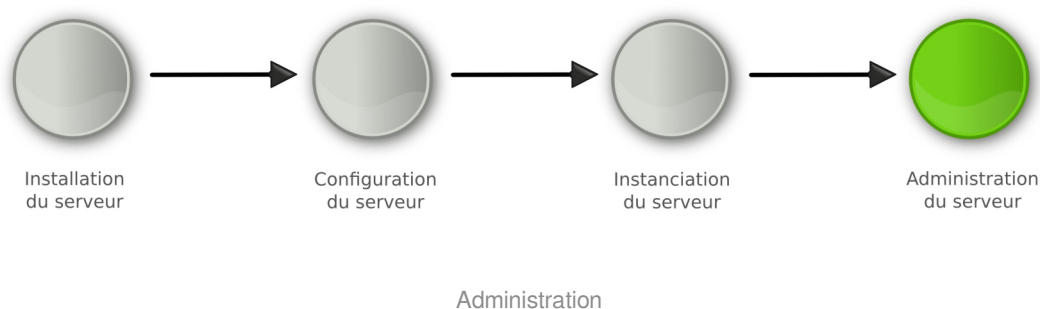
L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

À l'issue de cette phase, le serveur est utilisable en exploitation.

Cette phase doit être complétée par un diagnostic complet du module à l'aide de la commande `diagnose -L` .

Chapitre 6

Administration du module Horus



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.

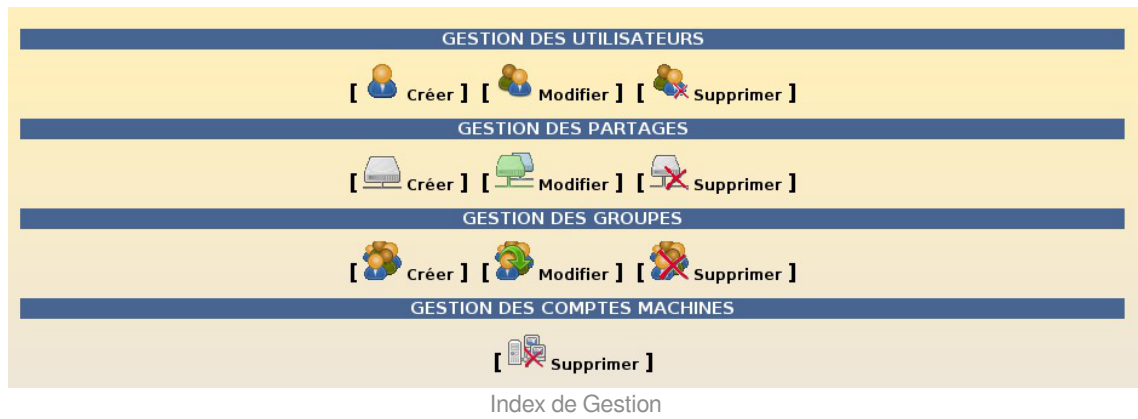
1. Fonctionnalités de l'EAD propres au module Horus

1.1. Gestion des comptes Horus

Le menu **Gestion** est dédié à la gestion des utilisateurs, des groupes, des clients et des partages du module Horus.

Index

Le sous-menu **Index** présente sur une seule page des raccourcis vers toutes les actions possibles du menu **Gestion**.



1.1.1. Gestion des groupes

Le sous-menu **Groupes** permet de créer, modifier et supprimer les groupes d'utilisateurs Horus.

Créer un groupe

Le formulaire de création d'un groupe Horus est découpé en 3 blocs distincts :

GESTION DES GROUPES

CRÉER UN GROUPE

Nom du groupe

UTILISATEURS [-] [+]

A B C D E F G H I J K L M N
 O P Q R S T U V W X Y Z
 Tous

| Utilisateurs disponibles | | Utilisateurs du groupe |
|--|--|------------------------|
| Tout Aucun Inverser <input type="checkbox"/> admin <input type="checkbox"/> test | ➔ Ajouter ➜ Retirer | Tout Aucun Inverser |

GROUPES [-] [+]

Groupes existants:

- DomainAdmins (Réservé eole)
- DomainUsers (Réservé eole)
- PrintOperators (Réservé eole)
- applidos (Réservé eole)
- minedu (Réservé eole)

PARTAGES [-] [+]

Ajouter des partages et les lier au groupe
 Liste des partages associés au groupe

Nom du partage (sans accent)

➔
Ajouter

➜
Retirer

[✓ Valider]

Création d'un groupe dans l'EAD

Pour créer un groupe, seul le *Nom du groupe* est requis (premier bloc).

Il est possible d'inscrire un ou plusieurs utilisateurs existants au groupe dès sa création (deuxième bloc).

Il est enfin possible d'affecter un ou plusieurs nouveaux partages au groupe dès sa création (troisième

bloc).

Modifier un groupe

Une liste déroulante permet de sélectionner le groupe à éditer.

Une fois le groupe choisi, deux blocs similaires à ceux du formulaire de création de groupe apparaissent.

Ils permettent respectivement d'inscrire/désinscrire des utilisateurs au groupe et d'ajouter/supprimer des partages au groupe.

Modification d'un groupe dans l'EAD

⚠ Les groupes suivis de la mention (Réservé EOLE) sont des groupes spéciaux qu'il faut manipuler avec précaution.

💡 Le fait de supprimer la liaison entre un partage et un groupe (ou de supprimer le groupe lui-même) entraîne la suppression du partage dans l'annuaire mais pas celle de ses données. Il est donc possible de les récupérer en créant un nouveau partage du même nom (ou un partage utilisant le même chemin).

Pour ce genre de manipulation, il est préférable d'utiliser les actions du sous-menu **Partages**

Supprimer un groupe

Une liste déroulante permet de sélectionner le groupe à supprimer.

Les groupes spéciaux ne sont pas supprimables et n'apparaissent pas dans cette liste.

1.1.2. Gestion des utilisateurs

Le sous-menu **Utilisateurs** permet de créer, modifier et supprimer les utilisateurs Horus.

Le formulaire de création d'utilisateur Horus est assez simple.

The screenshot shows a web interface titled "GESTION DES UTILISATEURS" with a sub-section "CRÉER UN UTILISATEUR". On the left, there are navigation buttons: "Créer", "Modifier", and "Supprimer", along with a list of existing users: "admin" and "test". The main form contains the following fields and options:

- Nom de l'utilisateur: utilisateur
- Mot de passe: masked with 10 dots
- Forcer la modification du mot de passe à la 1ère connexion:
- Profil utilisateur: obligatoire (dropdown)
- Groupe principal: DomainUsers (dropdown)
- Quota utilisateur: 50 (input)
- Lettre de lecteur ('U:' conseillé): U: (dropdown)
- Activer l'utilisateur:
- Activation du shell (gestion de clients Linux):
- Membre du groupe DomainAdmins:
- Copier les groupes d'un autre utilisateur: (dropdown)

At the bottom right, there is a "Valider" button with a green checkmark icon.

Création d'un utilisateur dans l'EAD d'Horus

Pour créer un utilisateur, le *Nom de l'utilisateur* (login) et son *Mot de passe* sont requis.

Il est également possible de préciser :

- si l'utilisateur doit changer son mot de passe lors de sa première connexion Samba ;
- le profil Windows affecté à l'utilisateur ;
- le groupe principal de l'utilisateur ;
- un quota disque à affecter à l'utilisateur (en Mo) ;
- la lettre de lecteur utilisée pour monter son répertoire personnel ;
- si le compte utilisateur est activé ;
- si l'utilisateur dispose d'un shell Linux (nécessaire pour l'utilisation de clients GNU/Linux) ;
- si l'utilisateur est membre du groupe *DomainAdmins*.

La dernière option permet de récupérer la liste des groupes d'un autre utilisateur afin d'y inscrire le nouvel utilisateur (très pratique lors de la création de plusieurs utilisateurs à la chaîne).

⚠ DomainAdmins

Il est fortement **déconseillé** d'inscrire les utilisateurs au groupe *DomainAdmins*.

Cela leur donnera un accès en lecture et en écriture sur tous les partages y compris les répertoires personnels de tous les utilisateurs (*admin* inclus).

Modifier un utilisateur

Une liste déroulante permet de sélectionner l'utilisateur à éditer.

Une fois l'utilisateur choisi, trois blocs apparaissent.


Ils permettent respectivement :


- de modifier les paramètres spécifiques à l'utilisateur ;
- d'inscrire/désinscrire l'utilisateur à des groupes ;


- d'associer un rôle EAD à l'utilisateur (également possible *via* le menu **Édition de rôles**).

GESTION DES UTILISATEURS

MODIFIER UN UTILISATEUR

 **Créer**

 **Modifier**

 **Supprimer**

Nom de l'utilisateur

Mot de passe

Forcer la modification du mot de passe à la prochaine connexion

Profil utilisateur

Groupe principal

Quota utilisateur

Lettre de lecteur ('U:' conseillé)


Activer l'utilisateur

Activation du shell (gestion de clients Linux)

Copier les groupes d'un autre utilisateur

Associer des groupes à l'utilisateur

| Groupes disponibles | | Groupes de l'utilisateur |
|---|--|--------------------------------------|
| <input type="checkbox"/> Tout <input type="checkbox"/> Aucun <input type="checkbox"/> Inverser | <div style="color: red; font-size: 2em;">←</div> Retirer <div style="color: green; font-size: 2em;">→</div> Ajouter <div style="color: green; font-size: 1.5em;">[✓ Valider]</div> | <input type="checkbox"/> DomainUsers |
| <input type="checkbox"/> DomainAdmins <input type="checkbox"/> PrintOperators <input type="checkbox"/> applidos <input type="checkbox"/> comptabilite <input type="checkbox"/> minedu | | |


Associer un rôle à cet utilisateur

Modification d'un utilisateur dans l'EAD d'Horus

Les paramètres utilisateurs modifiables sont :

- le mot de passe de l'utilisateur ;
- forcer l'utilisateur à changer son mot de passe lors de sa prochaine connexion Samba ;
- le profil Windows affecté à l'utilisateur ;
- le groupe principal de l'utilisateur (à utiliser avec précaution) ;
- le quota disque affecté à l'utilisateur (en Mo, mettre 0 pour ne pas avoir de limite) ;
- la lettre de lecteur utilisée pour monter son répertoire personnel ;
- l'activation/la désactivation du compte utilisateur ;
- l'activation/la désactivation du shell Linux pour l'utilisateur (nécessaire pour l'utilisation de clients Linux) ;
- l'inscription de l'utilisateur aux groupes d'un autre utilisateur.

Supprimer un utilisateur

Une liste déroulante permet de sélectionner l'utilisateur à supprimer.

Vous pouvez choisir de conserver ou de supprimer le répertoire personnel (fichiers et répertoires) de

l'utilisateur.

1.1.3. Gestion des partages

Le sous-menu **Partages** permet de créer, modifier et supprimer les partages Horus.

Créer un partage

Le formulaire de création de partage est composé du formulaire lui-même et d'un tableau récapitulant les lettres de lecteurs déjà réservées pour d'autres partages.

| Lettres de partages déjà attribuées | |
|-------------------------------------|----|
| groupes | S: |
| minedu | X: |
| icones\$ | R: |
| applidos | F: |

Création d'un partage dans l'EAD d'Horus

Pour créer un partage, seuls les *Nom du partage* et nom du *Groupe associé* sont requis.

Si le groupe associé au partage n'existe pas, il sera créé avec les paramètres par défaut.

Il est également possible de préciser :

- le chemin du partage sur le serveur Horus (par défaut : `/home/workgroups/<partage>`) ;
- une lettre de lecteur à associer à ce partage (exemple : `L :`) ;
- si le *sticky bit* doit être activé sur le partage (seul le propriétaire du fichier pourra effacer ces fichiers) ;
- le modèle de partage à utiliser pour générer la section associée au partage dans la configuration Samba.

⚠ activation du sticky bit

Le "sticky bit" était nécessaire au fonctionnement de certaines applications mais il ne devrait plus être utilisé.

💡 Les modèles de partage

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

Par défaut, les partages utilisent le template Python :

```
/usr/share/eole/fichier/models/standard.tpl
```

Si vous souhaitez personnaliser certains partages (exemple : activer le *mode invité* sur un partage), il est possible de créer de nouveaux *templates* de partage dans ce même répertoire.

Les modèles créés apparaissent alors dans l'EAD et il devient possible de les affecter à un ou plusieurs partages.

Configuration du contrôleur de domaine (cf. Configuration du contrôleur de domaine)

Modifier un partage

Une liste déroulante permet de sélectionner le partage à éditer.

Une fois le partage choisi, il est possible de modifier :

- la lettre de lecteur associée au partage ;
- le modèle de partage à utiliser.

Supprimer un partage

Une liste déroulante permet de sélectionner le partage à supprimer.

Les partages spéciaux ne sont pas supprimables et n'apparaissent pas dans cette liste.

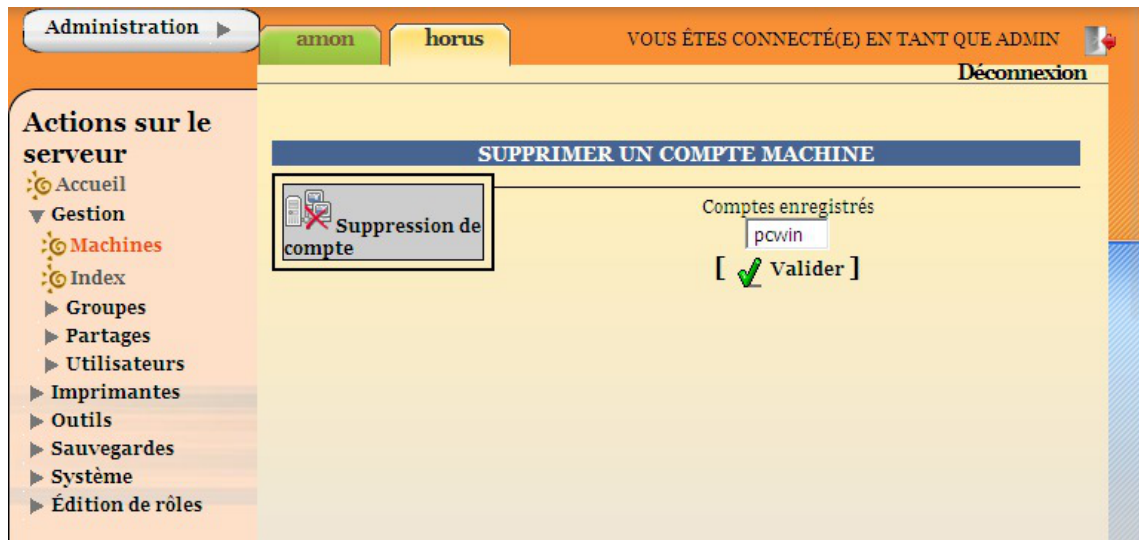


Supprimer un partage dans l'EAD d'Horus

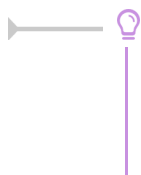
Vous pouvez choisir de conserver ou de supprimer les données (répertoire) du partage .

1.1.4. Suppression des comptes de machine

Le sous-menu **Machines** permet de consulter la liste des stations Windows enregistrées dans l'annuaire et, si nécessaire, de supprimer l'un de ces comptes de machine.



Supprimer une machine dans l'EAD d'Horus



La ré-inscription d'une station dans le domaine (formatage et réinstallation d'une machine avec un nom identique) peut parfois renvoyer une erreur.

La suppression du compte de la station peut aider à résoudre le problème.

1.2. Les ACLs

Des ACLs^[p.361] sont utilisées sur le système de fichiers pour permettre un réglage fin des droits d'accès aux partages et à leur contenu.

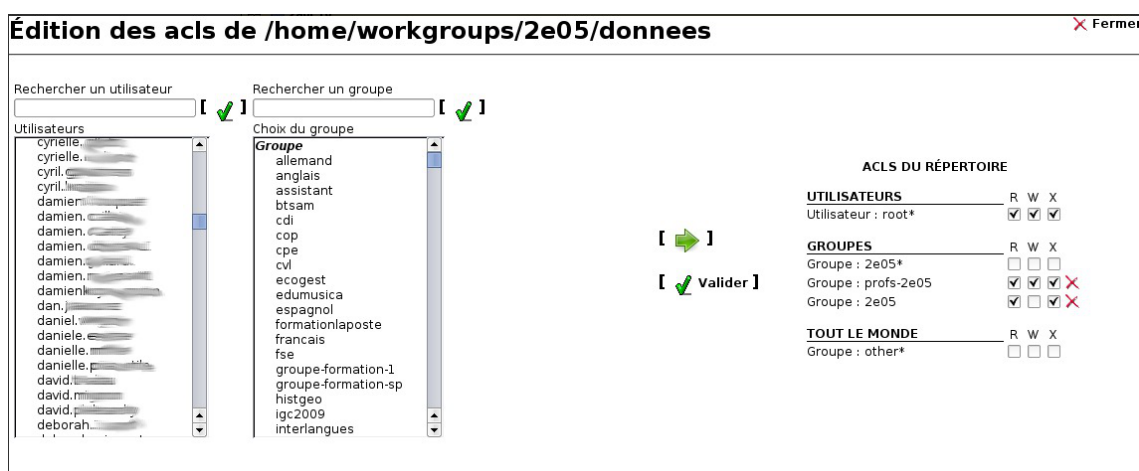
Modification des ACL sous Windows

Avec un utilisateur ayant les privilèges nécessaires, depuis un poste client Windows, clic droit sur le fichier/dossier => Propriétés => Sécurité ;

Modification des ACL dans l'EAD

Le menu Outils/Gestion des Acls permet de modifier les ACLs^[p.361] (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.



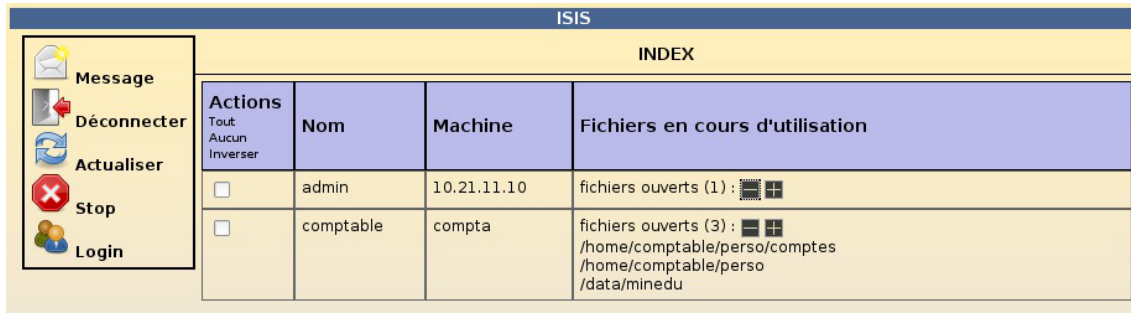
Interface de gestion des ACLs

Le caractère "*"

L'étoile indique que l'utilisateur ou le groupe en question est propriétaire du fichier ou du répertoire au niveau des droits Unix.

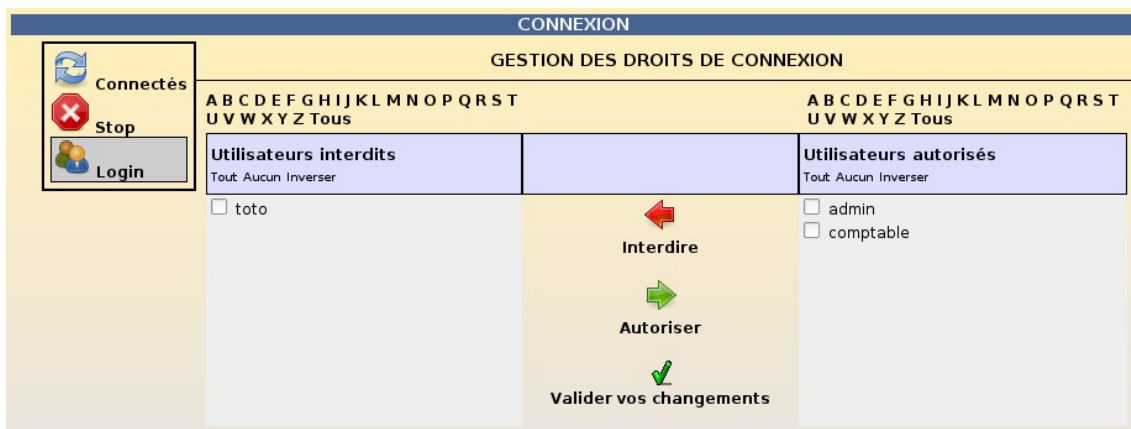
1.3. Gestion des connexions

Le sous-menu **Connexion** permet de lister les utilisateurs connectés, les fichiers ou dossiers ouverts, d'écrire à ces utilisateurs, de les déconnecter et de gérer l'activation/la désactivation des comptes.



Affichage des utilisateurs connectés

- le bouton **Message** permet de rédiger un message de type *Winpopup* à envoyer aux utilisateurs sélectionnés ;
- le bouton **Déconnecter** permet de déconnecter et désactiver les comptes des utilisateurs sélectionnés ;
- le bouton **Actualiser** met à jour la liste des connectés et de leurs fichiers ;
- le bouton **Stop** permet de déconnecter et désactiver tous les comptes ;
- le bouton **Login** permet d'accéder au formulaire de gestion de l'activation des comptes. La fenêtre suivante s'ouvre :



Activation/Désactivation des comptes

Le formulaire de gestion de l'activation des comptes permet de gérer l'activation/la désactivation des comptes utilisateurs d'une manière globale.

Les boutons **Connectés** et **Stop** permettent d'accéder aux actions décrites précédemment.

1.4. Quotas disque

Fonctionnement des quotas disque

Il est possible, pour chaque utilisateur, de limiter la quantité de données qu'il peut stocker sur le serveur en lui imposant un quota disque maximum.

Les quotas sont composés d'une limite douce (soft) et d'une limite dure (hard).

Les règles suivantes s'appliquent à l'utilisateur :

- il ne peut pas dépasser la limite dure ;
- il peut dépasser la limite douce pendant 7 jours ;
- passé ce délai, seule la limite douce est prise en compte et il est obligé de supprimer des données afin de repasser en dessous de celle-ci ;
- à partir de là, le processus de la limite douce/dure reprend et l'utilisateur peut à nouveau dépasser la limite douce pour une durée maximale de 7 jours.

Dans l'EAD, c'est la limite douce qui est indiquée.

Sur les modules Scribe et Horus, la limite dure vaut le double de la limite douce.

Les quotas sur le module Horus

Le sous-menu **Quotas disque** permet de connaître l'espace disque utilisé par chaque utilisateur et de repérer les éventuels dépassements de quotas disque alloués.

| Utilisateur | Espace utilise | Delai |
|-------------|----------------|---------|
| admin | 0 (Mo) | |
| toto | 52/50 (Mo) | 6 jours |
| titi | 1 (Mo) | |

Le tableau indique, pour chaque utilisateur du domaine, le rapport entre l'espace disque utilisé et l'espace disponible.

La colonne de droite précise le délai accordé aux utilisateurs dépassant le quota pour purger leurs fichiers.

Désynchronisation des quotas disque

Il peut arriver qu'il y ait une désynchronisation entre l'utilisation réelle du disque et le système de vérification des quotas.

Cela se traduit généralement par le fait que des utilisateurs sont considérés à tort comme dépassant leur quota disque.

La commande `quotacheck` permet de corriger le problème. Son utilisation demande quelques précautions.

Exemple d'utilisation de quotacheck sur le module Scribe où `/home` est la partition utilisée pour les données et les quotas utilisateurs.

1. arrêter les différents services susceptibles d'écrire sur la partition (samba, proftpd, exim4, ...);
2. démonter les éventuels montages liés à cette partition (images ISO, ...);
3. désactiver les quotas sur la partition : `quotaoff /home` ;
4. lancer la vérification des quotas : `quotacheck -vug /home` ;
5. réactiver les quotas sur la partition : `quotaon /home` ;
6. remonter les partitions : `mount -a` ;
7. démarrer les services précédemment arrêtés.

Pour le module Horus, il faut remplacer `/home` par `/data`.

1.5. Observation des virus

Le menu `Outils/` 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.

| GESTION DES CONNEXIONS | |
|---|--|
| VIRUS DÉTECTÉS | |
| Le 12 janvier, le virus WormKiller a été détecté dans le fichier <code>/home/e/eleve.test/perso/joli.scr</code> | |
| Le 11 janvier, le virus Eicar-Test-Signature a été détecté dans le fichier <code>/home/a/admin/perso/test.txt</code> | |

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`

1.6. Scripts administratifs

Le sous-menu `Scripts administratifs` permet de lancer l'exécution des scripts de pre/post installation

pour les applications nationales.

Ces scripts sont fournis à l'équipe EOLE par le Pôle Ingénierie, Hébergement National et Expertise Technique de Paris, anciennement CAPTI (adresse à usage académique : <http://pole.in.ac-paris.fr>).



Exécution de scripts administratifs dans l'EAD

Le formulaire d'*Exécution de scripts administratifs* présente la dernière version de chaque script sous la forme d'une liste déroulante.

Une fois l'application nationale installée sur Horus, il suffit de choisir le script de post-installation associé et de cliquer sur le bouton **Exécuter**.



Il est possible d'ajouter un script en respectant les règles suivantes :

- le fichier doit être placé dans le répertoire : `/usr/share/minedu/scripts`
- il doit être exécutable et posséder l'extension `.sh`
- il doit contenir une ligne de commentaire spéciale débutant par `#MENU=`

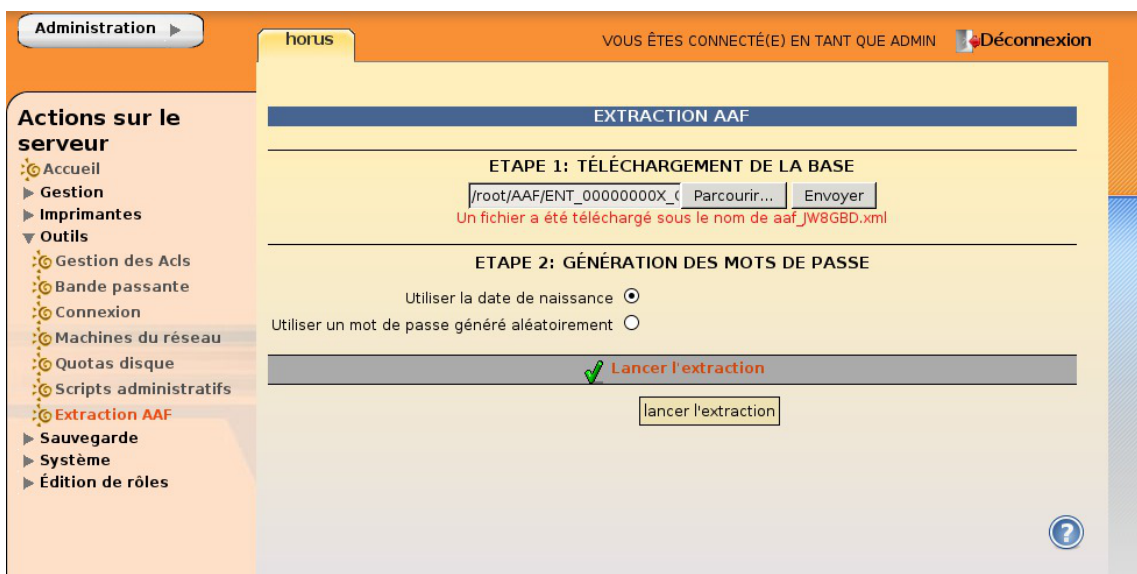
1.7. Extraction AAF

Le sous-menu **Extraction AAF** permet de créer des comptes pour les personnels administratifs de l'établissement à partir d'informations extraites de l'annuaire fédérateur (AAF).

Le fichier XML des personnels doit être fourni par l'Académie.

Le nom de ce fichier est traditionnellement de la forme :

`ENT_<rne_etablissement>_Complet_<date>_PersEducNat_0000.xml`





N'oubliez pas de cliquer sur le bouton **Envoyer** pour que votre fichier soit bien téléchargé.

Le bouton **Lancer l'extraction** permet de lancer les traitements.

Pour chaque personnel administratif défini dans le fichier extrait d'AAF, un compte de la forme "prenom.nom" sera créé.

Par défaut les utilisateurs seront inscrits à un groupe correspondant à leur fonction au sein de l'établissement (direction, assistant,...).

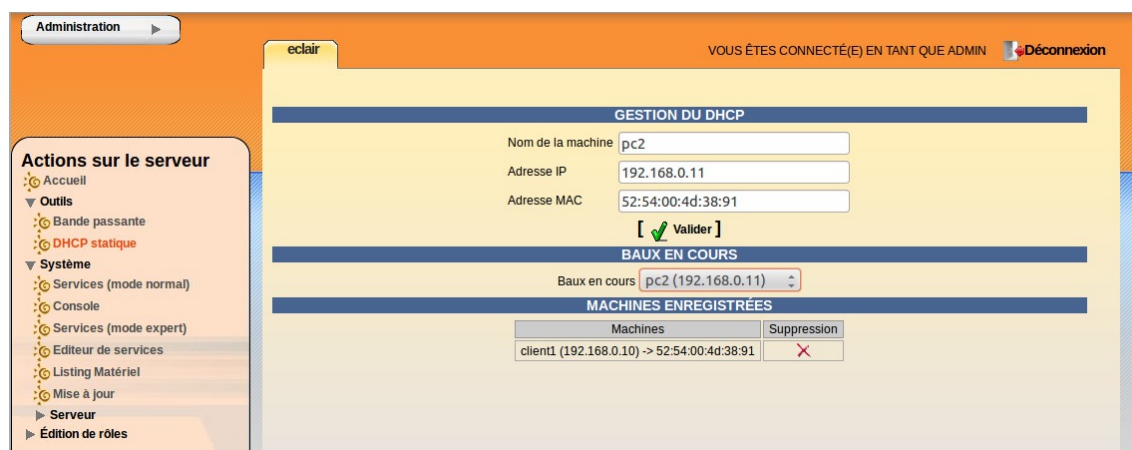


Dans la version actuelle du programme, les mots de passe attribués aux nouveaux utilisateurs sont stockés dans le fichier `/tmp/passwords.csv`.

1.8. Réserveation 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.



Réserveation d'adresse dans l'EAD

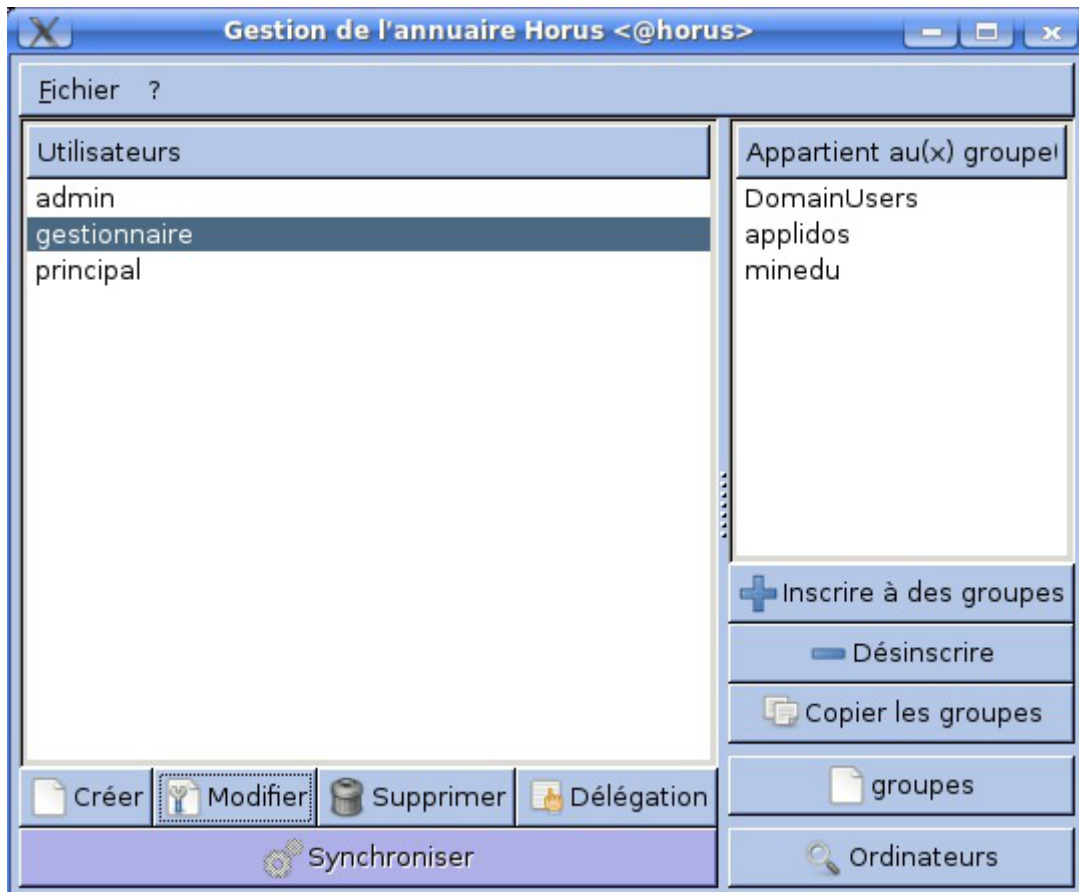
Pour associer un nom et une adresse IP à une machine, il faut connaître son adresse MAC.

Pour faciliter les enregistrements, les informations sur les stations déjà connues du serveur DHCP sont directement réutilisables.

Pour cela, il suffit de sélectionner la machine souhaitée au niveau de la liste déroulante **Baux en cours**.

2. Gestion des utilisateurs sur le module Horus

L'outil Frontend Horus est composé d'un serveur installée sur le module Horus et d'une interface graphique GTK^[p.365] permettant de gérer facilement les utilisateurs, les groupes et les partages sur le module.



L'outil Frontend Horus

Utilisateurs autorisés

Les utilisateurs autorisés à utiliser l'outil Frontend Horus sont :

- l'utilisateur `admin`
- les autres utilisateurs LDAP dans la mesure où une délégation de droit leur a été attribué.

Principales fonctionnalités

- création/modification/suppression d'utilisateur ;
- délégation de droits sur les membres d'un groupe ;
- importation d'utilisateurs en masse (Fichier/Import d'utilisateurs) ;
- création/modification/suppression de groupe et de partage.

Format du fichier d'importation d'utilisateurs

Le fichier d'importation doit être au format CSV^[p.362] avec séparateur point-virgule et comporter les champs suivants :

- login
- groupes (séparés par des virgules)
- lettre de lecteur
- mot de passe

Exemple : `toto;minedu,applidos;U;pass`

Le serveur sur le module

La partie serveur est installée sur le module Horus mais doit être activé.

Son activation est possible via l'interface de configuration du module, dans l'onglet `Services`, passer `Activation du service horus_frontend` à `oui`.



Le client et le serveur utilisent le port 7080 pour communiquer.

L'état d'activation du serveur associé à l'outil Frontend Horus est disponible par la commande `diagnose`.

Le client Frontend Horus sur le serveur

Le client Frontend Horus est pré-installé sur le serveur Horus (paquet nommé `frontend-horus`).

Le client s'exécute à l'aide la commande : `frontend_horus`.

Le client Frontend Horus pour GNU/Linux

Le client Frontend Horus peut être installé sur une machine cliente GNU/Linux.

Ce client est téléchargeable sur le FTP du projet à l'adresse à l'adresse :

`ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-ng.tar.gz`

Il faut procéder au désarchivage :

```
$ tar xvzf frontend-horus-ng.tar.gz
```

Pour exécuter le client :

```
$ cd frontend-horus
```

```
$ ./frontend.py
```



L'application requiert l'installation de `python`, `python-gtk2` et `python-glade2` sur la machine.



Des scripts python proposant des fonctionnalités équivalentes sont disponibles dans le répertoire `/usr/share/eole/backend`.

Le client Frontend Horus pour Windows

Le client Windows est téléchargeable sur le FTP du projet à l'adresse :

`ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-setup.exe`

3. Les sauvegardes

3.1. Généralités sur la sauvegarde

La sauvegarde^[p.369] 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.369] :

- 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.

3.1.1. 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.

3.1.2. 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.

3.1.3. Sauvegarde différentielle

Une **sauvegarde différentielle** réalise une copie des fichiers créés 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.

3.1.4. Des outils de sauvegarde

Les systèmes GNU/Linux embarquent depuis toujours des outils unitaires d'archivage qui permettent de réaliser des embryons de stratégie de sauvegarde.

Ainsi des outils tels que la commande `tar` permettent de créer des archives sur des médias locaux (disques, ou lecteurs de bandes).

Via des scripts se basant sur les dates de modifications, il est possible d'implémenter les méthodes de sauvegarde détaillées dans les paragraphes précédents.

Des outils plus complexes, et souvent propriétaires, ont été développés depuis, pour faciliter la création de ces sauvegardes (gestion du contenu à sauvegarder), mais aussi pour faciliter la gestion du calendrier de sauvegarde (programmation des tâches et des successions de sauvegardes).

Enfin, la plupart de ces outils intègrent la gestion de la restauration, avec la possibilité de choisir la date cible à restaurer.

Les solutions logicielles les plus connus sont :

- **Tivoli Storage Manager** (TSM) - IBM
 - <http://www-306.ibm.com/software/tivoli/products/storage-mgr/>
- **Time Navigator** - Atempo
 - <http://fr.atempo.com/products/timeNavigator/default.asp>
- **Networker** - EMC/Legato
 - <http://france.emc.com/products/detail/software/networker.htm>
- **ARCserve Backup** - Computer Associate
 - <http://www.ca.com/us/data-loss-prevention.aspx>
- **Arkeia Network Backup** - Arkeia

- <http://www.arkeia.com/products/arkeianetworkbackup/index.php>
- **Bacula** - Bacula
 - <http://bacula.org>
- **Bareos** - Bareos
 - <http://www.bareos.org>

3.2. La sauvegarde EOLE

EOLE 2.5 utilise l'outil de sauvegarde libre **Bareos**.

Backup Archiving REcovery Open Sourced 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.369]
- les ACLs^[p.361]

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.

3.2.1. 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>

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:

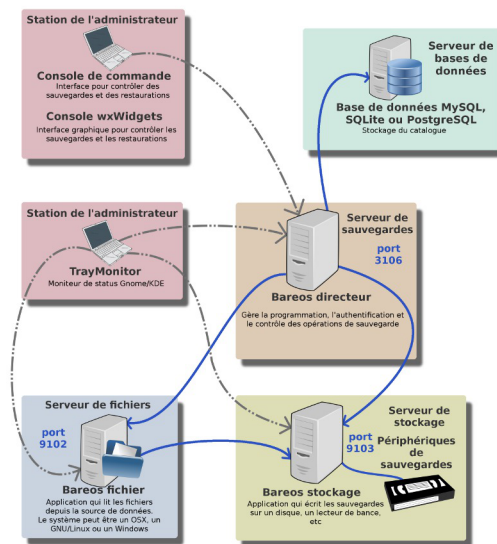
- les fichiers de configuration ;
- la base de données.

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.

<http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-1150008.9>

3.2.2. Architecture de Bareos

Bareos est construit suivant une **architecture distribuée** :



Architecture distribuée de Bareos

Noter que ces applications peuvent fonctionner sur moins de machines que celles indiquées ici. Vous pouvez tout faire sur une machine si vous voulez seulement sauvegarder un disque local sur une cassette ou sur un disque locale.

Les numéros de ports indiqués sont ceux par défaut et peuvent être changés.

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 et 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.

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.*

3.2.3. 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.

3.2.3.a. Activation et configuration de Bareos

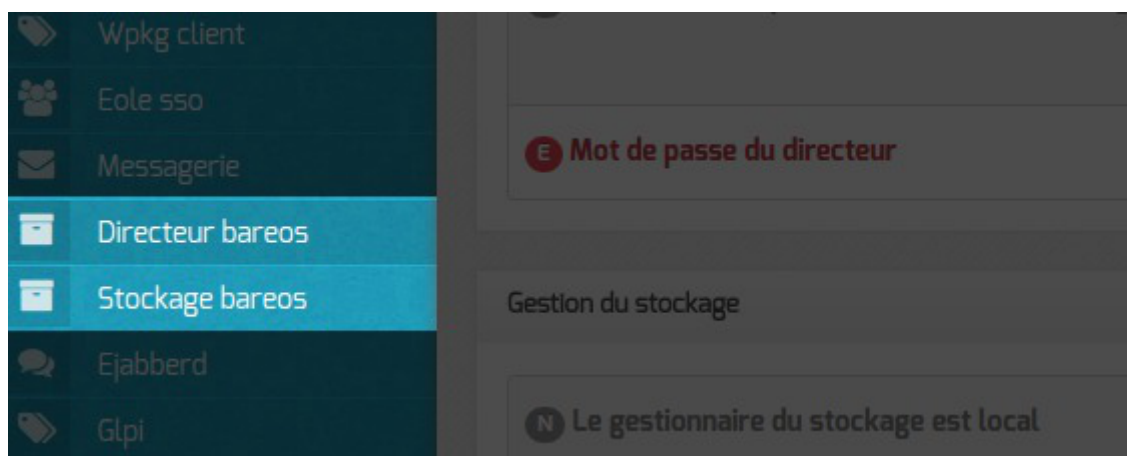
La sauvegarde du serveur et le support de stockage de la sauvegarde sont activés par défaut sur certains modules, il peuvent être activés/désactivés dans l'onglet **Services** de l'interface de configuration du module.

| | | | |
|--|-----|---|---|
| N Activer la sauvegarde du serveur | oui | ▼ | ✎ |
| N Activer le support de stockage de la sauvegarde | oui | ▼ | ✎ |

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.



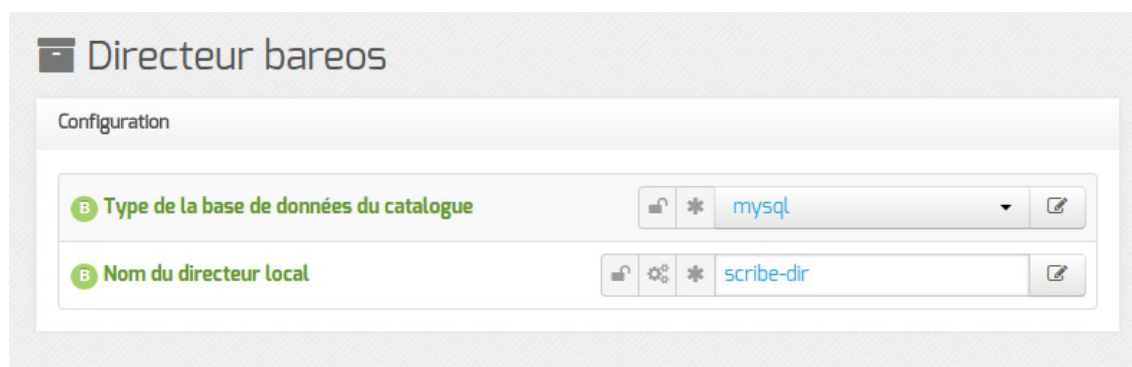
Si le support de stockage de la sauvegarde est activé (Activer le support de stockage de la sauvegarde à oui) un onglet **Stockage bareos** apparaît dans l'interface de configuration du

module.

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



Vue de l'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.

Directeur bareos

Configuration

B Type de la base de donnée du catalogue : mysql

B Nom du directeur local : scribe-dir

N Période de rétention des sauvegardes complètes : 6

N Unité de valeur pour la rétention des sauvegardes complètes : months

N Période de rétention des sauvegardes différentielles : 5

N Unité de valeur pour la rétention des sauvegardes différentielles : weeks

N Période de rétention des sauvegardes incrémentales : 10

N Unité de valeur pour la rétention des sauvegardes incrémentales : days

Gestion du stockage

N Le gestionnaire du stockage est local : oui

Vue de l'onglet Directeur Bareos

Ensuite, il est nécessaire de définir les durées de rétention^[p.363] des différents espaces de stockage (totale, différentielle et incrémentale).

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

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



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

Pour cela, voici un exemple de configuration :

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

Avec la politique de sauvegarde suivante :

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

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



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

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

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

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

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

```
# bareosregen.sh
La régénération 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

stockage.

The screenshot shows the 'Vue de l'onglet Directeur Bareos' configuration page. It includes several fields:

- Mot de passe de la base de données MySQL de la sauvegarde:** A password field containing '0eba5a3046bd940c7e90b872c...' with a checkmark icon.
- Délai alloué pour l'exécution complète d'une sauvegarde:** A numeric input field set to '0'.
- Niveau de compression des sauvegardes:** A dropdown menu set to 'GZIP6'.
- Mot de passe du directeur:** A password field containing '543f1dc3a31822d314c278360aE'.

Below the fields, the text 'Type de compression et délai alloué' is centered.

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.

The screenshot shows the 'Stockage bacula' configuration page. It features a 'Configuration' section with a field for 'Nom du serveur de stockage' containing the value 'horus-sd'.

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.

The screenshot shows the 'Configuration des accès distants au stockage' dialog box. It contains the following fields:

- Nom du directeur Bareos distant:** A field with a dropdown menu, a checkmark icon, and a close icon.
- Adresse IP du directeur distant:** A text input field with a checkmark icon.
- Mot de passe Bareos distant:** A password input field with a checkmark icon.
- Montrer/Cacher:** A button to toggle password visibility.
- Nom du directeur Bareos distant:** A button to add a new entry.

Autoriser des clients Bacula 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.240]

3.2.3.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.370].

Il est préférable de déporter le serveur de stockage Bareos plutôt que d'utiliser le protocole SMB [p.370].

Ce type de sauvegarde sera utilisé, par exemple, pour les NAS [p.367].

Les informations suivantes sont demandées :

- Nom de machine de la machine distante (n'accepte pas les majuscules) ;
- IP de la machine distante ;
- le nom du Partage ;
- optionnellement le Login, le Mot de passe .

CONFIGURATION DE L'OUTIL DE SAUVEGARDE BAREOS

SUPPORT DE SAUVEGARDE

Support de sauvegarde

PARAMÈTRES DE SAUVEGARDE POUR : SMB

Nom machine distante

IP machine distante

Partage

Login (facultatif)


Mot de passe (facultatif)

PARAMÈTRES D'ENVOI DES LOGS (FACULTATIF)

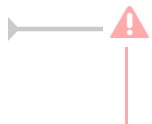
Mail admin sauvegarde pour les erreurs

Mail admin sauvegarde

TEST DU MONTAGE


 ERREUR : bareos n'est pas configuré
 [ OK]

Configuration d'un support de sauvegarde distant dans l'EAD



Les informations stockées dans les sauvegardes sont sensibles, il est 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`).

CONFIGURATION DE L'OUTIL DE SAUVEGARDE BAREOS

SUPPORT DE SAUVEGARDE

Support de sauvegarde

PARAMÈTRES DE SAUVEGARDE POUR : USB


Chemin d'accès

PARAMÈTRES D'ENVOI DES LOGS (FACULTATIF)

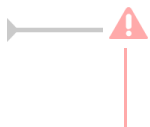
Mail admin sauvegarde pour les erreurs

Mail admin sauvegarde

TEST DU MONTAGE


ERREUR : bareos n'est pas configuré

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.368].

Voir la documentation officielle de Bareos pour le paramétrage :

<http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-480004>

CONFIGURATION DE L'OUTIL DE SAUVEGARDE BAREOS

La configuration est **manuelle**. Voir le template "bareosupport.conf".

SUPPORT DE SAUVEGARDE

Support de sauvegarde

PARAMÈTRES D'ENVOI DES LOGS (FACULTATIF)

Mail admin sauvegarde pour les erreurs

Mail admin sauvegarde

TEST DU MONTAGE

●

ERREUR : bareos n'est pas configuré

[✓ OK]

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.365] : 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 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 `bareosmount.py -t` retourne des erreurs.

Le montage à la main donne des erreurs :

```
# mount -t cifs //<adresseServeur>/sauvhorus /mnt/sauvegardes/
-ouusername=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/
-ouusername=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/
-ouusername=sauvegarde,password=***,sec=ntlm
```

```
# mount -t smbfs //<adresseServeur>/sauvhorus /mnt/sauvegardes/
-ouusername=sauvegarde,password=***,sec=ntlm
```

Il faut créer le fichier `/etc/eole/bareos.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=ntlm
://{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.370].

Il est possible de déclarer plusieurs destinataires en séparant les adresses par des virgules.

Exemple : `admin@ac-dijon.fr,technicien@ac-dijon.fr`

3.2.3.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 à configurer manuellement :

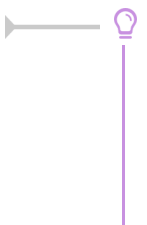
```
# bareosconfig.py -s manual
```

Vous devez ensuite configurer le support dans le fichier template `/usr/share/eole/creole/distrib/bareosupport.conf`

Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE^[p.368].



`nom machine` ne doit pas comporter de majuscule



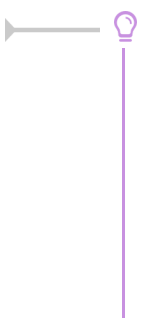
Pour tester le support de sauvegarde (USB local ou SMB), il est possible d'utiliser le script `bareosmount.py` :

```
# bareosamount.py -t
Test de montage OK
```

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.365] : 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 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 `bareosmount.py -t` retourne des erreurs.

Le montage à la main donne des erreurs :

```
# mount -t cifs //<adresseServeur>/sauvhorus /mnt/sauvegardes/
-ouusername=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/
-ouusername=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/
-ouusername=sauvegarde,password=***,sec=ntlm
```

```
# mount -t smbfs //<adresseServeur>/sauvhorus /mnt/sauvegardes/
-ouusername=sauvegarde,password=***,sec=ntlm
```

Il faut créer le fichier `/etc/eole/bareos.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}'
```

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

```

3.2.4. 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

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`

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 :

```
# bareos.py -x <numéro job>
```

ou encore :

```
# bareos.py --job to delete=<numéro job>
```

3.3. 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.

3.3.1. Restauration complète



La restauration d'un serveur se fait sur un serveur instancié.

Préparation du serveur

Mise à jour

Idéalement, le niveau de mise à jour du serveur avant restauration doit être identique au à celui du serveur sauvegardé.

Mettre à jour les paquets :

```
Maj-Auto
```


Choix du mode conteneur ou non

Si le serveur sauvegardé était en mode conteneur, il faut re-créeer 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
```

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
```

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 ?
[ooui/non]
```

Ne pas tenir compte du message d'erreur suivant :

```
ERREUR : /var/lib/eole/config/schedule.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
```

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`.

3.3.2. Restauration partielle

Rechercher un fichier à restaurer

Pour rechercher un fichier ou un répertoire dans le support de sauvegarde (sur la dernière sauvegarde uniquement), on utilise l'option `--search` :

```
# bareosrestore.py --search nom_du_fichier
```

Il est possible d'utiliser les caractères `?` ou `*` pour remplacer respectivement un ou plusieurs caractères en l'échappant de la façon suivante :

```
# bareosrestore.py --search nom_du \*
```

Il est également possible de lister le contenu d'un répertoire sauvegardé avec l'option `--ls folder` :

```
# bareosrestore.py --ls folder /etc/eole
```

```
liste du contenu de /etc/eole
```

```
config.eol
```

Restauration d'un fichier ou d'un répertoire

Pour restaurer un fichier de la dernière sauvegarde, on peut utiliser la commande :

```
# bareosrestore.py --file /chemin_absolu/nom_du_fichier
```

Exemple :

```
# bareosrestore.py --file /etc/eole/config.eol
```

Pour restaurer un répertoire et l'intégralité de son contenu, on peut utiliser la commande :

```
# bareosrestore.py --folder /chemin_absolu/nom_du_répertoire
```

Exemple :

```
# bareosrestore.py --folder /usr/share/ead2/backend/config
```

Restauration de l'ensemble des fichiers sauvegardés

Pour restaurer l'ensemble des fichiers sauvegardés, il est possible d'utiliser la commande :

```
# bareosrestore.py --all_files
```

Restauration spécifique

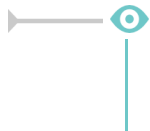
Les bases de données, les quotas, l'annuaire, ... ne sont pas sauvegardés sous forme de fichiers binaires.

Ils sont extraits avant la sauvegarde.

Pour restaurer, il existe une procédure particulière, différente suivant l'application.

Pour connaître les possibilités, faire :

```
# bareosrestore.py --help
```



Pour restaurer l'annuaire :

```
# bareosrestore.py --ldap
```

Restauration manuelle

Avant de lancer la restauration il est préférable de vérifier que le chemin du nœud du périphérique est toujours bon.

Il peut changer en fonction du nombre de périphériques connectés :

```
# bareosmount.py -t
```

Si le périphérique n'a plus le même nœud la commande `bareosmount.py` renvoie :

```
ERREUR : le périphérique /dev/sdb1 n'existe pas
```

Il faut alors changer la configuration du support :

```
# bareosconfig.py -s usb --usb_path=/dev/device usb
```

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 -c /etc/bareos/bconsole.conf
```

Dans cet exemple nous verrons comment restaurer le fichier `/home/a/admin/perso/icones.url`

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`

Taper la commande suivante (attention aux majuscules/minuscules et à la saisie sans accents) :

```
restore fileset=Complete
```

Il est possible de choisir directement le support de sauvegarde des fichiers en utilisant à la place la commande suivante :

```
restore fileset=FileSetSauvegarde
```

Cette commande indique à `bconsole` d'initialiser une restauration.

Vous avez alors plusieurs choix, les plus pertinents sont :

```
To select the JobIds, you have the following choices:
```

```
[...]
```

Depuis que l'utilisateur a supprimé le fichier le système n'a effectué que des sauvegardes incrémentales alors le fichier est toujours présent dans la sauvegarde, choisissez la sauvegarde la plus récente pour un client.

```
5: Select the most recent backup for a client (sélectionner la sauvegarde réussie la plus récente)
```

Depuis que l'utilisateur a supprimé le fichier le système a effectué une sauvegarde complète (Full) alors le fichier n'est présent que dans les sauvegardes précédant la sauvegarde complète, sélectionner la dernière sauvegarde pour un client avant une certaine date et entrez une date antérieure à la dernière sauvegarde complète.

6: Select backup for a client before a specified time (sélectionner la dernière sauvegarde réussie avant une date spécifiée)

La console propose trois options :

The defined FileSet ressources are :

1 : FileSetCatalog

2 : FileSetDefault

3 : FileSetSauvegarde

Il faut ensuite choisir le support de sauvegarde des fichiers (et non celui du catalogue) :

3 : FileSetSauvegarde

Un prompt apparaît et permet de naviguer dans l'arborescence des sauvegardes :

cwd is : /

\$ ls

etc/

home/

root/

usr/

var/

\$ cd /home/a/admin/perso

Il faut marquer les fichiers/dossiers à restaurer avec la commande `mark` (attention, la commande mark est récursive) :

\$ mark icones.url

1 file marked.

Pour "dé-marquer" un fichier marqué par erreur :

\$ unmark icones.url

1 file unmarked.

Lorsque les fichiers et les dossiers à restaurer sont sélectionnés, passer à l'étape suivante avec la commande :

\$ done

bconsole propose plusieurs options, il faut choisir le job de restauration, ici l'option numéro 3 :

3: Restore file

On obtient alors le message suivant :

Bootstrap records written to /var/lib/bareos/xxxxxxxxx.restore.2.bsr

[...]

Ok to run ? (yes/mod/no) :

La restauration peut maintenant être lancée en répondant `yes` à la question.

Il ne sera plus possible d'abandonner après cette étape.

```
OK to run? (yes/mod/no): yes
```

La restauration est alors placée dans une file d'attente. Le numéro `JobId` est affiché à l'écran.

Il est possible de changer les paramètres de restauration en répondant `mod` à la question :

```
OK to run? (oui/mod/non): mod
```

```
Parameters to modify :
```

```
1 : Level
```

```
2 : Storage
```

```
[...]
```

Par exemple pour restaurer dans un autre répertoire, il faut choisir `where` (9 dans le cas présent) et saisir le chemin de la restauration :

```
9 : Where
```

```
Please enter path prefix for restore (/ for none) : /home/restauration
```

```
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.

3.4. Ajouter des données à sauvegarder

Il est tout à fait possible d'ajouter des fichiers et/ou des répertoires à sauvegarder à ceux déjà configurés par défaut sur un module.

Pour cela il faut ajouter un fichier de configuration portant l'extension `.conf` dans le répertoire `/etc/bareos/bareosfichiers.d/`

Celui-ci ne doit comporter que les directives `Include` et `Exclude`, il ne faut pas, par exemple, spécifier le `Name` du FileSet car il est déjà défini dans le reste de la configuration.

Exemple d'un fichier de configuration pour la prise en charge de nouvelles données à sauvegarder :

```
Include {
```

```
Options {
```

```
# Sauvegarde des ACL
```

```

aclsupport = yes
# Tous les fichiers seront chiffrés en SHA1
signature = SHA1
# Compression des fichiers (niveau de compression 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` .

3.5. 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
```

3.6. 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

| Jobs during the past 24 hours | |
|-------------------------------|---|
| Running | 0 |
| Waiting | 0 |
| Successful | 8 |
| Unsuccessful | 0 |

100%

Running
Waiting
Successful
Unsuccessful

Bareos WebUI Version 14.2.1
© 2013 - 2015 Bareos GmbH & Co. KG, GNU Affero General Public License Version 3

Tableau de bord de bareos-webui

Dashboard Director Filesets Pools **Volumes** Storages Clients Jobs Logs Signed in as: admin_bareos

Volumes

Volumes per page: 10 | 25 | 50 | 100

| Volume | Name | Storage | Type | Last written | Status | Retention/Expiration | Maximum bytes | Current bytes | Free bytes |
|--------|-------------------------|---------|------|--------------|--------|----------------------|---------------|---------------|------------|
| 5 | scribe-dir-diff-0005 | 1 | File | today | Append | 35 days | 2 GB | 218.16 KB | 2 GB |
| 4 | scribe-dir-inc-0004 | 1 | File | today | Append | 10 days | 2 GB | 600.04 KB | 2 GB |
| 3 | scribe-dir-catalog-0003 | 1 | File | today | Used | expired | 2 GB | 265.75 KB | 2 GB |
| 2 | scribe-dir-full-0002 | 1 | File | today | Append | 180 days | 2 GB | 41.82 MB | 1.96 GB |
| 1 | scribe-dir-volume-0001 | 1 | File | today | Used | expired | 1 GB | 619 B | 1000 MB |

previous first 1 last next

Bareos WebUI Version 14.2.1
© 2013 - 2015 Bareos GmbH & Co. KG, GNU Affero General Public License Version 3

Affichage des volumes dans bareos-webui

Dashboard Director Filesets Pools Volumes Storages Clients **Jobs** Logs Signed in as: admin_bareos

Jobs

History Running Waiting Unsuccessful (past 24 hours) Successful (past 24 hours)

Jobs per page: 10 | 25 | 50 | 100

| Job | Name | Client | Type | Level | Start | End | Duration | Status | Action |
|-----|----------------|-----------|--------|--------------|---------------------|---------------------|----------|---------|--------|
| 15 | BackupCatalog | scribe-fd | Backup | Full | 2015-10-06 12:01:26 | 2015-10-06 12:01:26 | 00:00:00 | Warning | ⚙️ |
| 14 | JobSauvegarde | scribe-fd | Backup | Incremental | 2015-10-06 12:01:21 | 2015-10-06 12:01:22 | 00:00:01 | Warning | ⚙️ |
| 13 | JobSchedulePre | scribe-fd | Backup | Full | 2015-10-06 12:01:17 | 2015-10-06 12:01:17 | 00:00:00 | Success | ⚙️ |
| 11 | JobSauvegarde | scribe-fd | Backup | Differential | 2015-10-06 11:54:47 | 2015-10-06 11:54:48 | 00:00:01 | Warning | ⚙️ |
| 8 | JobSauvegarde | scribe-fd | Backup | Incremental | 2015-10-06 11:50:34 | 2015-10-06 11:50:34 | 00:00:00 | Warning | ⚙️ |
| 5 | JobSauvegarde | scribe-fd | Backup | Incremental | 2015-10-06 11:48:50 | 2015-10-06 11:48:51 | 00:00:01 | Warning | ⚙️ |
| 2 | JobSauvegarde | scribe-fd | Backup | Full | 2015-10-06 10:28:14 | 2015-10-06 10:28:23 | 00:00:09 | Warning | ⚙️ |
| 1 | JobSchedulePre | scribe-fd | Backup | Full | 2015-10-06 10:28:10 | 2015-10-06 10:28:11 | 00:00:01 | Success | ⚙️ |

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
```

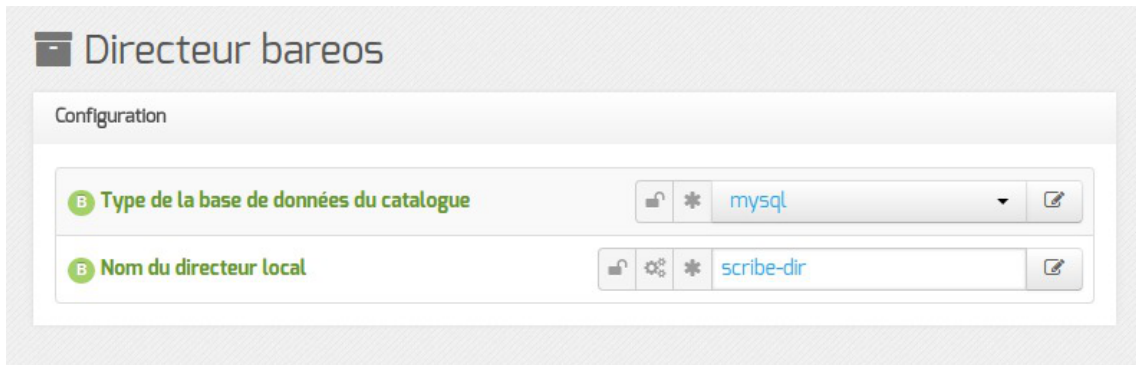


Le paquet est pré-installé sur les modules Scribe, Horus et AmonEcole.

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`.



Vue de l'onglet Directeur Bareos

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.

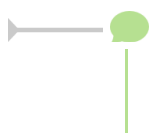
Dans l'onglet **Applications web**, il faut passer Activer Bareos WebUI (gestion de la sauvegarde) à oui.

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 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.184]

3.7. Diagnostic, rapport et résolution de problème

3.7.1. 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.

```

*** Sauvegarde
Test de Bareos Director :
.      Bareos Director => Ok
.      fichier de configuration => Ok
Test de Bareos Client :
.      Bareos Client => Ok
.      fichier de configuration => Ok
Test de Bareos Storage :
.      Bareos Storage => Désactivé
Statut des sauvegardes :
.      préparation sauvegarde => Inconnu : Aucune sauvegarde
.      sauvegarde principale => Inconnu : Aucune sauvegarde
.      sauvegarde catalogue => Inconnu : Aucune sauvegarde

```

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](#).

État des démons bareos

[Retour](#)

État : OK
 Date de la mesure : 2015-10-09 12:13:00
 Aucun problème détecté
 Intervalle de mesure : 60 s

| Description | état | Historique | Hôte | Port |
|-------------|--------------------------------------|------------|-----------|------|
| bareos-dir | ● | | localhost | |
| bareos-fd | ● | | localhost | |
| bareos-sd | ● | | localhost | |

États des services Bareos dans l'EAD

Si l'un des services est arrêté, il est possible de le relancer à l'aide de la commande [service](#) :

```
# service bareos-dir restart
```

```
* Restarting Bareos Director bareos-dir ... [ OK ]
```

Tester le support de sauvegarde

Pour tester le support de sauvegarde USB local ou SMB, il est possible d'utiliser le script `bareosmount.py`.

```
1 root@scribe:~# bareosmount.py -t
2 Test de montage OK
3 root@scribe:~#
```

```
1 root@scribe:~# bareosmount.py -t
2 Problème de montage (1 essais restants)
3 ERREUR : périphérique /dev/sda1 non reconnu
4 Problème de montage (0 essais restants)
5 ERREUR : périphérique /dev/sda1 non reconnu
6 Échec du test de montage :
7 point de montage : Erreur
8 permissions : Erreur
9 montage : Erreur
10 root@scribe:~#
```

```
1 root@scribe:~# bareosmount.py -t
2 Problème de montage (1 essais restants)
3 [Errno 32] mount error(13): Permission denied
4 Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
5
6 Problème de montage (0 essais restants)
7 [Errno 32] mount error(13): Permission denied
8 Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
9
10 Échec du test de montage :
11 point de montage : Erreur
12 permissions : Erreur
13 montage : Erreur
14 root@scribe:~#
```

3.7.2. Base de donnée sqlite de Bareos irrécupérable

Lors d'un incident sur l'un des modules EOLE la base de donnée sqlite de Bareos peut être irrécupérable.

Il est possible de restaurer des données sans la base de données avec les commandes `bls` et `bextract`.

Inspiré de l'article suivant :
<https://pipposan.wordpress.com/2010/06/09/bacula-tape-restore-without-database/>

Il est également possible de réaliser la récupération avec la commande `bconsole`.

Montage du support de sauvegarde et affichage des volumes par date

La commande `ls -lrt` permet de trier l'affichage des volumes par date :

```
root@srv-scribe:~# ls -lrt /mnt/sauvegardes/
```

On voit une sauvegarde FULL le 06/06/2015 (de nombreux volumes de 2Go ont la même date) :

```
-rw-r----- 1 bareos root 1999997379 2015-06-06 02:02 ScribeVolume0044
-rw-r----- 1 bareos root 1999936662 2015-06-06 02:05 ScribeVolume0068
-rw-r----- 1 bareos root 1999936707 2015-06-06 02:09 ScribeVolume0045
[...]
-rw-r----- 1 bareos root 1999936658 2015-06-06 04:34 ScribeVolume-0241
-rw-r----- 1 root root 1999936613 2015-06-06 04:38 ScribeVolume-0302
```

Utilisation de la commande bsl

```
root@srv-scribe:~# bsl -j -V ScribeVolume0044 /mnt/sauvegardes
bsl: butil.c:282 Using device: "/mnt/sauvegardes" for reading.
15-jun 16:38 bsl 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 bsl JobId 0: Fin de Volume au fichier 0 sur le Device
"FileStorage" (/mnt/sauvegardes), Volume « ScribeVolume0044 »
15-jun 15:54 bsl 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:~# bsl -j -V ScribeVolume-0302 /mnt/sauvegardes
```



```
bls: butil.c:282 Using device: "/mnt/sauvegardes" for reading.
15-jun 15:59 bls JobId 0: Prêt à lire les données du volume «
ScribeVolume-0302 » depuis le device "FileStorage" (/mnt/sauvegardes).
Volume Record: File:blk=0:209 SessId=109 SessTime=1427205136 JobId=33
DataLen=174
15-jun 16:00 bls JobId 0: Fin de Volume au fichier 0 sur le Device
"FileStorage" (/mnt/sauvegardes), Volume « ScribeVolume-0302 »
15-jun 16:00 bls JobId 0: Fin de tous les Volumes.
```

Génération d'un fichier bootstrap avec la liste des volumes à utiliser (tous ceux du 06/06/2015)

```
root@srv-scribe:~# cat bootstrap.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
bootstrap.bsr /mnt/sauvegardes /home/restore/
```

Restauration LDAP

```
root@srv-scribe:~# service slapd stop
root@srv-scribe:~# md /home/sav/ldap
root@srv-scribe:~# mv /var/lib/ldap/*.* /home/sav/ldap/
root@srv-scribe:~# slapadd -l /home/sauv ldap.ldif
```

Restauration MySQL

```
root@srv-scribe:~# mysql pwd.py eole21 nomodif
root@srv-scribe:~# mysql -uroot -peole21 < /home/sauv mysql.sql
```

Restauration Quotas

```
root@srv-scribe:~# bareosrestore.py --quota
```

Restauration SID

```
root@srv-scribe:~# cat /etc/eole/${MODULE}_SID | xargs net setlocalsid
```

Reconfiguration du serveur

Il faut procéder à la reconfiguration du serveur à l'aide de la commande `reconfigure` .

3.8. Annexes

Voici un complément d'information (outils d'administration, liens, ...) pour aller plus loin avec Bareos.

3.8.1. 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 :

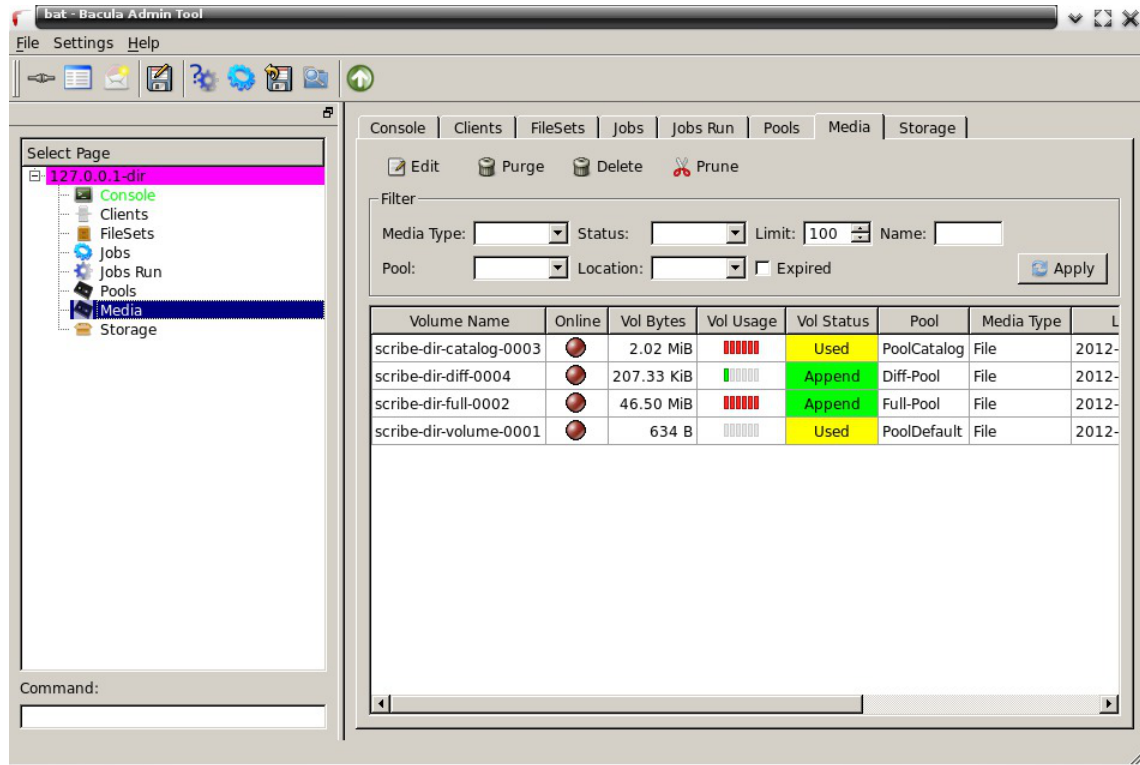
```
# apt-eole install bareos-bat
```

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>
```



BAT (Bacula Administration Tool)

- **bgnome-console** est une console graphique (notamment pour les opérations de restauration), mais nécessite l'installation des bibliothèques 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

3.8.2. Quelques références

Voici quelques références autour de Bareos et des sauvegardes.

- Définition de la sauvegarde : <http://fr.wikipedia.org/wiki/Sauvegarde>
- Le site officiel de Bareos : <http://www.bareos.org>
 - L'accès à la documentation en HTML mais aussi en PDF : <http://www.bareos.org/en/documentation.html>

- Tutoriel : <http://www.bareos.org/en/HOWTO.html>
- Manuel utilisateur : <http://www.bareos.org/en/manual/articles/manual.html>

Définition des éléments de sauvegarde Bareos :

<http://doc.bareos.org/master/html/bareos-manual-main-reference.html#x1-60001.3>

3.8.3. Un répertoire partagé comme supports de sauvegarde

Introduction

Les modules EOLE permettent d'utiliser plusieurs supports pour effectuer les sauvegardes, dont un répertoire partagé. Nous allons voir ici 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. Il peut aussi se trouver sur un disque dur externe connecté à la station par exemple (ou sur une clé USB pour faire des tests).

Il n'est pas impossible de donner des droits d'accès au partage à un compte du domaine mais cela pose problème pour les sauvegardes. 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. Or, pour éviter qu'un fichier/dossier ne soit modifié pendant la sauvegarde, Bareos arrête le service Samba. L'arrêt de Samba implique la non réponse du contrôleur de domaine. L'accès au partage n'est pas validé et la sauvegarde ne peut donc pas se faire.

Pour la sauvegarde, les accès au partage doivent donc impérativement se faire en utilisant un compte local du poste sur lequel se trouve le dossier partagé.

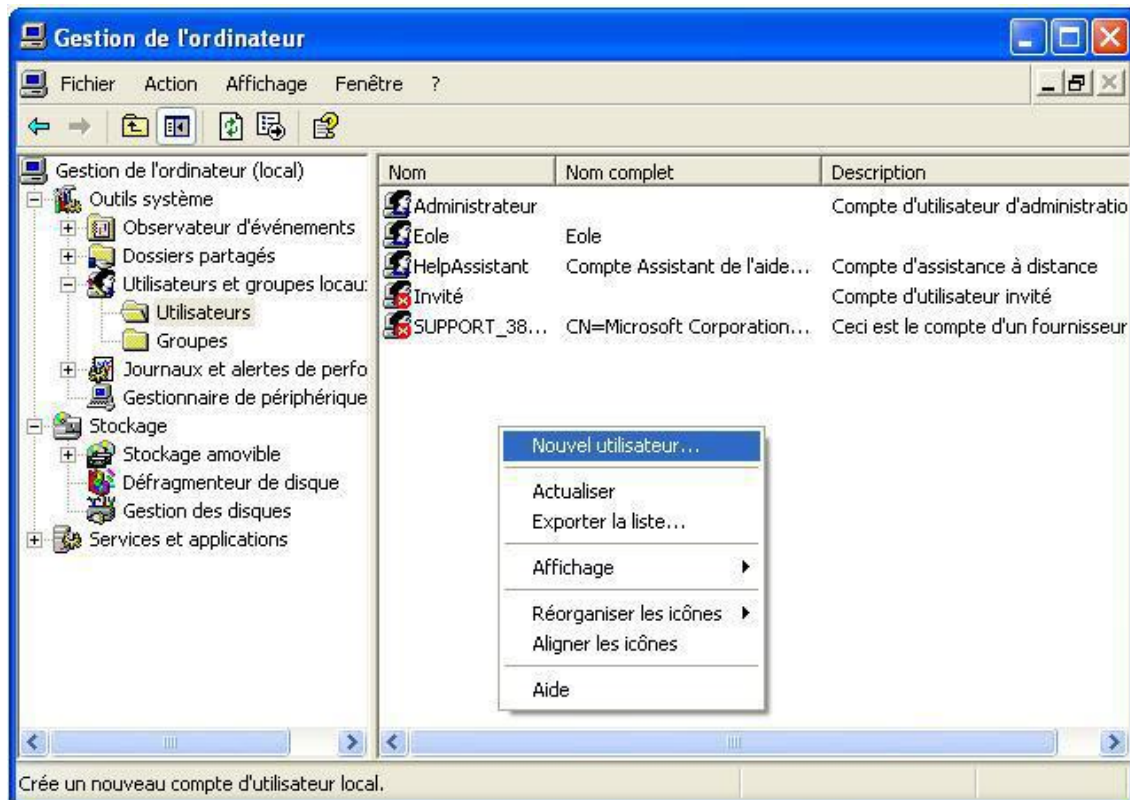
Création d'un compte sur le poste Windows XP

Ouvrez une session en administrateur local de la station sur laquelle vous voulez créer le partage. Puis ouvrez la console de **Gestion de l'ordinateur**.



Ensuite, créez un nouvel utilisateur (Menu "Action" ou clic droit dans l'espace vide de la colonne de

droite)

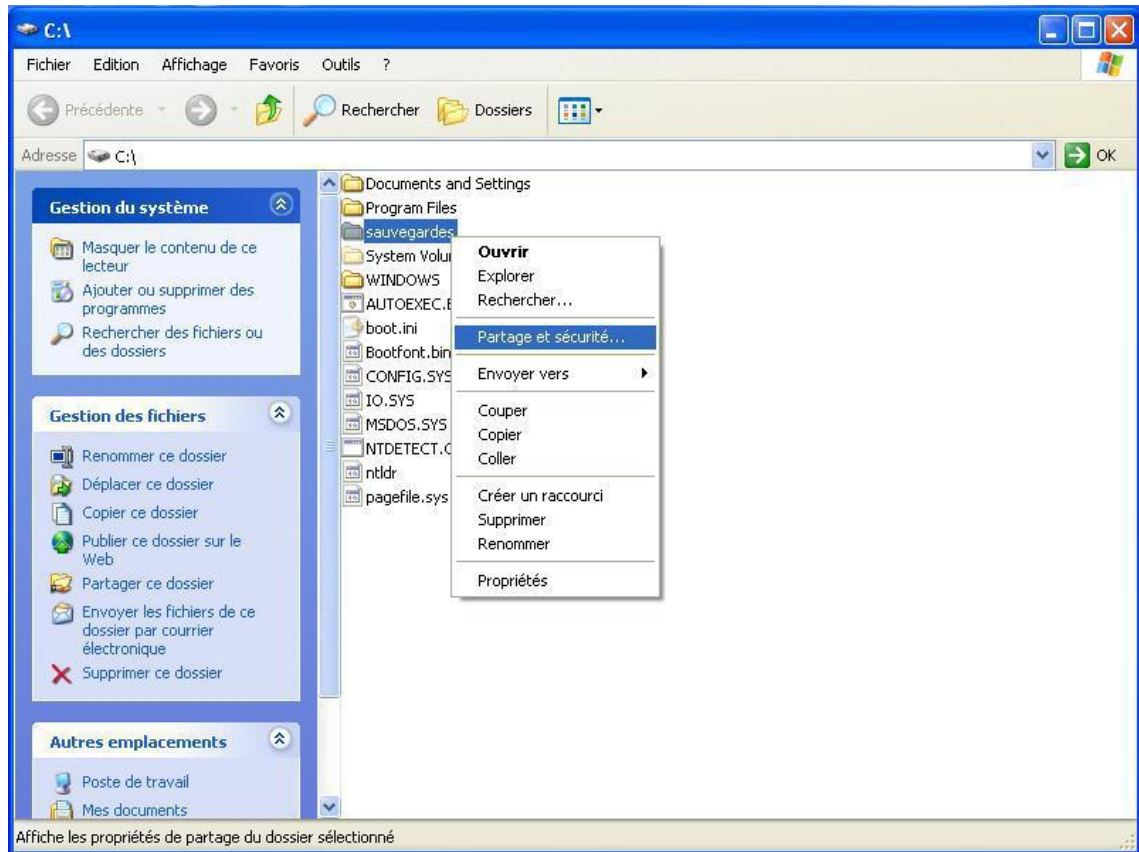


...avec les options configurées comme ceci :

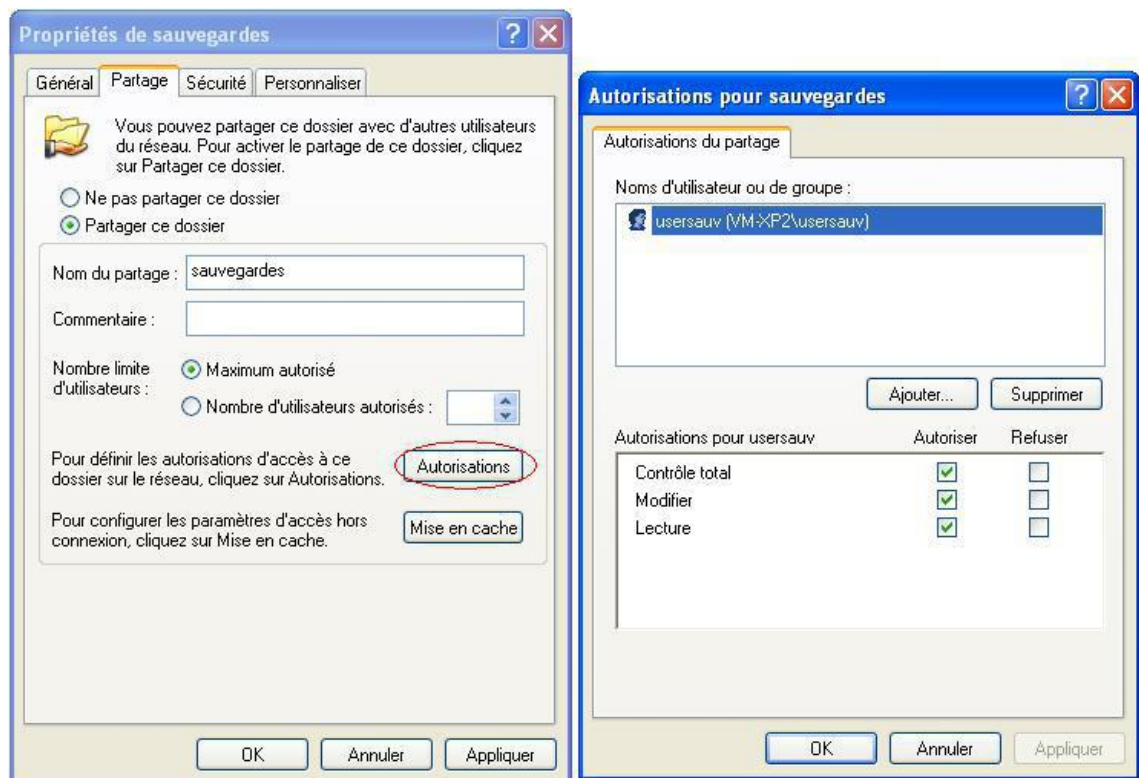


Partage du dossier et réglage des droits d'accès

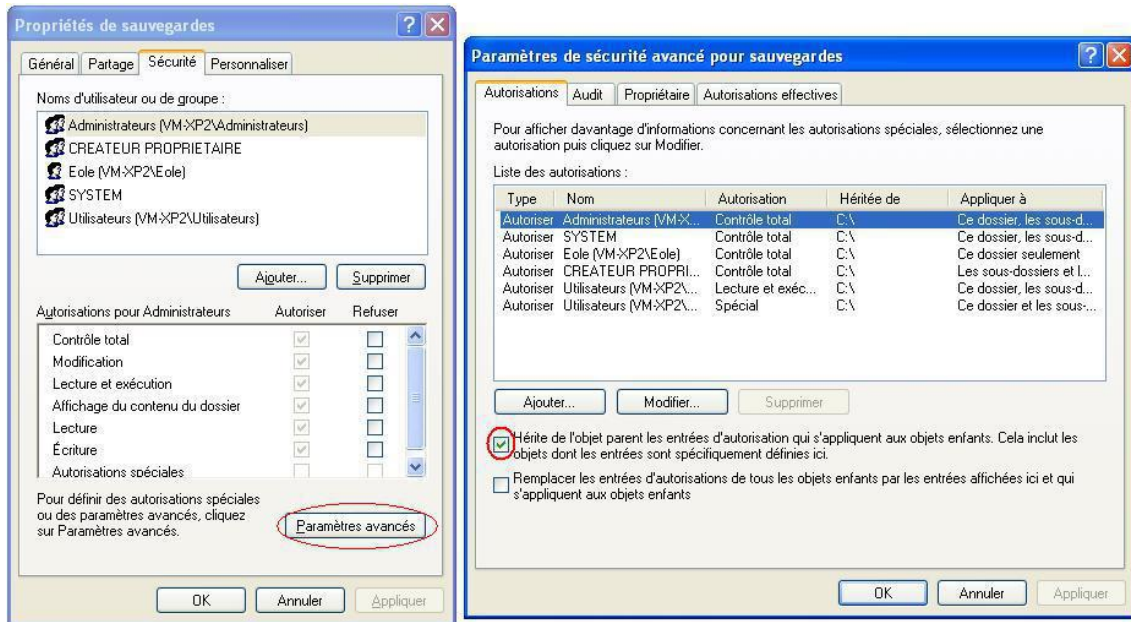
Après avoir créé un dossier "sauvegarde" à l'emplacement de votre choix, partagez-le (clic droit sur le dossier) :



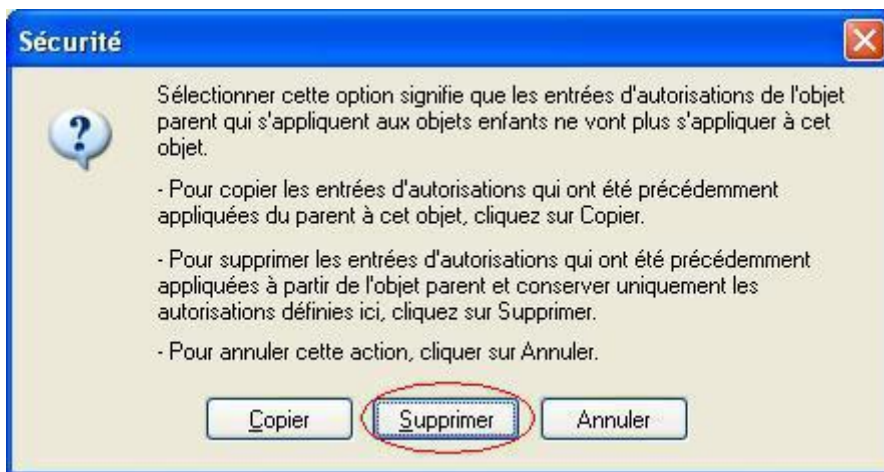
Puis cliquez sur **Autorisations**. Supprimez les autorisations par défaut ("*Tout le monde*") puis ajoutez "*usersauv*" avec "**Contrôle total**" :



Fermez la fenêtre des autorisations puis allez dans l'onglet "**Sécurité**" et cliquez sur "**Paramètres avancés**" :



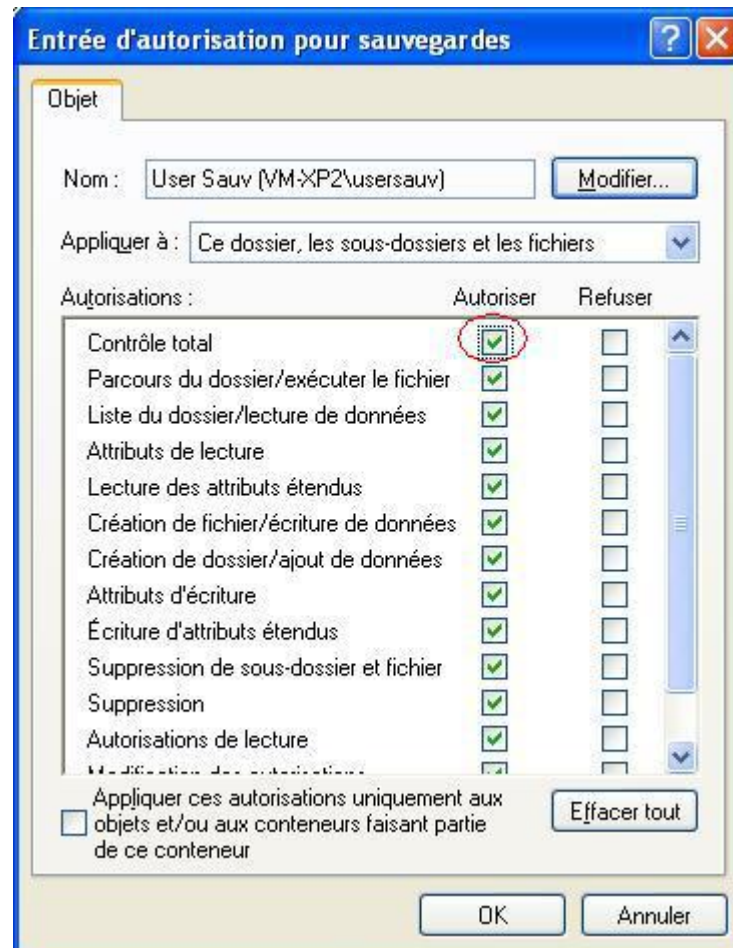
Décochez "Hérite de l'objet parent...", une fenêtre s'ouvre alors, sélectionnez "Supprimer" :



Ajoutez ensuite l'utilisateur "usersauv" toujours avec le "Contrôle total" :



Enfin, affectez le "Contrôle total" :



4. 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.362].

Deux interfaces sont disponibles pour gérer les imprimantes :

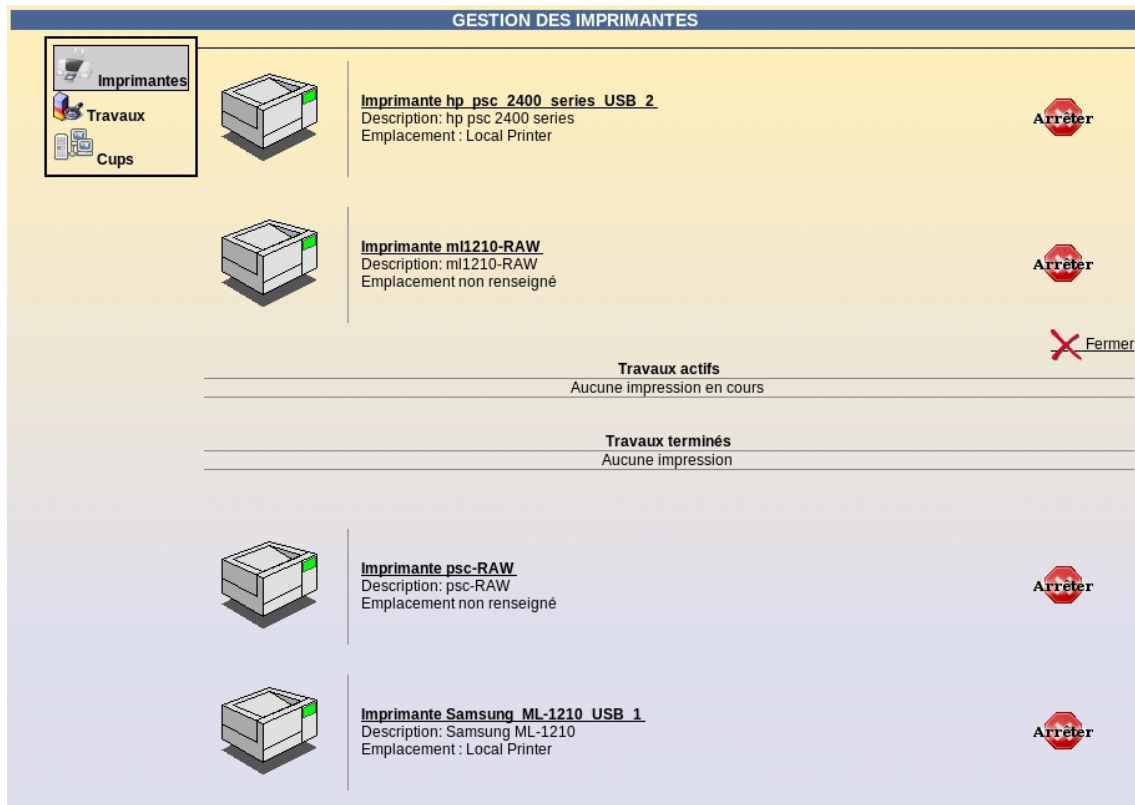
- l'interface simplifiée intégrée à l'EAD (gestion) ;
- l'interface de gestion CUPS (gestion et installation/configuration).

4.1. 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 ;
- consulter/interrompre/relancer les travaux d'impression ;
- arrêter/démarrer des imprimantes.



4.2. 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 groupe *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.

4.2.1. Création de l'imprimante

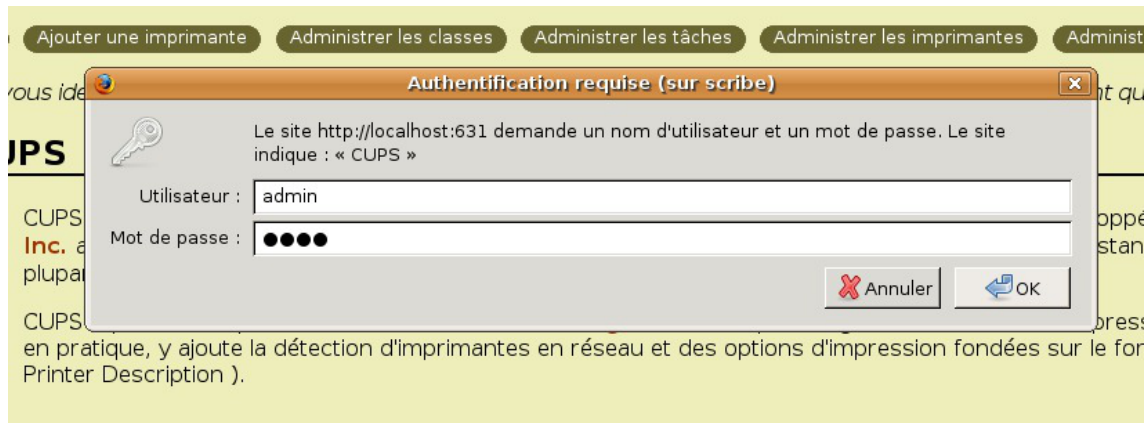
4.2.1.a. Ajouter une nouvelle imprimante

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*.



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**.

Ajouter une nouvelle imprimante

Nom :
(Peut comporter tout caractère imprimable, "/", "#", et espace exceptés)

Lieu :
(Lieu compréhensible pour un utilisateur, comme "Labo 1")

Description :
(Description compréhensible pour un utilisateur, comme "HP Laserjet recto/verso")

Poursuivre

Description de la nouvelle imprimante CUPS

4.2.1.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.

Matériel pour Epson_740

Matériel : EPSON Stylus COLOR 740 USB #1 (EPSON Stylus COLOR 740) ▼

- AppSocket/HP JetDirect
- EPSON Stylus COLOR 740 USB #1 (EPSON Stylus COLOR 740)
- Internet Printing Protocol (http)
- Internet Printing Protocol (ipp)
- LPD/LPR Host or Printer
- LPT #1
- SCSI Printer
- Serial Port #1
- Windows Printer via SAMBA

Matériel pour une imprimante locale CUPS

> Les imprimantes réseaux

Il existe un grand nombre de protocoles réseaux pour les imprimantes : AppSocket/HP JetDirect, Internet Printing Protocol (HTTP ou IPP). Généralement, les imprimantes réseaux sont capables 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 Epson_740

Matériel : AppSocket/HP JetDirect ▼

Poursuivre

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.

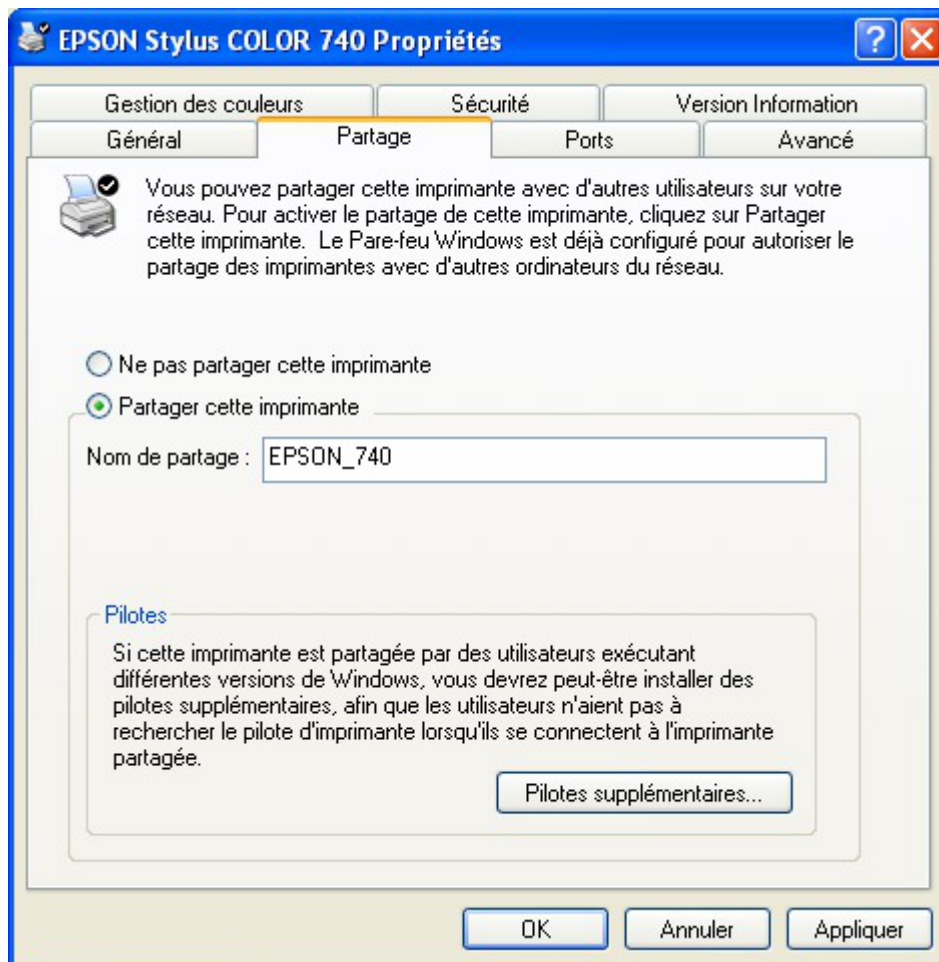
Il est possible d'accéder directement à l'imprimante du poste sans passer par le serveur. Cette documentation ne traite pas de ce cas.

Dans le menu Windows **Démarrer/Imprimantes et télécopieurs** cliquer droit sur votre imprimante et choisir **Partager...**.



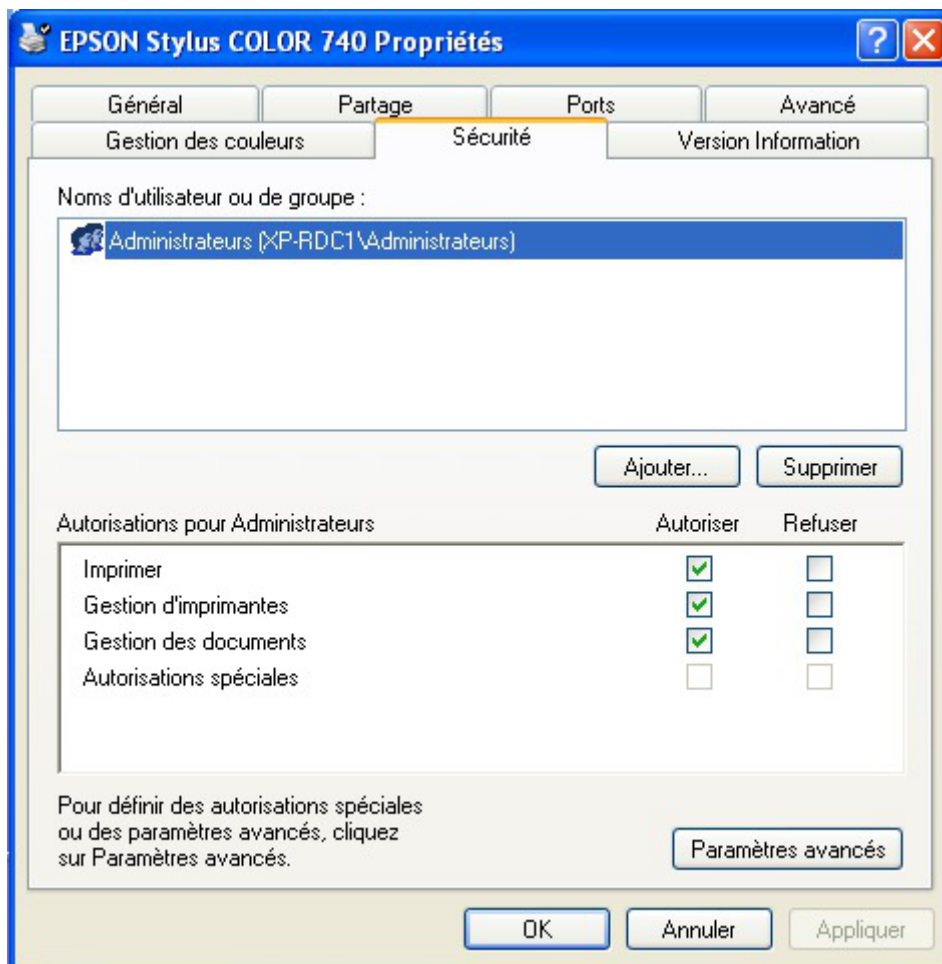
Partager une imprimante sous Windows

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.



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.

4.2.2. Choix du pilote

Il existe deux catégories de choix pour les pilotes d'impression.

- utilisation du pilote client Windows ;
- utilisation du pilote CUPS.

4.2.2.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.

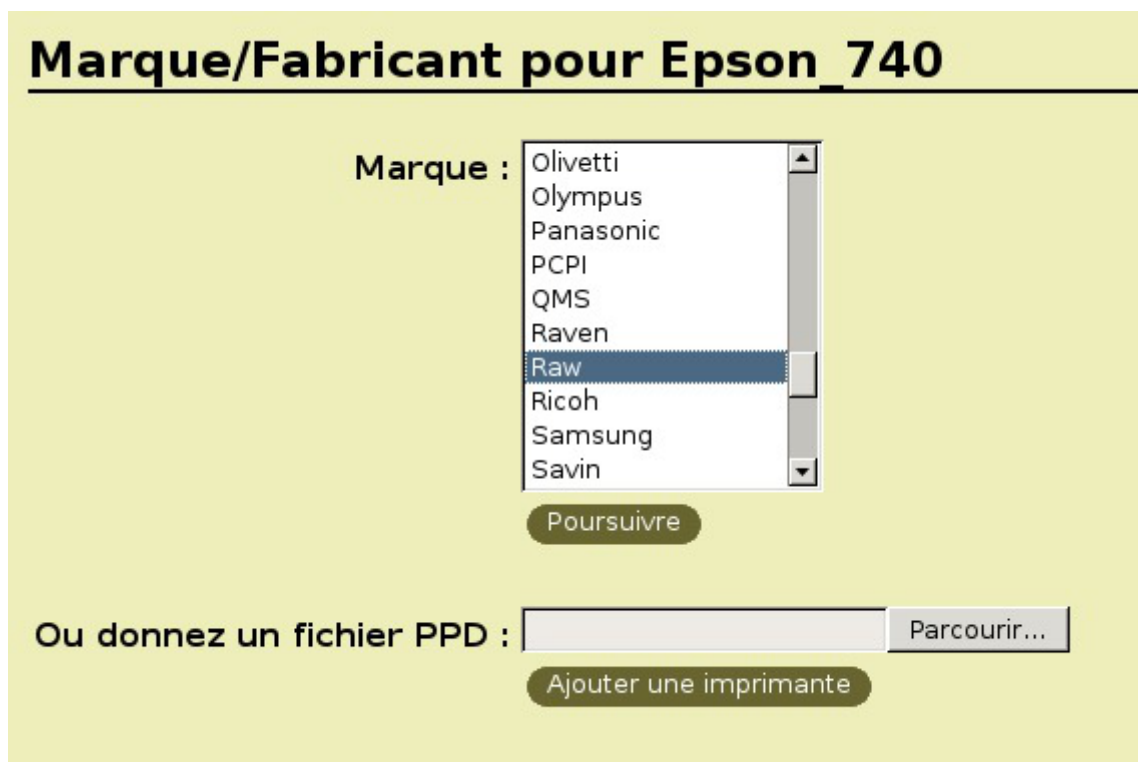
Le pilote CUPS est plus simple à mettre en place. Il est particulièrement adapté aux réseaux hétérogènes. Par contre, les pilotes ne sont souvent pas écrits directement par les constructeurs.

4.2.2.b. Utilisation des pilotes clients Windows

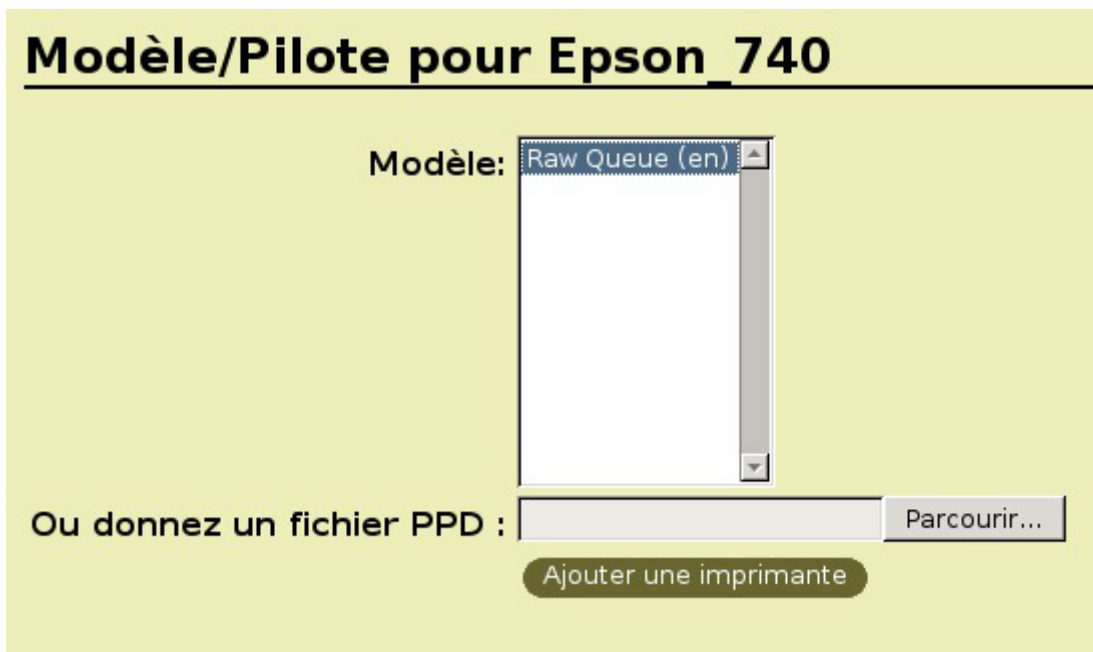
Configuration de CUPS

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



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**.



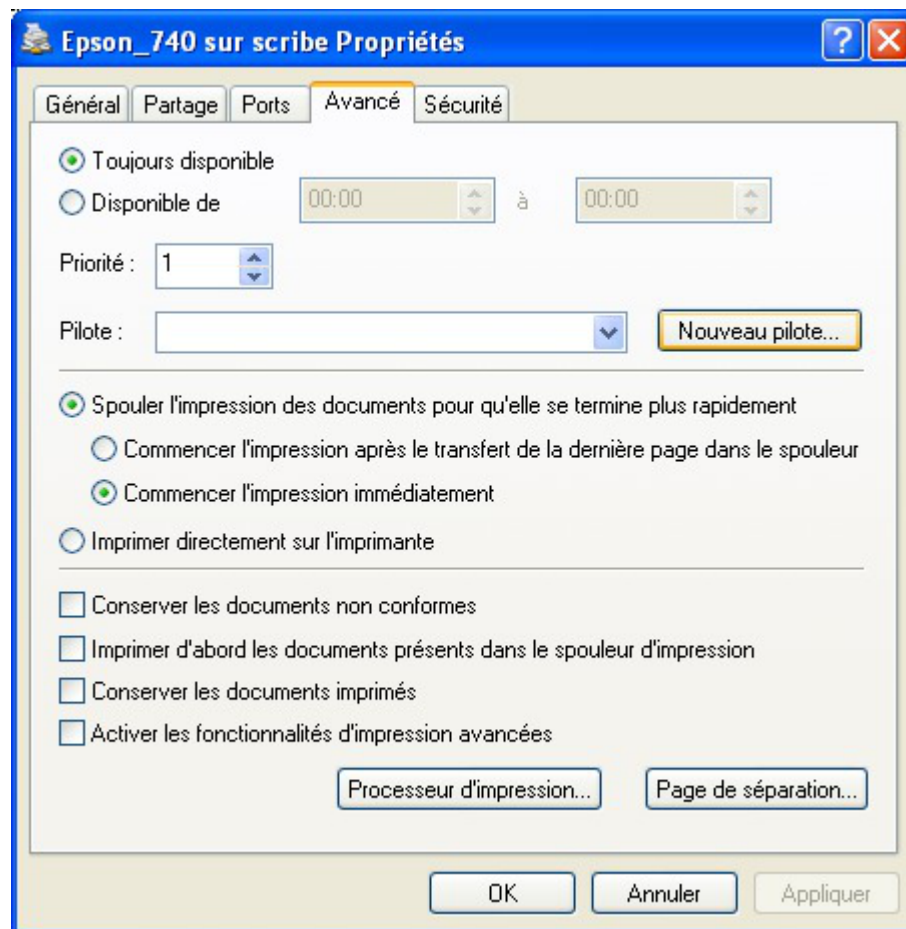
Propriété de l'imprimante sous Windows

Répondre **non** à la question "*Voulez-vous installer le pilote maintenant?*".



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 correspond à ce que vous souhaitez.

🟢 Dans l'onglet "Partage" il est possible d'installer des "Pilotes supplémentaires..." pour les autres versions de Windows.

4.2.2.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/Fabricant pour Epson_740

Marque :

Poursuivre

Ou donnez un fichier PPD : Parcourir...

Ajouter une imprimante

Marque/Fabriquant de la nouvelle imprimante CUPS

Modèle/Pilote pour Epson_740

Modèle:

Parcourir...

Ajouter une imprimante

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

Microsoft. Cela ne s'appliquera que pour les versions de Windows supérieures ou égales à Windows 2000.

Si vous utilisez encore des versions de Windows inférieures, 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'impressions 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.

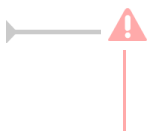
4.2.3. Quotas d'impression

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>

4.3. Gestion des imprimantes sous Windows



Ceci ne concerne pas les postes Windows Millennium et inférieur et nécessite l'utilisation du logiciel ESU^[p.364].

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.

4.4. 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

5. Compatibilité entre GFC et le module Horus

La qualification de GFC (Gestion Financière et Comptable) sur le module Horus est réalisée par l'équipe de diffusion de Montpellier.

L'actualité des applications nationales est consultable sur le site intranet de diffusion : <http://diff.in.ac-montpellier.fr/>

Les tests de compatibilités réalisés entre les différentes versions de GFC et et version du module Horus sont disponibles dans la rubrique **Publications** : <http://diff.in.ac-montpellier.fr/index.php/gfc/publications>



Il existe également un espace dédié au module Horus sur le site de diffusion du Pôle de Compétence de Paris :

<http://pole.in.ac-paris.fr/diffusion/HORUS>

6. Mise en place des sondes EQOS



EQoS permet à tout responsable, personnel de direction en établissement ou autorité académique, de mesurer la qualité de service de ses applications selon des critères objectifs.

Ces outils sont développés par pôle de Compétences Inter-Académique de Nancy-Metz (adresse à usage académique <https://pole.in.ac-nancy-metz.fr>).

Leur mise en place sur un module EOLE est simplifiée par la réalisation d'un paquet nommé `eole-egos`, pour l'installer :

```
# Query-Auto
```

```
# apt-eole install eole-egos
```

```
# reconfigure
```



Une documentation est disponible sur le site du pôle Compétences (adresse à usage académique) : <https://pole.in.ac-nancy-metz.fr/wiki/EqosDispoInstallSonde> [<https://pole.in.ac-nancy-metz.fr/wiki/EqosDispoInstallSonde>]

7. Les clients Windows

7.1. Installation et configuration des clients Windows

7.1.1. Principe

Le module Horus agissant comme un contrôleur de domaine, les stations Windows doivent dans un premier temps être intégrées dans le domaine.

Mises à jour et sécurité

Les mises à jour n'apportent pas seulement de nouvelles fonctionnalités, elles corrigent aussi des failles de sécurité.

Il est donc important que **les clients soient aussi à jour**.

Cela concerne aussi bien le **système d'exploitation** (Windows Update) que **les programmes installés** (Firefox, Java, QuickTime, etc.).

Des vulnérabilités peuvent, en effet, toucher n'importe quel programme.

Ne pas appliquer les mises à jour rendrait votre système vulnérable aux attaques.

Rappelons à ce sujet que, statistiquement, la majorité des attaques proviennent de l'intérieur et non de l'extérieur.

7.1.2. Configuration réseau

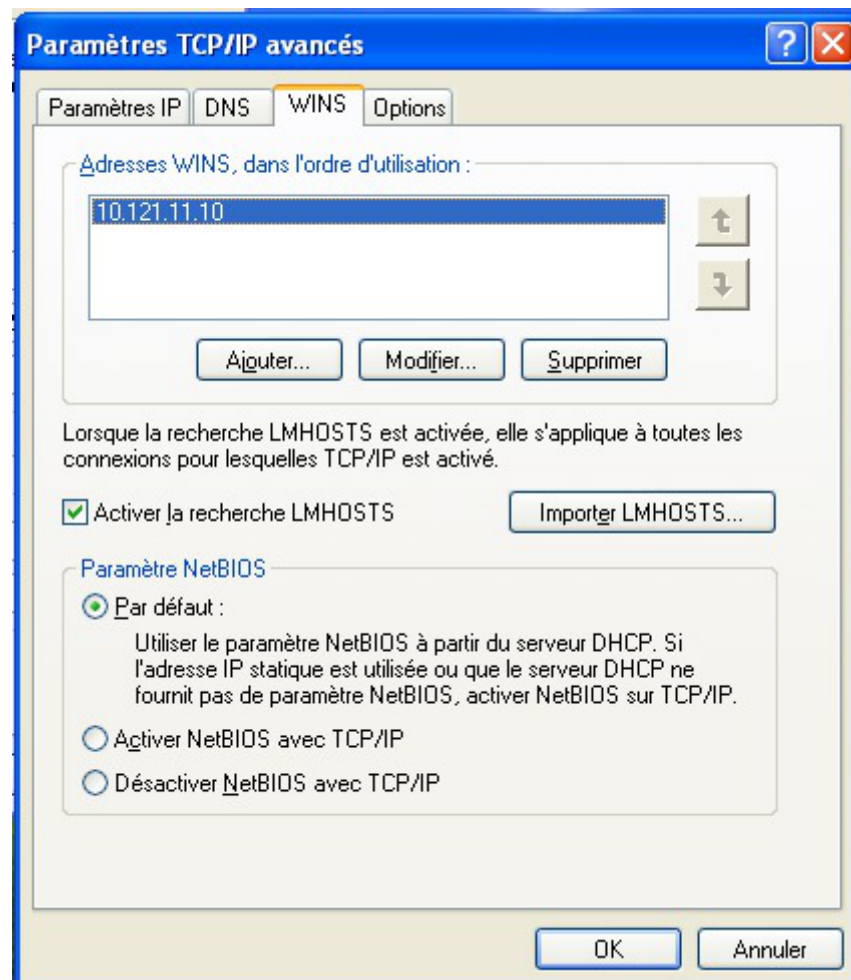
Avant l'intégration au domaine, il est indispensable de s'assurer que les paramètres réseau de la station soient corrects (adresse IP, passerelle, DNS, WINS).

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.372] ;
- 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 .



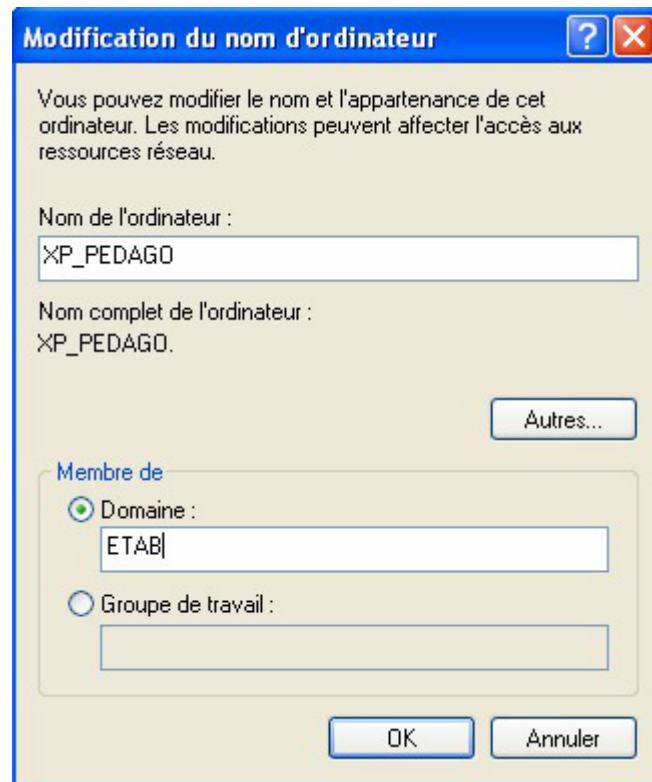
Configuration du serveur WINS dans Windows XP

7.1.3. Intégration et installation du client Horus manuelle

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 Modifier... ;
- 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.



Intégration manuelle au domaine

Intégration au domaine avec Windows 7

Particularité 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\LanmanWorkstat`

`DWORD DomainCompatibilityMode = 1`


`DWORD DNSNameResolutionRequired = 0`

Un fichier `Win7_Samba3DomainMember.reg` est mis à disposition pour modifier la base de registre dans `/home/esu/Console/`.

Ajoutez la station au domaine de la façon suivante :

- Aller dans le menu Démarrer ;
- Clic droit sur Ordinateur et sélectionner Propriétés ;

Système

Évaluation :  L'indice de performance Windows doit être actualisé.

Processeur : QEMU Virtual CPU version 1.7.0 3.40 GHz

Mémoire installée (RAM) : 1,00 Go

Type du système : Système d'exploitation 64 bits

Stylet et fonction tactile : La fonctionnalité de saisie tactile ou avec un stylet n'est pas disponible sur cet écran

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur : win7admin1 [Modifier les paramètres](#)

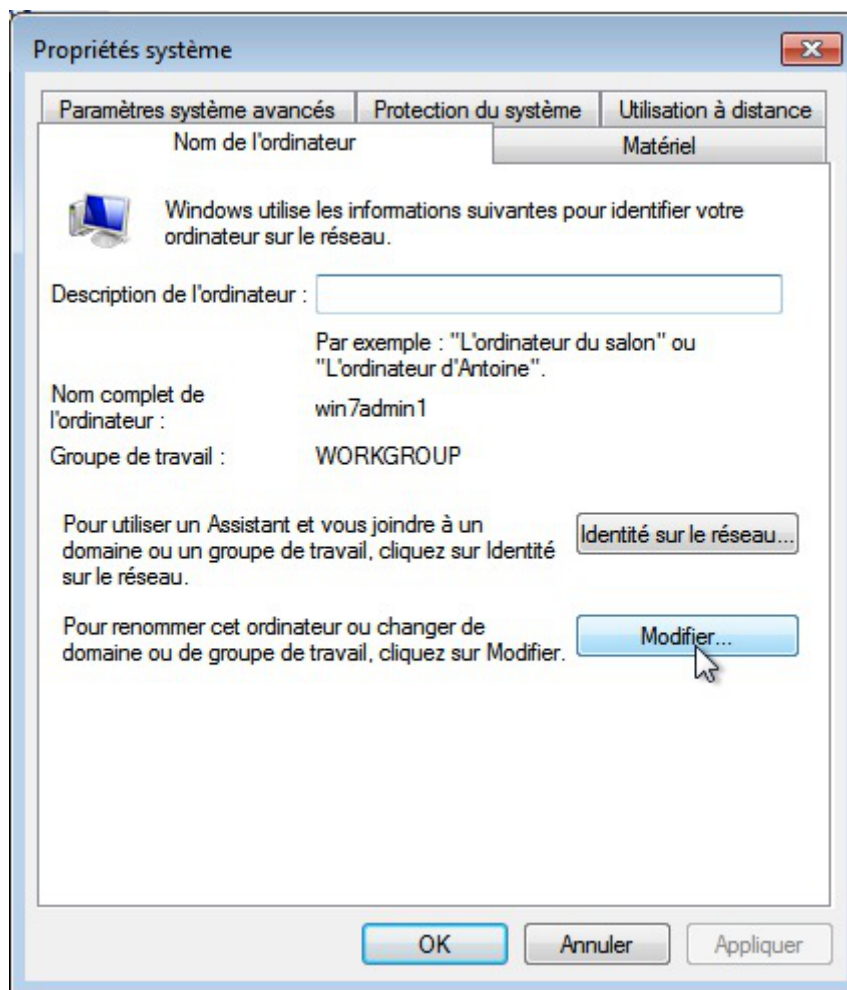
Nom complet : win7admin1

Description de l'ordinateur :

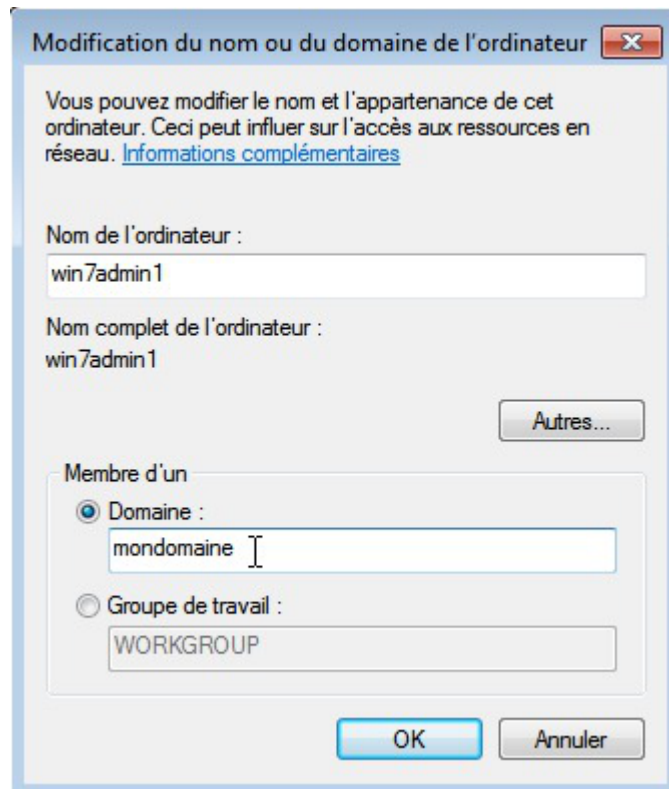
Groupe de travail : WORKGROUP

Activation de Windows

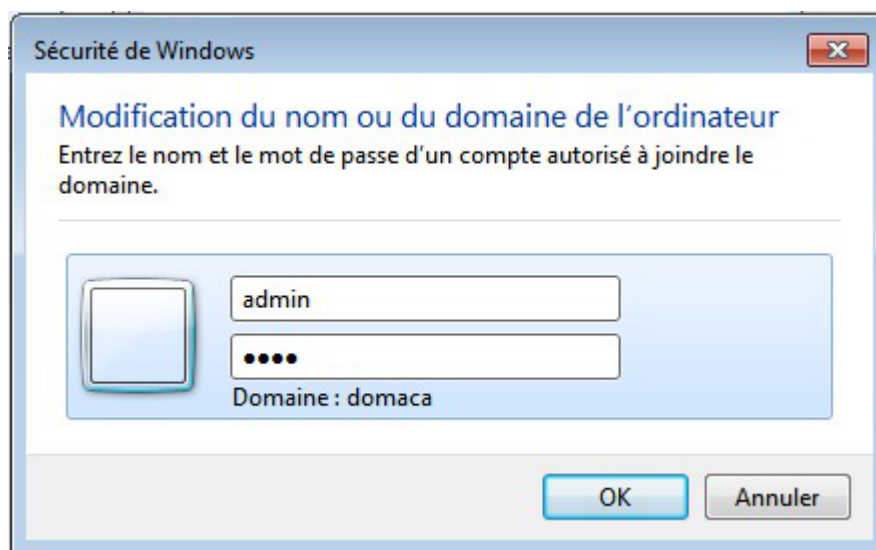
- Cliquer sur **Modifier les paramètres** ;



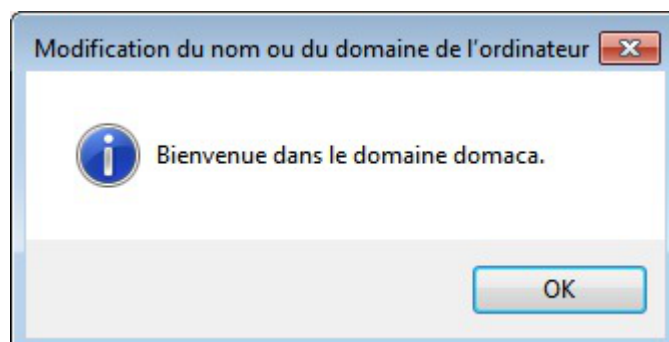
- Cliquer sur le bouton **Modifier...** ;



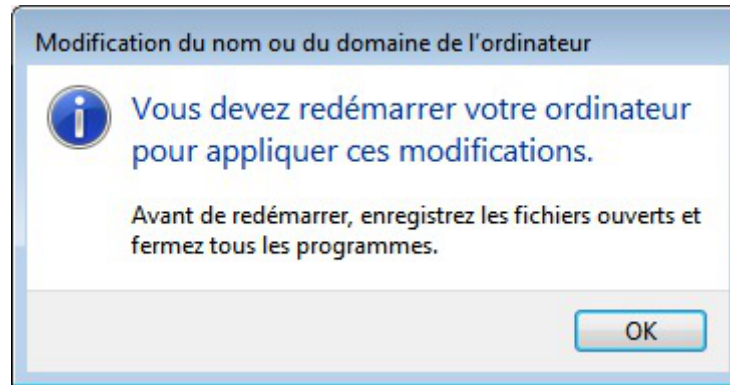
- Renseigner le nom de domaine Samba et cliquer sur **OK** ;



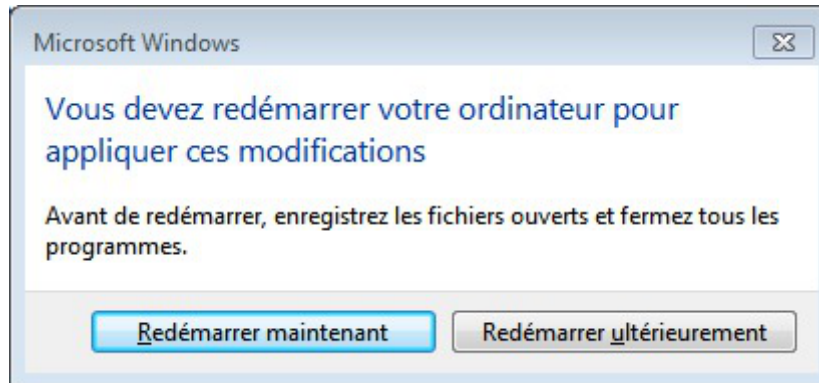
- Utiliser le compte admin ou un compte ayant les droits suffisants pour finaliser l'intégration ;



- Confirmer le message de bienvenue ;



- Confirmer le message d'avertissement ;



- Redémarrer maintenant.

Installation du client Horus

★ Pré-requis à l'installation du client Horus

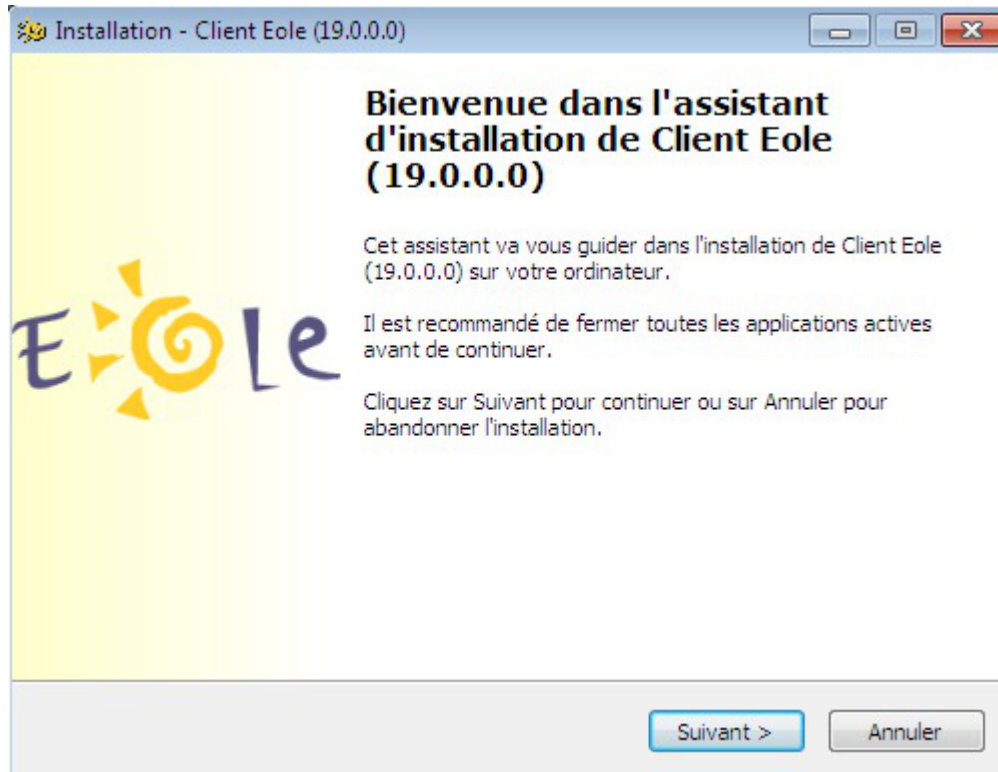
Le service pack 3 pour Windows XP est recommandé pour un fonctionnement correct du client Horus.

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_horus>`.

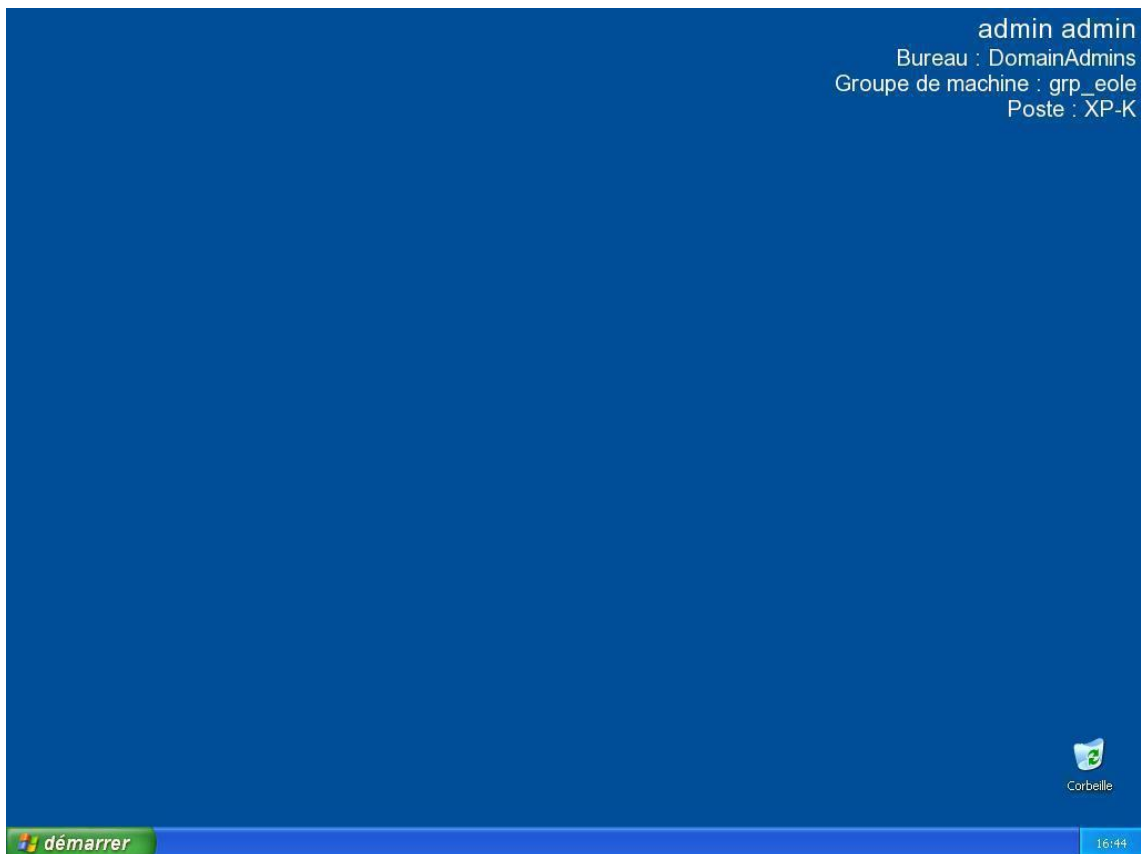
Installation manuelle du client

L'installateur du client possède un raccourci accessible avec l'utilisateur **admin** dans `U:\Install_Eole_Client`.



Une fois installé, le programme d'installation demande un redémarrage.

Après cela, l'ouverture de session suivante devrait ressembler à cela :



Bureau par défaut de l'utilisateur "admin"

Installation et redémarrage automatique

Il est possible d'installer le client en mode automatique à l'aide d'un fichier `.bat` contenant ceci :

```
1 echo off
2 rem il faut empecher le redemarrage par le premier installeur
3 echo Installation du service de mise a jour
4 U:\client\cliscribe-updater-setup.exe /VERYSILENT /NORESTART
5 echo Installation du client
6 U:\client\cliscribe-setup.exe /VERYSILENT
7 echo redemarrage...
8 echo on
```

En fin d'installation le système redémarrera sans poser de question.

7.1.4. Intégration et installation du client Horus automatique

PrepaWin et IntegrDom sont à utiliser sur un module Horus 2.5.1.

À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

7.1.4.a. PrepaWin

PrepaWin et IntegrDom sont à utiliser sur un module Horus 2.5.1.

À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel PrepaWin est une contribution de Jérôme Labriet de l'académie de Besançon, il permet de préparer et d'intégrer une station Windows XP ou Seven Professionnel 32 ou 64 bits sur un domaine Horus.

Pour plus d'informations, vous pouvez consulter le document suivant :

http://eole.ac-dijon.fr/pub/Documentations/divers/IntegrDom_PrepaWin_Scribe.pdf

7.1.4.b. IntegrDom

PrepaWin et IntegrDom sont à utiliser sur un module Horus 2.5.1.

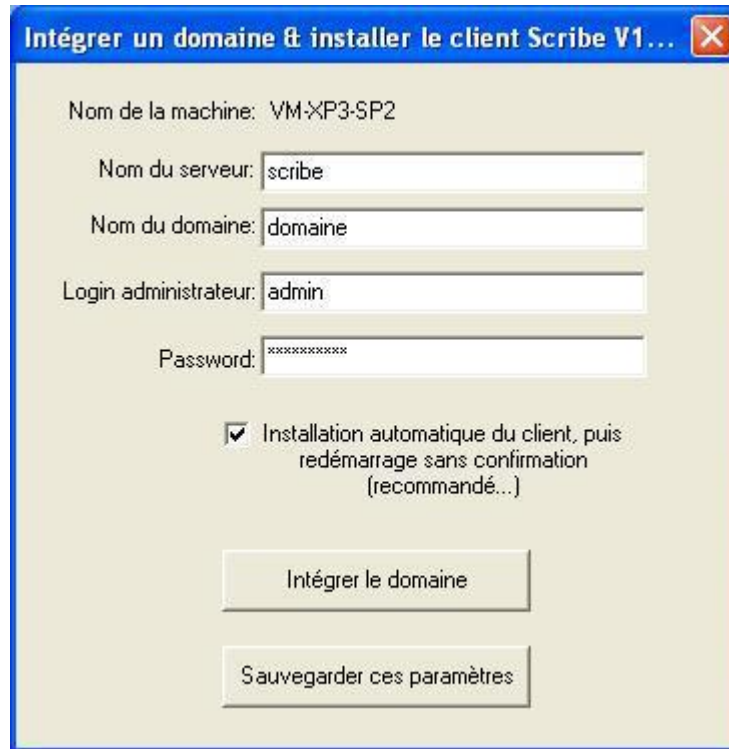
À partir de la version 2.5.2 du module il faut utiliser JoinEOLE.

Le logiciel IntegrDom est une contribution de Daniel Piquée de l'académie de la Réunion, il permet de joindre une station XP au domaine et d'y installer le client Horus en une seule fois.

Le logiciel IntegrDom est fourni dans le répertoire personnel de l'utilisateur admin.

Il est possible de pré-paramétrer le logiciel :

- se connecter en admin sur une station déjà intégré 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*.

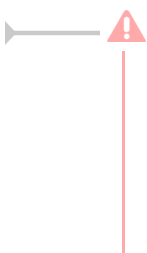
Les erreurs éventuellement retournées par IntegrDom sont celles retournées par l'utilisation de la fonction NetJoinDomain : [http://msdn.microsoft.com/en-us/library/aa370433\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa370433(v=vs.85).aspx).

7.1.4.c. JoinEOLE

À partir de la version 2.5.2 du module, PrepaWin et IntegrDom ont été supprimés au profit du script JoinEOLE qui est disponible dans le dossier `IntegrDom` situé dans le répertoire perso de l'`admin`.

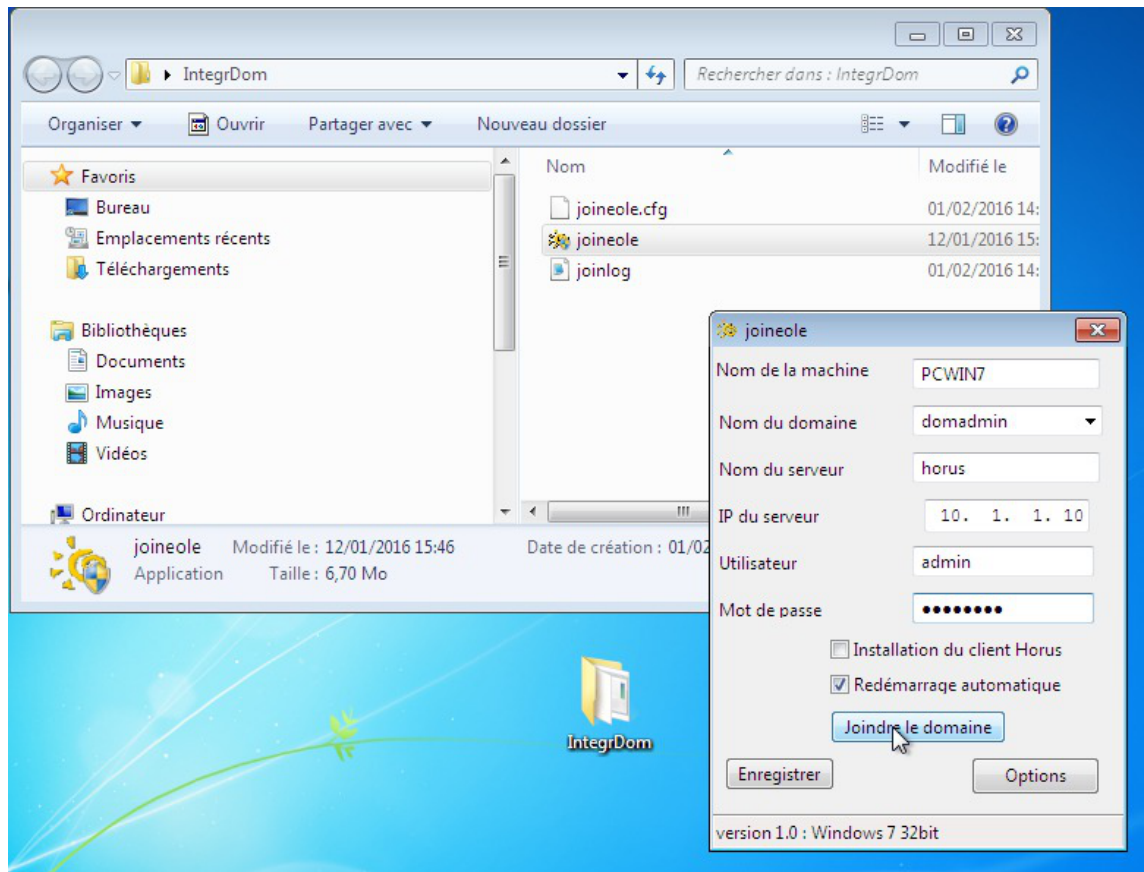
L'outil JoinEOLE prépare la station, la joint au domaine et installe de façon optionnelle le client pour Scribe ou Horus. De ce fait, il peut également être utilisé pour joindre les postes à un domaine Horus sur lequel le logiciel ESU n'est pas activé.

Le logiciel JoinEOLE est une contribution de Christophe Dezé de l'académie de Nantes.

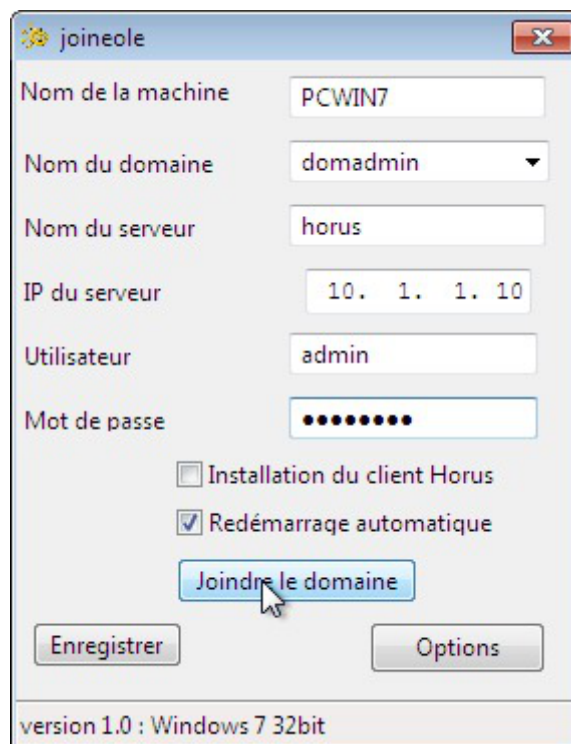


Il n'est pas possible de lancer l'exécution de JoinEOLE directement depuis le lecteur réseau car l'utilitaire ne gère pas les chemins UNC^[p.372].

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 rattachée, le nom netbios du serveur ainsi que l'adresse IP du serveur Scribe ou Horus.



L'utilitaire permet l'intégration au domaine et installe directement le client si Installation du client est cochée.

La case Redémarrer automatiquement est précochée.

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.

7.1.4.d. Joinscribe

`joinscribe` est une contribution de Christophe Dezé de l'académie de Nantes, il permet l'intégration au domaine et l'installation du client Horus qui s'exécute depuis le serveur.

L'outil `joinscribe` n'est pas pré-installé sur le serveur Horus.

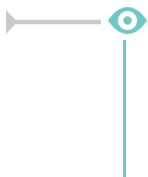
Il s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
# apt-eole install joinscribe
```

Avant d'exécuter `joinscribe`, il faut préparer le poste client de la manière suivante :

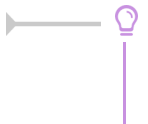
- dans les "options des dossiers", onglet **Affichage**, décocher l'option **Utiliser le partage de fichiers simple** ;
- mettre un mot de passe à l'utilisateur administrateur ;
- désactiver le pare-feu de Windows.

Une fois les postes clients préparés, lancer `joinscribe` depuis la console du serveur Horus.



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 Horus les fichiers `/var/log/joinscribe/` et sur le poste client `c:\windows\eoled\tmp\ParamIntegr.log`.

7.1.5. Mise à jour du client Horus

Le client Horus installé sur les stations Windows est automatiquement mis à jour si une nouvelle version est disponible sur le serveur. L'installateur du client Horus présent sur le serveur est fourni par le paquet `controle-vnc-client`. Autrement-dit, si le paquet `controle-vnc-client` est mis à jour sur le serveur, les clients Windows se mettront automatiquement à jour au prochain redémarrage.

Principe de la mise à jour du client :

- lors de l'installation du client Horus, le fichier `%WINDIR%\Eole\install.ini` est créé. Ce fichier contient la version du client installé ;
- à chaque démarrage de la station le service de mise à jour du client vérifie sur le serveur si une nouvelle version est disponible en téléchargeant le fichier `http://<adresse_module>:8790/install.ini` ;
- si une nouvelle version est disponible, le service désinstalle l'ancienne version, redémarre, installe la

nouvelle version et redémarre à nouveau.

Le fichier de référence du serveur est `/home/client_horus/install.ini`. (lié pour "admin" dans `U:\client\install.ini`).

Les opérations effectuées par le service de mise à jour du client Horus sont journalisées dans `%WINDIR%\cliscribe_updater.log`.

Le service de mise à jour du client Horus est accompagné d'une fenêtre d'indication de l'avancement qui s'affiche lorsqu'un utilisateur ouvre une session pendant la mise à jour du client Horus.



Fenêtre d'avancement de la mise à jour



Si pour une raison précise la mise à jour des clients doit être **ponctuellement** désactivée, il est possible de le faire :

- par station, en renseignant "VERSION = 0" dans le fichier `%WINDIR%\Eole\install.ini` ;
- pour toutes les stations, en renseignant "VERSION = 0" dans le fichier `/home/client_scribe/install.ini`.



Il est fortement déconseillé de désactiver la mise à jour du client parce que :

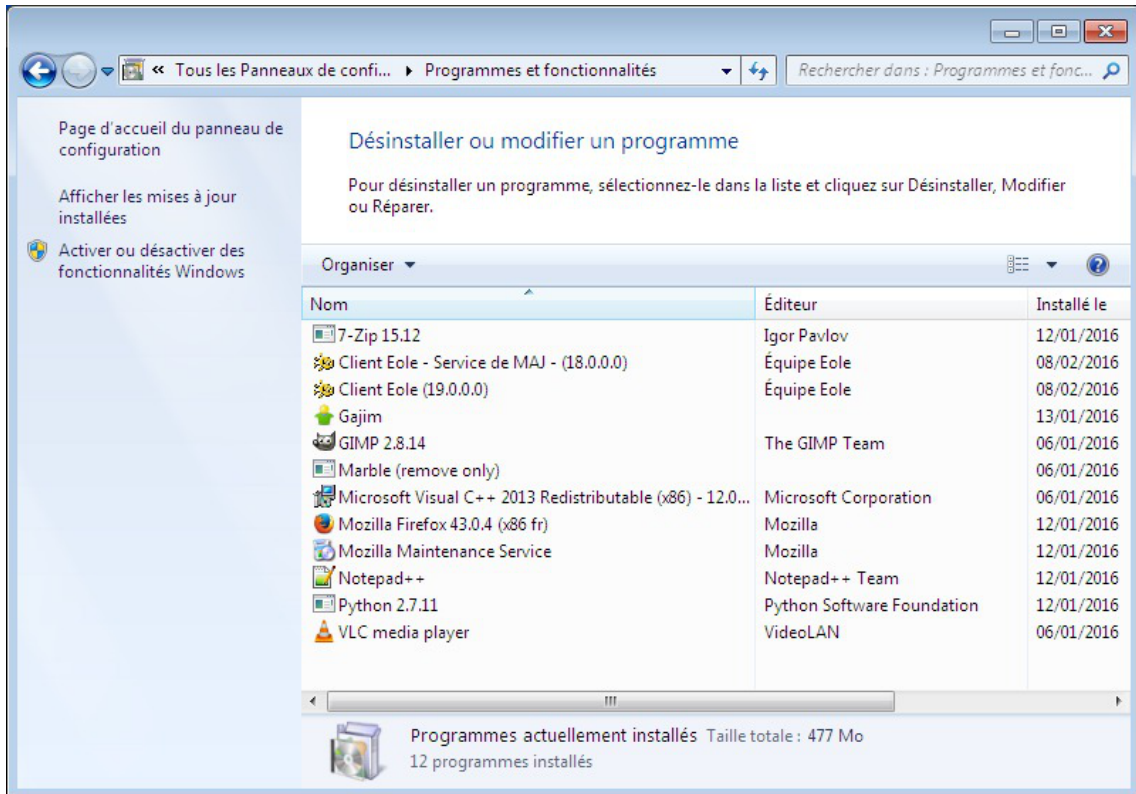
- le serveur sera à jour et pas le client, certaines actions risquent de ne plus fonctionner ;
- les nouvelles fonctionnalités ne seront pas disponibles ;
- les mises à jour peuvent contenir des corrections de sécurité.

Aucune aide ne pourra être apportée si le client n'est pas à jour.

7.1.6. Désinstallation du client Horus

La désinstallation du client EOLE s'effectue dans :

- Panneau de configuration
- Ajout/Suppression de programmes



Le client EOLE est composé de deux parties :

- le client ;
- le service de mise à jour du client.

Elles sont installées simultanément mais demandent une désinstallation séparée.

Le service de mise à jour du client doit être désinstallé avant le client car, au démarrage de la machine, si le client n'est pas trouvé, le service de mise à jour le réinstallera automatiquement.

7.2. Administration des clients Windows

Afin de faciliter l'administration des clients, divers outils ont été développés et installés sur le module Horus :

- **ESU**, configuration du poste client et de l'environnement de l'utilisateur, composé d'une console et d'un client ;
- **l'EAD**, action sur les postes et les utilisateurs.

Fonctionnement général sous Windows

Sur un module Horus installé de façon standard (pas d'adaptations locales), de l'installation du poste client à sa mise en production, on peut décrire les étapes comme ceci :

- installation du poste client ;
- intégration au domaine Horus ;
- installation du client Horus ;

- utilisation.

À cet instant les utilisateurs peuvent utiliser le poste client. Le module Horus est livré avec une configuration ESU par défaut.

Ensuite, via la **console ESU**, l'administrateur ("**admin**" par défaut) peut personnaliser la configuration, ajouter des groupes de machines, des groupes d'utilisateurs, modifier les règles, etc.

Fichiers invisibles sur les partages

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

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

- `desktop.ini` : les fichiers `desktop.ini` générés par le fonctionnement de Windows sont cachés à l'utilisateur (`hide files = /desktop.ini/` dans le fichier `smb.conf`) ;
- `$recycle.bin` : les fichiers `$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 fichiers `.scanned:*` générés par Scannedonly^[p.369] sont cachés et inaccessibles par l'utilisateur (`veto files = /.scanned:*/`).

7.2.1. Scripts personnalisés

Lorsqu'un utilisateur ouvre une session Windows sur le domaine Horus, le serveur génère un fichier `\\horus\netlogon<login>.bat`

Ceci est réalisé par l'intermédiaire du programme `/usr/share/eole/fichier/dyn-logon.py` qui génère le script `<login>.bat` en fonction de l'utilisateur, de ses groupes d'appartenance et du système d'exploitation de la station cliente (Win9X, Win2K, WinXP, Vista).

Par défaut, sur le module Horus, seuls les lecteurs réseaux des partages de l'utilisateur sont montés par ce script.

Pour ajouter des instructions au fichier `<login>.bat`, il est possible d'utiliser des scripts personnalisés pour :

- un utilisateur particulier : `\\horus\netlogon\users<login>.bat`
- une machine particulière : `\\horus\netlogon\machines<machine>.bat`
- un groupe particulier : `\\horus\netlogon\groups<group>.bat`
- un système d'exploitation particulier : `\\horus\netlogon\os<os>.bat`
- un groupe et un système d'exploitation : `\\horus\netlogon\os<os><group>.bat`
- un utilisateur et un système d'exploitation : `\\horus\netlogon\os<os><login>.bat`

Le contenu de ces fichiers sera ajouté au fichier `\\horus\netlogon<login>.bat`

Exemples

Pour ajouter une commande à tous les membres du groupe `DomainUsers` mais que pour les postes windows XP, le fichier sera :

```
\\horus\netlogon\os\WinXP\DomainUsers.bat
```

Pour ajouter une commande à tous les membres du groupe `compta` quelque soit le poste :

`\\horus\netlogon\groups\compta.bat`



Par défaut le contenu sera ajouté au début du fichier et donc avant le montage des lecteurs. Si vous voulez que le contenu soit ajouté après, il faut insérer `%NetUse%` dans le script personnalisé.

Les lignes suivants cette balise seront ajoutées à la fin du script `<login>.bat`



- les systèmes d'exploitations supportés sont : Win9X, Win2K, WinXP et Vista ;
- Windows 7 est traité de la même manière que Windows Vista (OS=Vista) ;
- les noms de machines doivent être écrits en minuscules.

7.2.2. Les profils utilisateurs

Les profils utilisateurs représentent l'environnement par défaut des utilisateurs.

Il existe trois types de profils qui sont gérés par les modules EOLE :

- le **profil local** :

il est stocké sur la station Windows, l'environnement est donc différent lorsque l'utilisateur change de poste.

- le **profil itinérant** :

il est stocké dans le répertoire personnel de l'utilisateur, l'environnement suit l'utilisateur.

- le **profil obligatoire** :

il est stocké dans un répertoire commun, l'environnement est le même pour tous **mais** il faut générer les profils avant de pouvoir l'utiliser.

Il n'y a rien de particulier à faire pour les profils locaux ou itinérants par contre les profils obligatoires doivent être créés.



Pour plus d'informations concernant les profils d'utilisateurs, veuillez consulter la documentation officielle de Microsoft :

<http://technet.microsoft.com/fr-fr/library/cc738303%28v=WS.10%29.aspx>



Profils utilisateurs vs ESU

Il est important de distinguer les profils utilisateurs (notion interne à Windows) et ESU.

En effet les profils utilisateurs sont appliqués en premier et définissent un environnement de 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.

7.2.2.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 adaptées 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

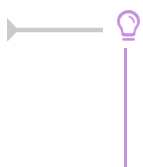
Si des profils autres que locaux (exceptés les profils admin et admin.profil) sont déjà présents sur la machine, il est préférable de les supprimer.

Afin d'éviter des effets de bords, n'installez que les logiciels nécessaires à la génération du profil.

Il arrive que certains logiciels mal programmés paramètrent des valeurs qui provoquent une erreur lorsque le profil est appliqué sur une station où le logiciel n'est pas installé.

Installation des programmes à pré-paramétrer dans le profil obligatoire

Toutes les applications n'ont pas forcément besoin d'être paramétrées dans le profil obligatoire. Il peut arriver que certaines applications n'apprécient pas ce mode de fonctionnement. Il est nécessaire de faire des tests pour en déterminer la liste.



L'utilisation d'un logiciel de virtualisation (proposant l'enregistrement de l'état à un instant t) permet d'installer une version propre de Windows et de repartir du profil utilisé lors de la dernière copie.

Génération du profil

Pour générer un profil prêt à être copié il faut pré-paramétrer les applications, l'explorateur et le bureau :

- ouvrir une session avec l'utilisateur "*admin.profil*" sur un client XP ;
- 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 privé 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:\.ConfigApplications Data**.

Ces dernières informations sont donc retrouvées lors de la prochaine ouverture de session. Par exemple, LibreOffice enregistre la validation de sa licence une fois pour toutes.

Le fond d'écran bénéficie d'une gestion particulière dans ESU :

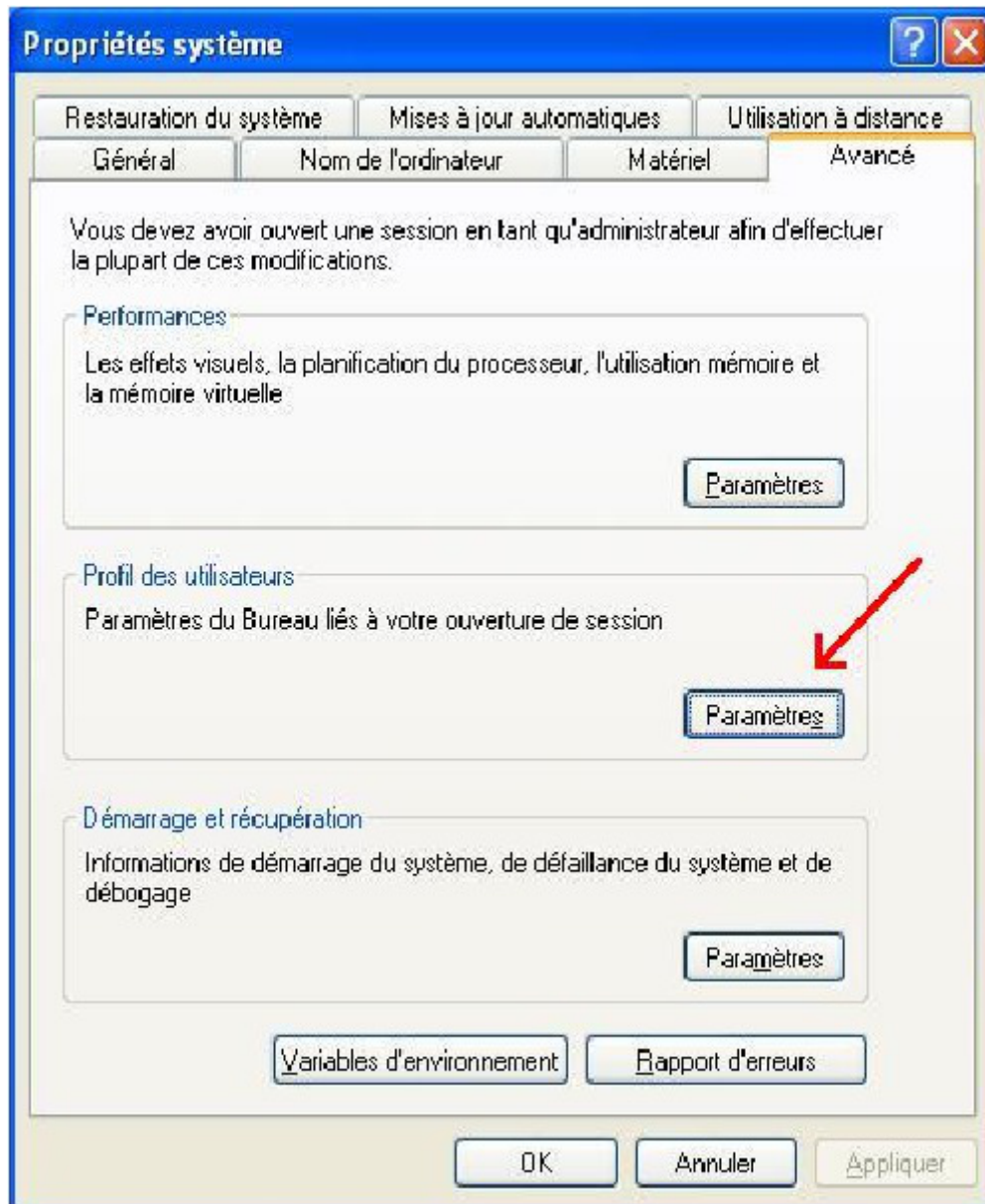
- la spécification d'un fichier image à afficher
- l'ajout d'informations textuelles en haut à droite.

Les deux étant incompatibles, il vaut mieux le désactiver pour éviter tout effet de bord. Pour se faire sélectionner **Aucun** dans **Propriétés de l'affichage/Bureau/Arrière-plan**.

Copie du profil

Ouvrir une session avec l'utilisateur **admin**. Aller dans le **Panneau de configuration** → **Système** → **Propriétés** → **Avancé**. Dans le cadre **Profil des utilisateurs** cliquer sur **Paramètres**.

Dans la nouvelle fenêtre, sélectionner le profil correspondant à l'utilisateur **admin.profil**.

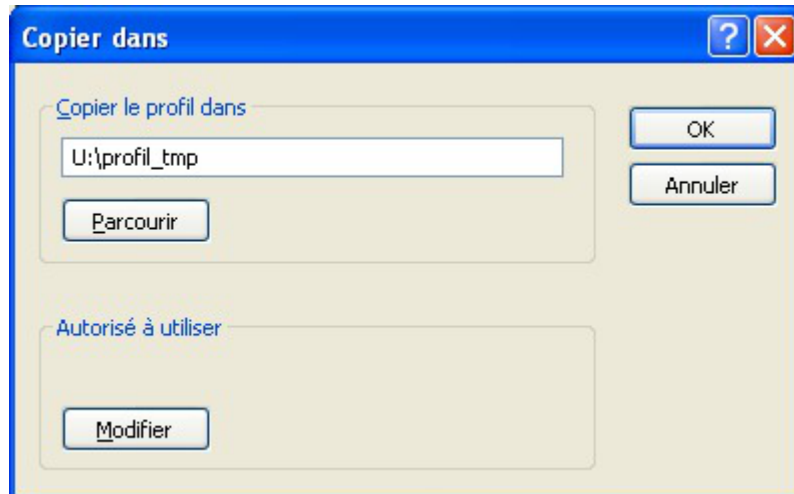


Dans la partie **Autorisé à utiliser** cliquer sur **Modifier**. Entrer **tout le monde** puis cliquer sur **Vérifier les noms**.



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`

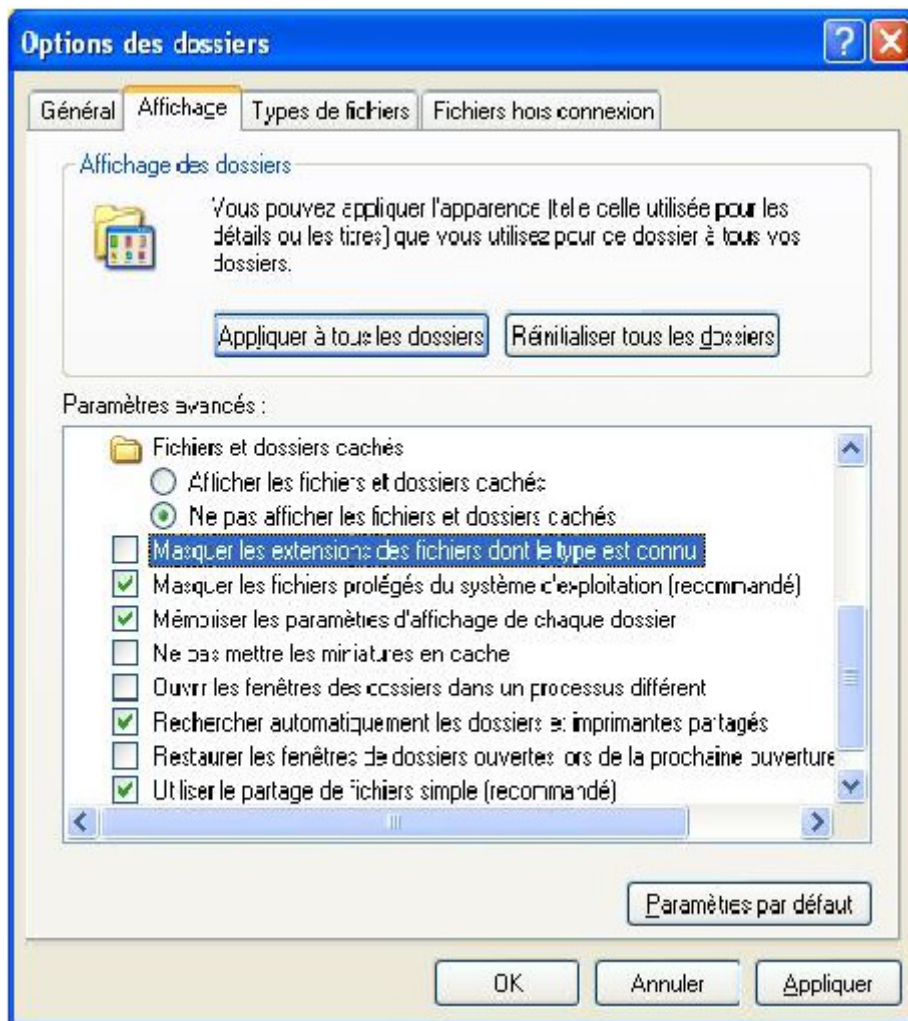
Sur le module Scribe, il est également possible d'utiliser le dossier `\\<adresse_serveur>\netlogon\profil2`

Ceci permet de spécifier un profil différent pour certains utilisateurs (ex. : profil pour les professeurs et profil2 pour les élèves).

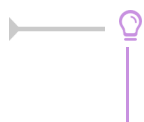
Lorsque le profil est copié directement sur le serveur dans le répertoire `\\<adresse_serveur>\netlogon\profil\`, Windows applique automatiquement les droits d'écriture à tout le monde sur le dossier profil.
Le passage par un répertoire temporaire évite d'avoir à manipuler les droits et diminue le risque 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`).

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.

7.2.2.b. Création de profil obligatoire sous Windows 7

Pour générer un profil obligatoire sous Windows 7, la marche à suivre est à peu près la même que pour Windows XP :

1. créer un utilisateur `admin.profil` possédant un profil local ;
2. ouvrir une session avec `admin.profil` ;
3. paramétrer le profil et fermer la session ;
4. ouvrir une session avec `admin` pour copier le profil.

La subtilité se trouve ici, sous Windows 7 le bouton `Copier vers` est grisé pour les utilisateurs du domaine.

Une des solutions permettant de contourner le problème est d'utiliser un utilitaire nommé `Windows Enabler`.

Sous Windows 7 SP1, pour que `Windows Enabler` fonctionne, il faut impérativement désactiver l'

UAC^[p.371] 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.

7.2.2.c. Les sessions locales

Si des chemins ont été 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.371]AC^[p.371].

Le programme `logon.exe` affiche alors la question : Ré-initialiser le Menu démarrer et le Bureau ? suivit par celle de l'UAC^[p.371] (si il est activé) pour la validation de l'action.

L'UAC^[p.371] 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.

7.2.3. Gestion des configurations clientes avec ESU

7.2.3.a. Introduction

Présentation

ESU^[p.364] 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.

7.2.3.b. La console ESU

> Présentation

La console ESU sert à paramétrer les règles qui seront appliquées sur les machines clientes lors de l'ouverture de session. La liste des règles disponibles est définie dans le fichier `\\<adresse_serveur>\esu\Console\ListeRegles.xml`. Elles sont réparties en deux groupes :

- les règles "machines" définissant le comportement global des machines, elles sont appliquées quelque soit l'utilisateur qui se connecte ;
- les règles "utilisateurs" définissant l'environnement de l'utilisateur comme les restrictions, le paramétrage de l'explorateur et du fond d'écran, etc.

Par défaut, seul l'utilisateur **admin** a accès à la console. Pour faciliter l'accès un raccourci est créé dans son répertoire personnel (U:).

La console est organisée en trois parties :

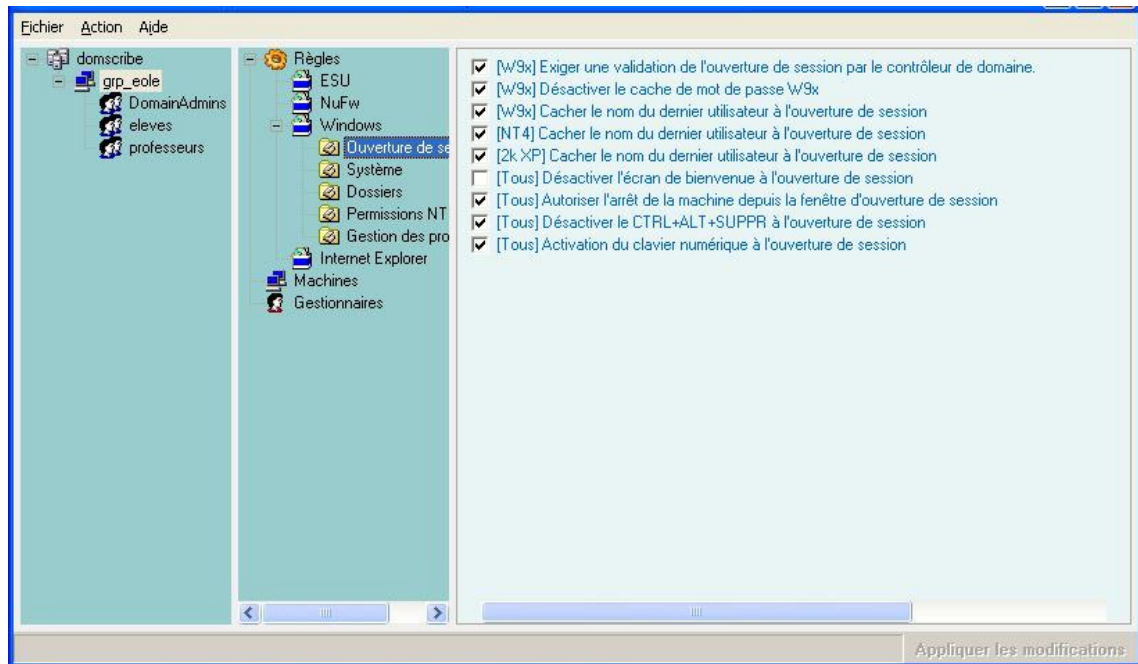
- la première liste les groupes de machines du domaine, et les utilisateurs/groupes gérés dans ce groupe de machines ;
- la seconde contient les différentes catégories de règles. Ces catégories peuvent comporter des sections ;
- la troisième partie affiche les règles et leur paramétrage.

La première colonne montre l'organisation générale d'ESU. La première ligne indique le nom du domaine.

Celui-ci contient un ensemble de groupes de machines définis en fonction du nom des machines. Chaque groupe de machine contient des utilisateurs ou des groupes d'utilisateurs.

Lors de l'ouverture de session, ESU va chercher à quel groupe de machines appartient la machine sur laquelle l'utilisateur se connecte. Si un groupe de machine est trouvé, ESU va chercher s'il contient l'utilisateur ou un des groupes auxquels l'utilisateur appartient.

La liste des groupes de machines et des utilisateurs est parcourue du haut vers le bas. Si une machine appartient à plusieurs groupes, le premier sera utilisé, les autres ignorés. Il en va de même pour les utilisateurs/groupes d'utilisateurs.



Fenêtre principale d'ESU

> Les groupes de machines

Création d'un nouveau groupe de machines

Les groupes de machines servent à regrouper les machines dans une même configuration en fonction de leur nom.

A l'installation du module, ESU est pré-configuré avec un groupe de machines *grp_eole* paramétré afin de prendre en compte toutes les machines du domaine (Simplement le caractère "*").

Ce groupe de machines a été pré-crée 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**.

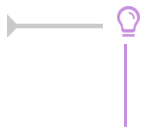
Renseignez le nom du groupe de machine (ici *technologie*) et paramétrez les noms des machines à ajouter au groupe.



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 joker (*) pour paramétrer les noms de machines prises en compte par le groupe

Une fois le groupe de machines créé, il faut établir sa priorité par rapport au groupe de machine *grp_eole* (si il n'a pas été supprimé) : clic droit sur le groupe de machine et choisir "**Augmenter la priorité**".

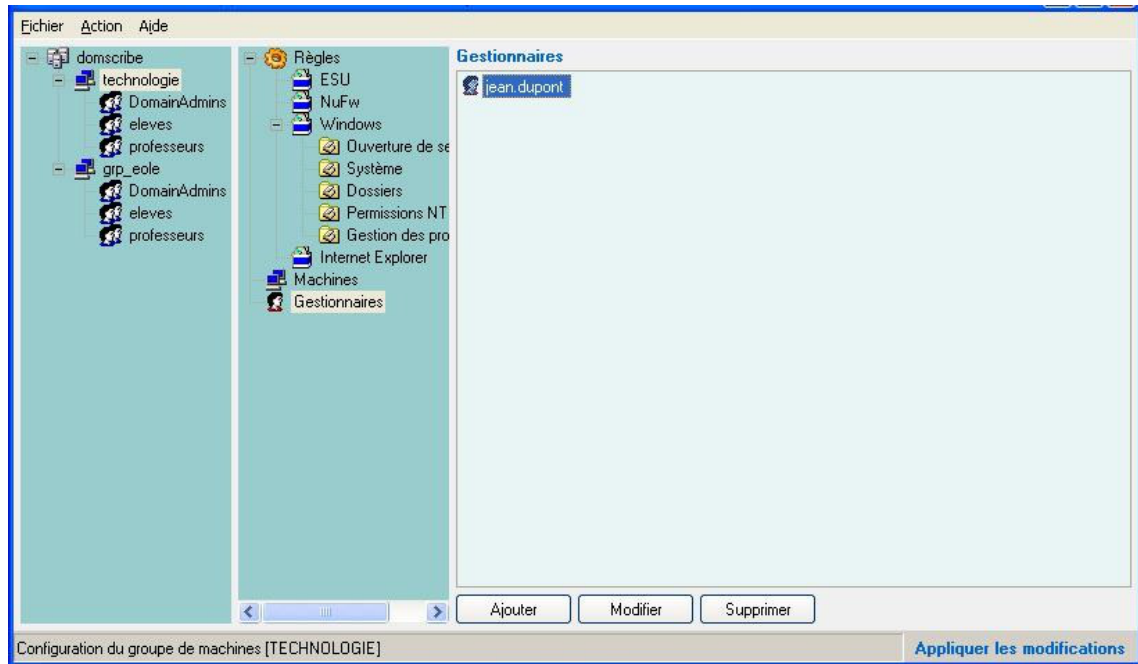


Augmenter la priorité d'un utilisateur

Les Gestionnaires

L'item "**Gestionnaires**" permet de déléguer l'administration d'un ou plusieurs groupes de machines à un autre utilisateur ou à un autre groupe. Lorsqu'un utilisateur lance la console, il n'a accès qu'aux groupes de machines pour lesquels il est défini comme gestionnaire.

Le gestionnaire peut modifier la configuration ESU de son groupe de machines et a aussi accès en écriture au répertoire contenant les icônes (`I:\<nom_du_groupe_de_machines>\`).



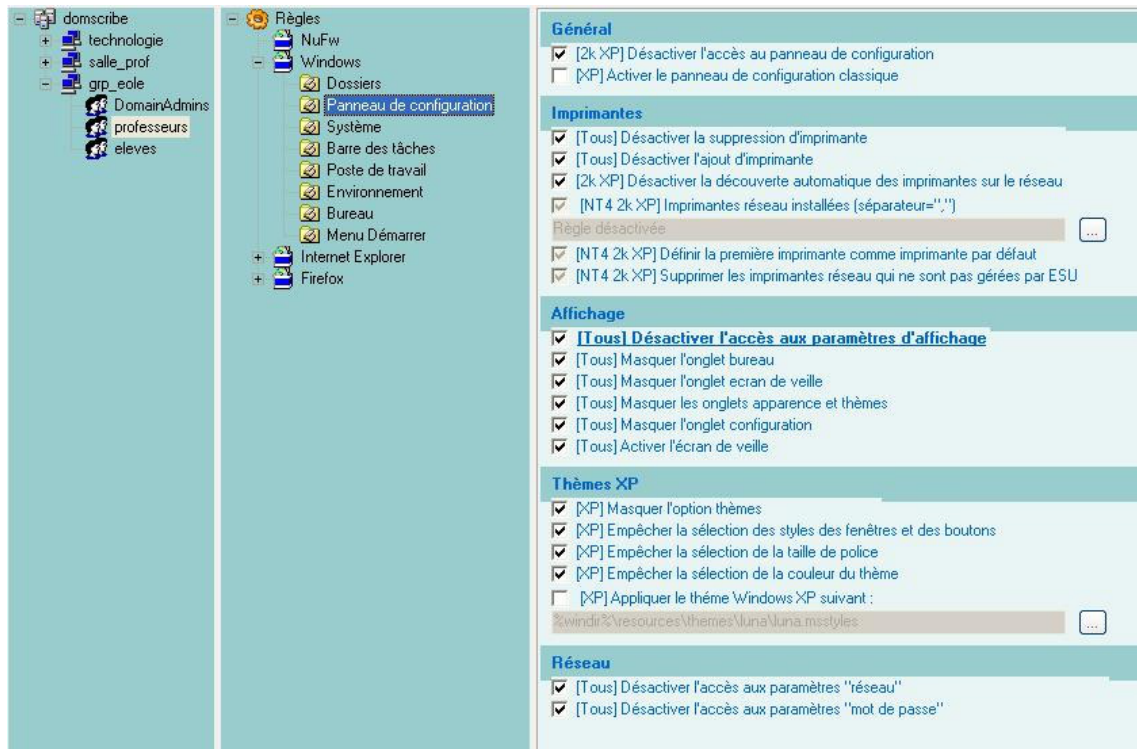
Ajout de gestionnaires dans un groupe de machines

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

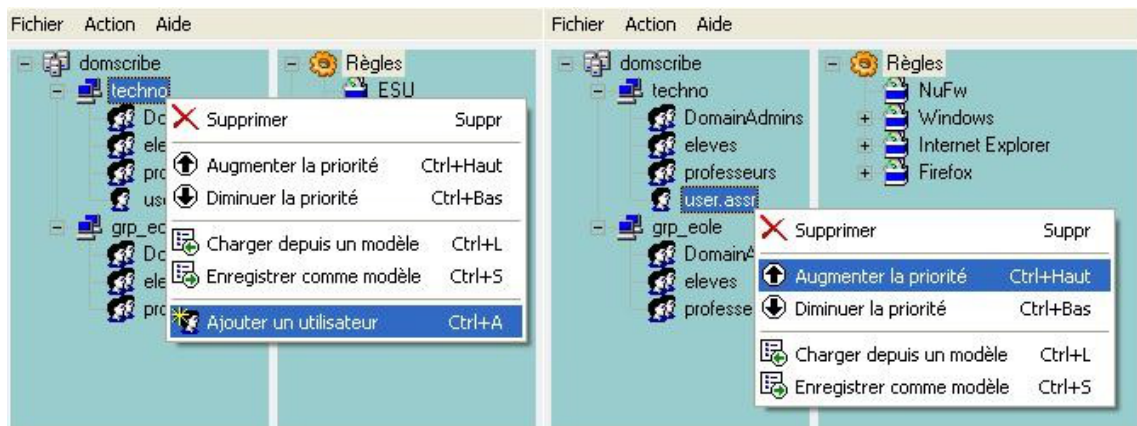
Un environnement différent peut être appliqué en fonction du nom de l'utilisateur ou des groupes auxquels il appartient.



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 *elevés*. Pour lui appliquer une configuration spécifique, il faut lui affecter une priorité supérieure à celle du groupe *elevés*.



Augmenter la priorité d'un utilisateur

> 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.

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

Sur les autres modules, l'onglet **Esu** n'est visible qu'après activation du service dans l'onglet **Services** en passant l'option : Utiliser le logiciel ESU à oui.

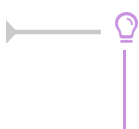


Vue de l'onglet Esu de l'interface de configuration du module

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

Après avoir passé la variable Activer le proxy ESU à oui il faut saisir l'adresse IP ou le nom du proxy ESU dans le champ Adresse du proxy ESU et si besoin changer le port 3128 proposé par défaut.

Le champ Ne pas utiliser le proxy ESU pour permet d'ajouter plusieurs adresses IP, réseaux, noms de domaine et noms de machines pour lesquels le proxy ESU ne sera pas utilisé (exemple de valeurs : mozilla.org, asso.fr, 192.168.1.0/24).



Sur le module AmonEcole, l'adresse IP du proxy correspond à celle renseignée dans l'onglet **Interface-1** (variable : adresse_ip_eth1_proxy_link).

L'utilisation du logiciel ESU modifie profondément la configuration des stations clientes (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.361] tels que sauvegardés.

Vous pouvez restaurer la base de registre de la station en appliquant des fichiers .REG^[p.361] tels que celui fourni par l'archive suivante :
<ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip>

Dans le cas où, sur le module Horus, on active ESU, il devient obligatoire d'installer le logiciel client Horus.

À l'inverse, l'installation du client sans procéder à l'activation d'ESU n'a pas de sens.

> Trucs et astuces

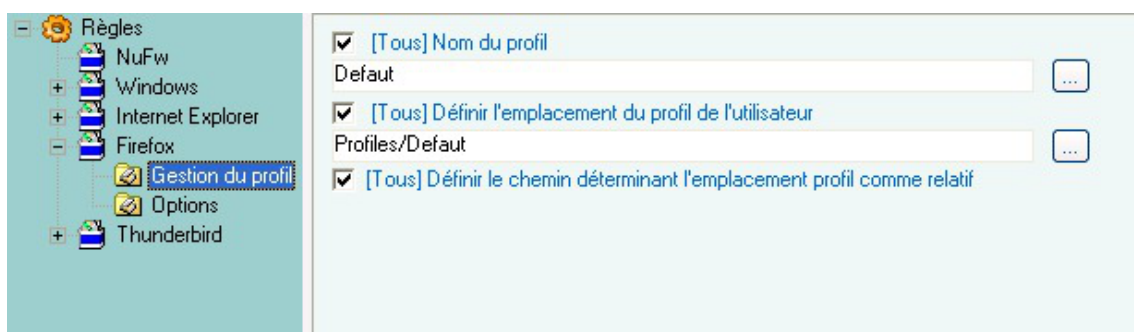
Les dossiers d'icônes

- les icônes placées dans `R:\grp_eole_Machine\Bureau` seront visibles par tous les utilisateurs ;
- les icônes placées dans `R:\grp_eole\professeurs\Bureau` ne seront visibles que par les professeurs.

Attention, l'utilisateur *admin* fait partie du groupe *professeurs* mais, il est également membre du groupe *DomainAdmins*. Au vu des priorités, c'est le dossier défini d'icônes du groupe *DomainAdmins* (`R:\grp_eole\professeurs\Bureau`) qui lui sera proposé.

Firefox

Afin de paramétrer correctement la *Gestion du profil* Firefox avec ESU, il faut sélectionner au moins une *Option*, la page de démarrage par exemple.



Configuration ESU du profil Firefox

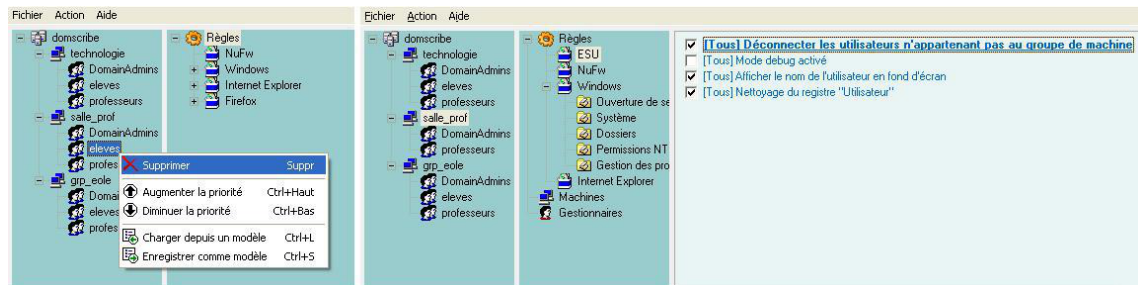


Configuration ESU des options Firefox

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.

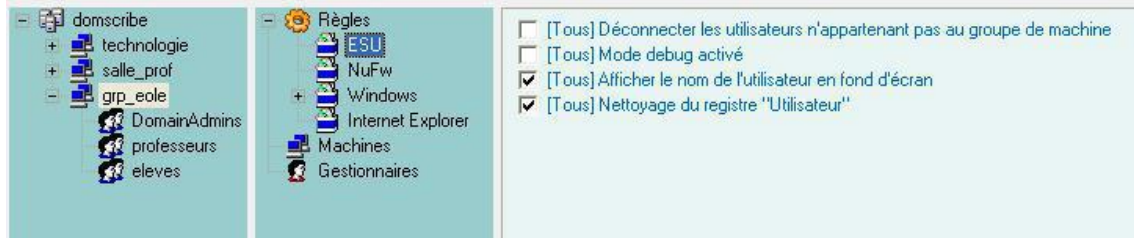
Pour les groupes d'utilisateurs

- `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*).

7.2.3.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.



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%
- %GROUPE%
- %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%
GROUPE == %GROUPE%
IP == %IP%
NUMBER_OF_PROCESSORS == %NUMBER_OF_PROCESSORS%
PROCESSOR_IDENTIFIER == %PROCESSOR_IDENTIFIER%
PROCESSOR_LEVEL == %PROCESSOR_LEVEL%
#####

```


D'autre informations ...

#####

Résultat :

```

USERLNAME == admin admin
COMPUTERNAME == VM-XP1
ESU_OS == WinXP
ESU_GU == DomainAdmins
GROUPES == ['DomainAdmins', 'DomainUsers', 'PrintOperators', 'professeurs']
IP == 192.168.230.157
NUMBER_OF_PROCESSORS == 1
PROCESSOR_IDENTIFIER == x86 Family 15 Model 4 Stepping 8, GenuineIntel
PROCESSOR_LEVEL == 15

#####
D'autre informations ...
#####

```

7.3. Déploiement d'applications pour Windows avec WPKG

WPKG est une application de déploiement d'applications pour Windows.

Elle permet l'installation, la mise à jour et la dés-installation automatique de logiciels.

<http://wpkg.org/>

L'application WPKG est composée d'un exécutable (`wpkg.js`) et de fichiers de configuration XML copiés dans un dossier partagé sur le serveur de fichier.

Les fichiers XML sont séparés en 3 parties :

- **packages**, les applications installables ;
- **hosts**, les postes ou groupes de postes ;
- **profiles**, la liste de packages à installer pour un host.

Le fichier `wpkg.js` doit être exécuté sur les postes Windows. Il lit les fichiers XML (`config/host/profiles/packages`) et installe en conséquence les applications sur les postes.

Afin d'exécuter `wpkg.js` automatiquement il faut utiliser un lanceur, au choix :

- WPKG Client ;
- Wpkg-GP ;
- une tâche planifiée Windows ;
- n'importe quel autre programme capable d'exécuter `wpkg.js`.

Dans le cas de l'utilisation de WPKG Client et de Wpkg-GP, ils s'installent sous forme de service Windows et s'exécute au démarrage de la machine.



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`.

7.3.1. Installation et configuration

Installation et utilisation de WPKG sur un serveur EOLE

WPKG peut être utilisé sur un serveur Scribe ou Horus si le paquet `eole-wpkg` est installé.

Le paquet s'installe avec la commande :

```
# apt-eole install eole-wpkg
```

L'application WPKG est alors stockée dans le répertoire partagé `\\<SERVEUR>\wpkg`

Elle est paramétrée en accès anonyme et en lecture seule (lecture/écriture pour DomainAdmins).

L'accès au répertoire partagé wpkg n'étant pas très pratique, on peut ajouter un lien symbolique dans le dossier personnel (U:) de l'utilisateur admin (comme c'est déjà le cas pour le partage esu) :

```
# ln -s /home/wpkg/ /home/a/admin/perso/wpkg
```



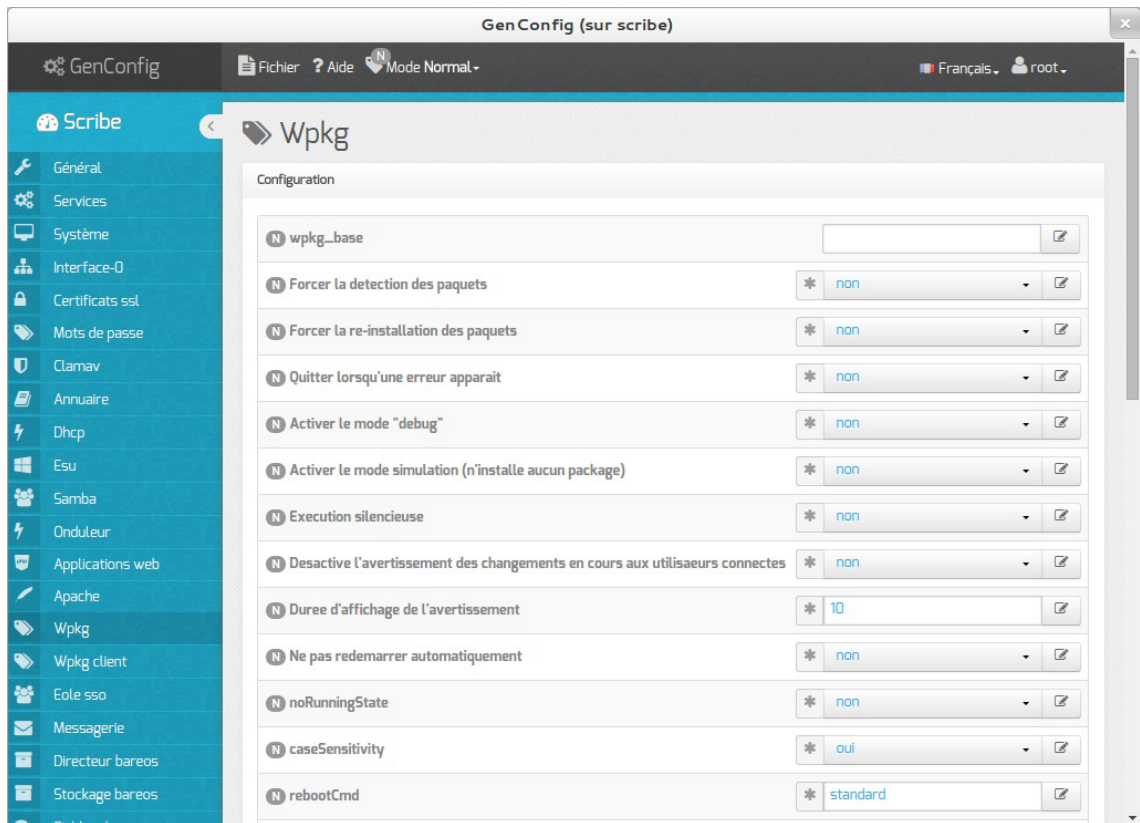
Le paquet `eole-wpkg` fournit les dictionnaires et templates permettant de gérer la configuration de WPKG depuis le serveur Zéphir.

Configuration

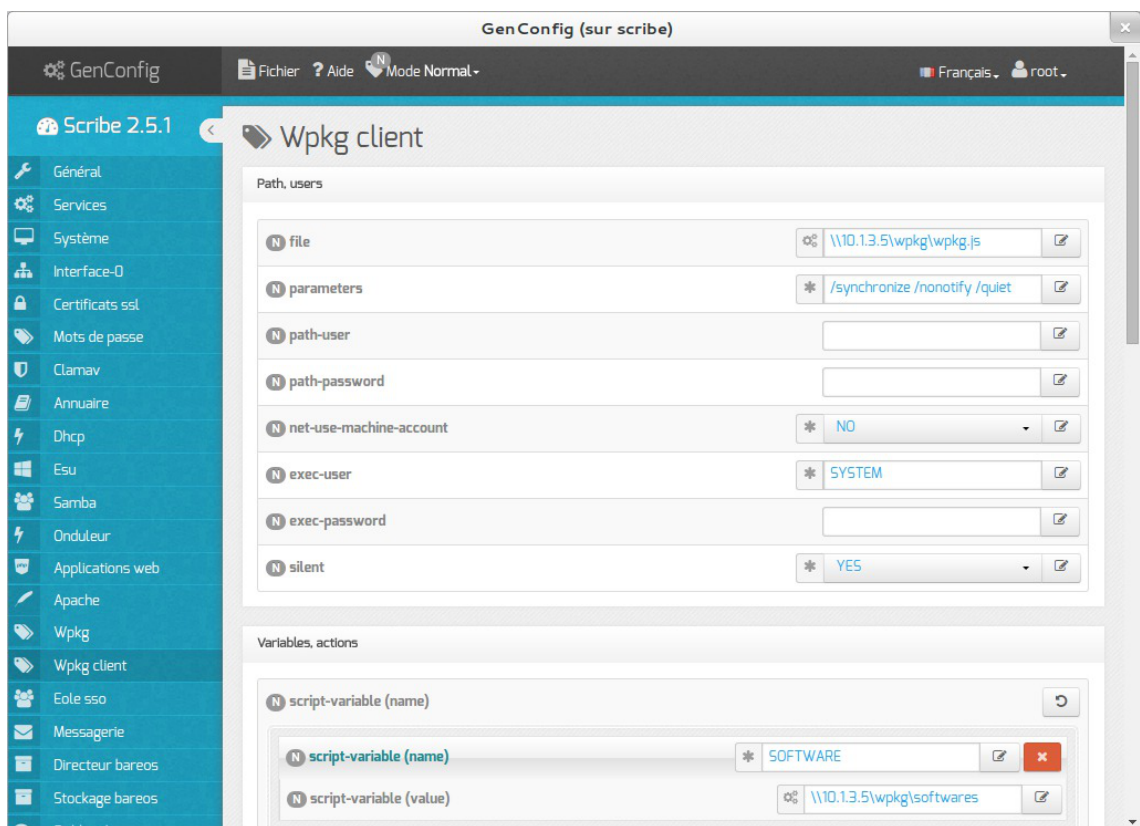
L'outil de gestion de la configuration est l'interface de configuration du module.

Dans l'interface de configuration du module, dans l'onglet `Services`, le service `Gérer la configuration WPKG` est à `oui` par défaut et 2 onglets concernant WPKG sont visibles :

- Wpkg : les options paramétrables du fichier `config.xml` (options de wpkg.js)



- Wpkg client : les options paramétrables des fichiers `settings.xml` (WPKG Client) et `wpkg-gp.ini` (Wpkg-GP)



#fixme compléter l'essentiel de la configuration

Il faut ensuite reconfigurer le serveur à l'aide de la commande `reconfigure` :

```
# reconfigure
```

Installation du client WPKG

Il existe plusieurs façons d'exécuter le moteur `wpkg.js` sur un poste Windows. Il est recommandé d'utiliser les applications suivantes :

- WPKG Client pour Windows XP : <http://wpkg.org/files/client/stable/>
- Wpkg-GP pour Windows Vista et supérieurs : https://drive.google.com/folderview?id=0B9Eadi-crzpOvEtTM01aYm5YNm8&usp=drive_web



Il ne faut installer que l'un des deux, installer WPKG Client et Wpkg-GP sur la même machine provoque des comportements inattendus.

Des scripts `.bat` permettent une installation des clients sans question. Pour que ces scripts fonctionnent il faut télécharger les clients en prenant soin de les placer au bon endroit et de bien les nommer.

Après avoir téléchargé les clients (Wpkg-GP et WPKG Client), pour que les scripts fonctionnent il faut les renommer en :

- `WPKG_Client32.msi`
- `WPKG_Client64.msi`
- `Wpkg-GP_x86.exe`
- `Wpkg-GP_x64.exe`

Depuis un poste Windows, télécharger les 4 installeurs (2 en 32bits et 2 en 64bits) et les copier de manière à obtenir :

- `\\<SERVEUR>\wpkg\WPKG_Client32.msi`
- `\\<SERVEUR>\wpkg\WPKG_Client64.msi`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x86.exe`
- `\\<SERVEUR>\wpkg\Wpkg-GP_x64.exe`

Configuration du contenu de WPKG avec l'application Wpkg-Manage

Un fois WPKG installé, il faut configurer les applications et leurs dépendances ainsi que les machines sur lesquelles elles seront installées.

Wpkg-Manage est une application écrite par Christophe Dezé de l'académie de Nantes permettant de gérer la configuration utilisateur de WPKG.

La configuration consiste à définir :

- des hosts, liste de machines associés à un profile ;
- des profiles, liste de paquets à installer ou à mettre à jour ;
- des packages, descriptions des applications à installer (commandes, tests, etc.).

<http://eole.ac-dijon.fr/pub/Outils/Wpkg-manage/>

Wpkg-Manage permet de gérer le contenu de WPKG, ses fonctionnalités principales sont :

- import des groupes de machines ESU dans WPKG ;
- association des groupes de machines avec les paquets ;
- possibilité de génération de nouveau paquets ;
- téléchargement semi-automatique des installeurs (`.exe`, `.msi`) ;
- fichiers exemples de paquets.

L'installation de l'application Wpkg-Manage doit se faire manuellement depuis le serveur :

```
# wget http://eoleng.ac-dijon.fr/pub/Outils/Wpkg-manage/wpkg-manage.zip
# unzip wpkg-manage.zip
# mv wpkg-manage /home/wpkg/
```



WPKG utilise les notions suivantes :

- hosts (nom de la machine, possibilité d'expression régulière. Ex.: "cdi.*")
`http://wpkg.org/Hosts.xml:fr`
- packages (description d'une application, version, chemin vers .exe, etc.)
`http://wpkg.org/Packages.xml:French`
- profiles (association entre les "hosts" et les "packages" à y installer)
`http://wpkg.org/Profiles.xml:French`

Tests et exécutions manuelles

Il est parfois nécessaire d'exécuter WPKG manuellement sur un poste client pour faire des vérifications.

Il est possible d'exécuter directement le moteur WPKG sans utiliser le client à condition de renseigner les variables WPKG :

```
set ip-scribe=<ADRESSE IP SCRIBE>
set SOFTWARE=\\%ip-scribe%\wpkg\softwares
cscript \\%ip-scribe%\wpkg\wpkg.js /synchronize /nonotify /quiet
```

WPKG Client

Si le client est paramétré pour s'exécuter à l'arrêt de la station, il suffit d'arrêter le service WPKG :

```
net stop wpkg-service
```

Si le client s'exécute au démarrage de la station, il suffit de redémarrer le service :

```
taskkill /F /IM WPKGSrv.exe
net start wpkg-service
```

Wpkg-GP

Pour exécuter Wpkg-GP :

```
C:\Program Files\Wpkg-GP\Wpkg-GP-Test.exe
```

7.3.2. Les packages WPKG

Présentation

Les packages WPKG sont les fichiers décrivant l'installation et la désinstallation des applications Windows. Ils sont contenus dans le répertoire `wpkg/packages/`.

Les packages contiennent, entre autres, la version du logiciel et le chemin vers le programme d'installation.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- OpenSource -->
<packages>
<package id="7zip"
name="7-Zip"
revision="%version%"
reboot="false"
priority="0">
<variable name="version" value="922" />
<variable name="longversion" value="9.22" />
<variable architecture="x86" name="platf" value="" />
<variable architecture="x64" name="platf" value="-x64" />
<check type="logical" condition="or">
<check type="file" condition="versionequalto"
path="%PROGRAMFILES%\7-Zip\7zFM.exe" value="%longversion%.0.0" />
<check type="file" condition="versionequalto"
path="%PROGRAMFILES(x86)%\7-Zip\7zFM.exe" value="%longversion%.0.0"
/>
</check>
<e o l e d l
dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio
destname="7zip/7z%version%.msi" />
<e o l e d l
dl="http://sourceforge.net/projects/sevenzip/files/7-Zip/%longversio
destname="7zip/7z%version%-x64.msi" />
<install cmd='msiexec /qn /norestart /i
"%SOFTWARE%\7zip\7z%version%%platf%.msi" />
<upgrade cmd='msiexec /qn /norestart /i
"%SOFTWARE%\7zip\7z%version%%platf%.msi" />
<remove cmd='msiexec /qn /x
"%SOFTWARE%\7zip\7z%version%%platf%.msi" />
```



```
</package>
```

```
</packages>
```



Explication sur les balises :

- id : identifiant WPKG de l'application ;
- name : nom de l'application à afficher ;
- revision : nombre entier définissant la version de l'application, il doit être incrémenté pour que WPKG mette l'application à jour ("upgrade") ;
- check : test(s) pour vérifier la présence d'une application (si elle est déjà installée) ;
- install : commande(s) à exécuter pour installer l'application ;
- upgrade/downgrade : commandes pour mettre à jour / rétrograder une application ;
- remove : commande pour désinstaller une application.

Davantage d'explications sur le site officiel de WPKG : <http://wpkg.org/Packages.xml:French>

Le projet EOLE wpkg-package propose des packages adaptés à l'environnement EOLE :

<http://dev-eole.ac-dijon.fr/projects/wpkg-package/>

Il contient des fichiers `<package>.xml` directement fonctionnels dans un environnement Horus/Scribe, à quelques (exceptions) près, ainsi que des icônes, des scripts et des outils (dans le dossier `softwares`).

<http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/>

Liste des applications supportées :

<http://dev-eole.ac-dijon.fr/projects/wpkg-package/repository/revisions/master/show/packages>

Téléchargement du projet wpkg-packages

Sous Windows

Le logiciel TortoiseGit permet de récupérer les `.xml` sur nos dépôts : <http://tortoisegit.org/>

Une fois installé, récupérer le projet `wpkg-packages` à l'adresse <http://dev-eole.ac-dijon.fr/git/wpkg-package.git>

Sous GNU / Linux

La manipulation peut se faire depuis le serveur Scribe/Horus.

Il est nécessaire d'installer Git :

```
# apt-eole install git-core curl
```

Pour télécharger l'ensemble des fichiers `<packages>.xml` du dépôt il faut le cloner :

```
# cd /root
```

```
# git clone https://dev-eole.ac-dijon.fr/git/wpkg-package
```

Lorsque que le dépôt est déjà cloné il faut le mettre à jour :

```
# cd /root/wpkg-package
```

```
# git pull
```


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 `<eole dl>`. Cette balise indique l'URL où télécharger le ou les installateurs de l'application.

Pour télécharger l'ensemble des installateurs :

```
# cd /home/wpkg/packages/
# ./download installers.py
```



Certains installateurs 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 `icônes` avec les icônes du Bureau et du Menu démarrer correspondantes aux packages.

Ce dossier contient les icônes pour Windows 32-bits et 64-bits dans des sous-dossiers séparés, les chemins de ces icônes pouvant être différents.

Softwares

Le projet `wpkg-package` contient un dossier nommé `Softwares` nécessaire à l'exécution de certains packages. Il faut en copier le contenu dans le dossier `wpkg\softwares\` (dossier correspondant à la variable `%SOFTWARE%`). Ce dossier contient notamment un sous-dossier nommé `tools` qui rassemble divers outils comme par exemple `nircmd`, `setacl`, `wget`...

Fonctionnement du téléchargements des installateurs

Le fichier `.xml` contient une ou plusieurs balises `<eole dl>`.



```
< e o l e d l
dl="http://launchpad.net/ocsinventory-windows-agent/2.0/2.0.3/+down.
destname="ocsinventory\" unzip='1' />
```

- `dl` : lien vers le fichier à télécharger ;
 - `destname` : nom d'un dossier ou d'un fichier ;
- Dans le cas d'un dossier aucun changement de nom est effectué, le fichier est seulement placé dans le dossier. Dans le cas d'un nom de fichier, le fichier téléchargé est renommé.
- Dans tous les cas, si le dossier n'existe pas il est créé. Pour qu'un nom soit considéré

comme un dossier il doit se finir par le caractère `\` ou `\\`.

- unzip : indique s'il faut désarchiver le fichier téléchargé.

Contributions

Il est possible de contribuer à la maintenance de ces fichiers et à l'ajout de nouveaux packages. Il faut demander l'ouverture d'un accès sur la forge ou communiquer sur les listes de discussion.

Pour la création d'un nouveau paquet, voici quelques recommandations.

Convention de nommage

Certaines règles sont à respecter lors de la création d'un nouveau package afin de garder un système unifié et pérenne.

Un package est identifiable par les deux balises suivantes :

- id : identifiant unique de l'application dans WPKG (sensible à la casse) ;
- name : nom de l'application.

Le champ id est le plus important, il doit respecter les conventions suivantes :

- sans espace ;
- tout en minuscules ;
- sans numéro de version (`firefox` et non `firefox15`).

Tests des packages : check

La plupart des installeurs ajoute une entrée `Uninstall` pour apparaître dans la section `Ajout/Suppression de programmes` de Windows.

On peut utiliser cette clé pour tester la présence d'une application. Mais une clé de registre ne prouve pas qu'une application est réellement présente. Il faut aussi tester l'existence des fichiers de l'application.



```
<check type="uninstall" condition="exists" path="QT Lite
%version%" />
<check type="file" condition="exists" path="%progfiles%\QT
Lite\QuickTimePlayer.exe" />
```

Validation de la syntaxe XML

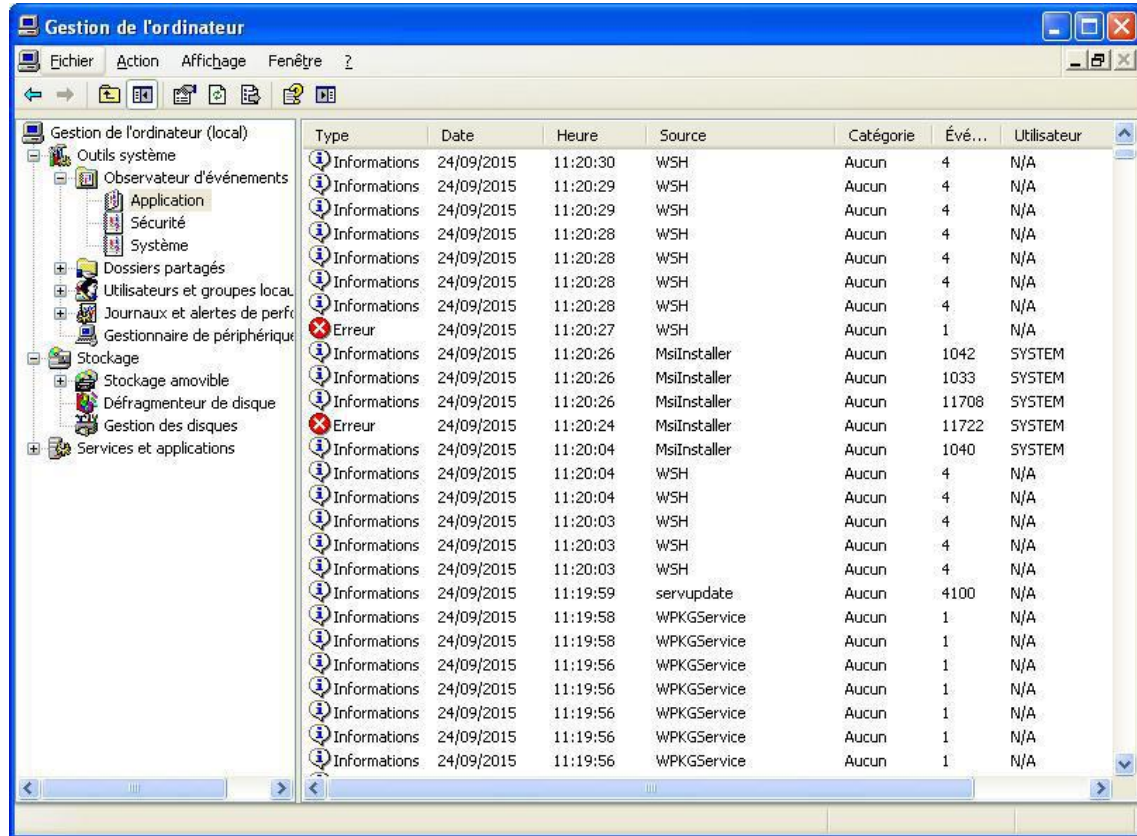
Il est toujours possible de faire une faute de frappe dans un fichier XML, un validateur XML en ligne permet de vérifier la syntaxe XML du fichier : <http://xmlvalidation.com/>.

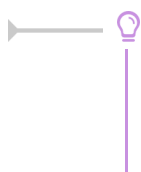
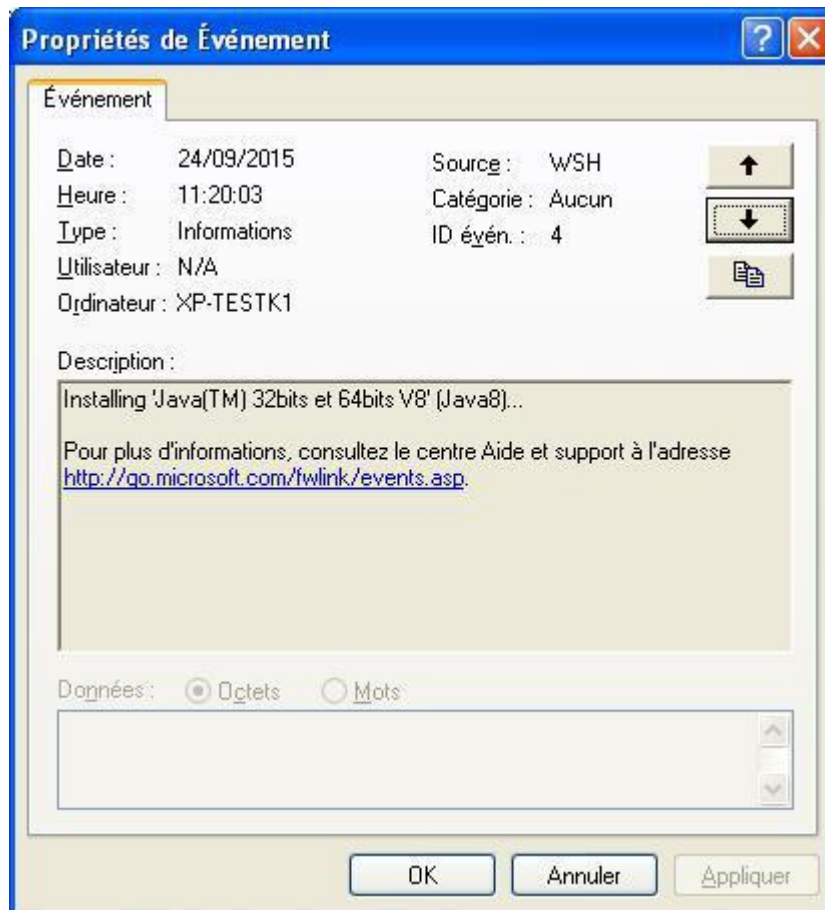
Voir aussi...

WPKG logiciels avec traitement particulier ^[p.313]

7.3.3. Journalisation des actions WPKG

Par défaut WPKG journalise ses actions dans l'observateur d'événements Windows, accessible dans la console de gestion de l'ordinateur (Microsoft Management Console) qui s'obtient avec un clic droit sur le Poste de travail puis Gérer dans le menu contextuel.





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 :

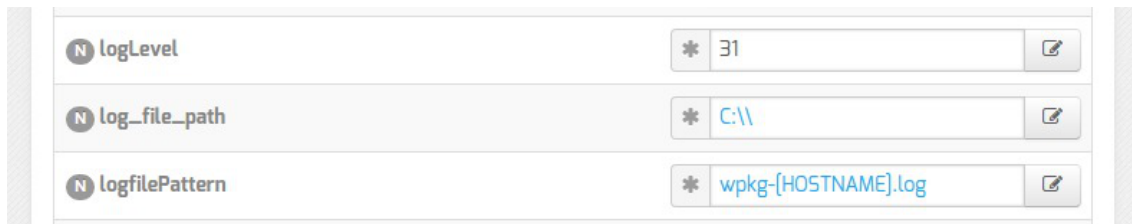
```
/log_file_path:c:/logLevel:31
```

- 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`.

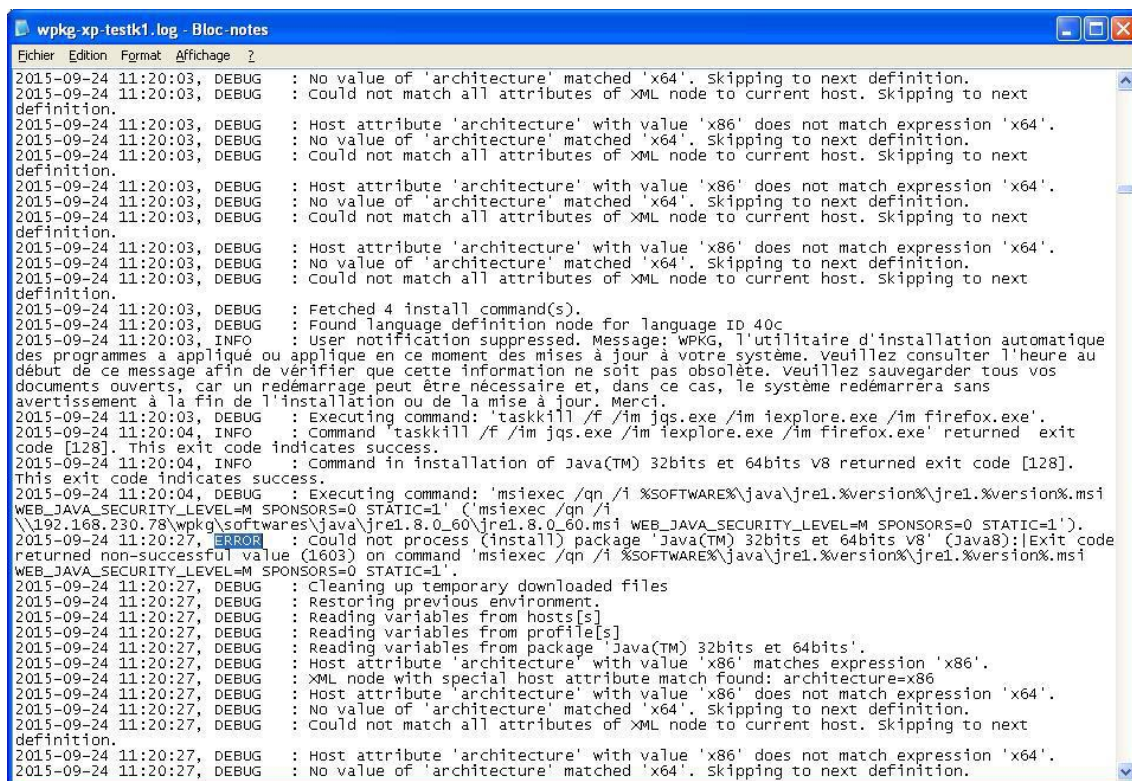


Enregistrer et quitter l'interface de configuration du module.

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`



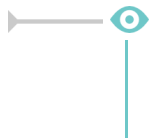
Granularité des logs

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 ;

- 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

7.3.4. WPKG scripts de pre et post installation

L'utilisation de dossiers dans un lecteur réseau pour les icônes du Menu Démarrer et du Bureau pose problème avec WPKG.

Une erreur se produit lorsque WPKG installe une application dont l'installateur 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 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'installateur 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'installateur ne trouve donc pas le lecteur `R:` et annule sa procédure d'installation. On peut observer le dossier `%PROGRAMFILES%\OpenOffice\` qui grossit 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'installateur 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

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
```

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>`

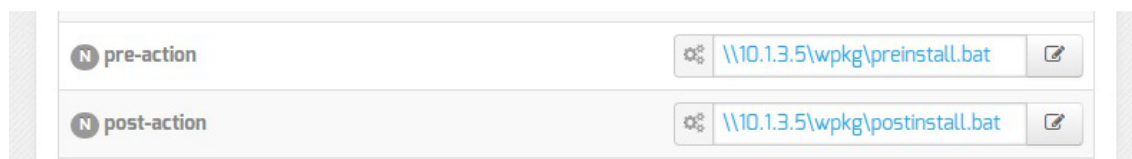
Cette méthode présente l'avantage de ne pas avoir à modifier la configuration des clients WPKG mais présente l'inconvénient de devoir les appeler pour chaque application dont l'installateur crée des icônes sur le Bureau et/ou dans le Menu démarrer.

- utiliser les actions `pre-action` et `post-action` de WPKG

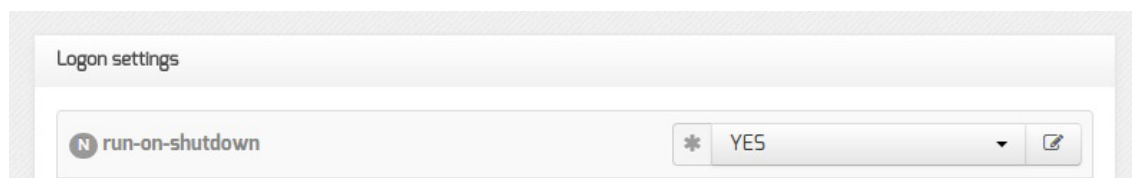
Cette méthode a l'avantage d'être faite une bonne fois pour toute mais demande à mettre la configuration WPKG à jour sur chaque poste.

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 passer 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 installateurs 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`).

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.

7.3.5. WPKG logiciels avec traitement particulier

Java

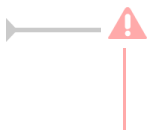
Sur Windows Vista/Seven il faut décompacter l'installateur Java pour récupérer le `.msi` et les fichiers qui l'accompagnent. Cette manipulation doit être effectuée sur un poste Vista ou supérieur.

Lancer manuellement l'installateur `jre-7uX-windows-XXX.exe` (en double-cliquant dessus).

Une fois que la fenêtre de l'installateur 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.

7.3.6. Quelques références

Documentation écrite par la DANE de l'académie de Lyon

WPKG sur un environnement Scribe

http://www2.ac-lyon.fr/serv_ress/mission_tice/wiki/doku.php?id=scribe:wpkg

Documentation écrite par l'académie de la Réunion

WPKG - Généralités

<http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:1.principe&ticket=>

WPKG - Installation sur un serveur Scribe

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:2.installation_sur_scribe&ticke

Wpkg-Manage : interface de gestion des packages à installer

http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:3.wpkg_manage

WPKG - Mise à jour des XML et installeurs

<http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:4.maj>

WPKG - Tests

<http://tice974.ac-reunion.fr/wiki-administrateurs/doku.php?id=scribe:wpkg:5.tests>

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

8. 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.

The screenshot shows the 'Proftpd' configuration window with a 'Configuration' tab. It contains a list of settings, each with a red 'E' icon, a gear icon, and an edit icon:

| Paramètre | Valeur |
|--|--------------|
| Nom du serveur FTP | [Champ vide] |
| Activer le chiffrement TLS | * non |
| Activer l'accès anonyme | * non |
| Activer des accès FTP supplémentaires | * non |
| Autoriser CAS en accès FTP | * oui |
| Utiliser le fichier '/etc/ftpusers' pour interdire l'accès FTP à des comptes utilisateur | * non |
| Nombre maximum d'utilisateurs simultanés | * 50 |
| Nombre maximum de processus pour ProFTPD | * 40 |
| Taille maximum du fichier récupéré (download) en Mb | * 500 |
| Taille maximum du fichier déposé (upload) en Mb | * 100 |
| Temps maximum d'inactivité avant déconnexion (en secondes) | * 1200 |

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.

| | |
|---------------------------------------|-------------|
| E Activer l'accès anonyme | * oui |
| E Chemin du répertoire anonyme | * /home/ftp |

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.

| | |
|--|---------------------------|
| E Activer des accès FTP supplémentaires | * oui |
| E Chemin du répertoire FTP supplémentaire | * /home/commun /home/data |

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.

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 Ajaxplorer 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.

9. Les applications web sur le module Horus

Le module Horus supporte nativement certaines applications web dont la plupart sont le résultat de la mutualisation inter-académique Envole^[p.363].

Elles sont adaptées pour fonctionner avec un serveur d'authentification unique. Grâce à cette méthode d'authentification unique, les utilisateurs du module Horus se connectent une seule fois pour accéder à l'ensemble des applications. Des rôles sont prédéfinis dans chacune d'elles. Il est possible dans certaines, de modifier les rôles prédéfinis pour l'utilisateur.

Le paramétrage du module Amon permet de rendre ces services web accessibles depuis l'extérieur de l'établissement.

Par défaut, **aucune application par défaut n'est définie** sur le module Horus.

Il est possible de modifier ce comportement en activant le serveur web Apache, dans l'interface de configuration du module, dans l'onglet Services, il faut passer la variable Activer le serveur web Apache à oui. L'onglet Applications web apparaît et propose entre autre d'activer l'application web phpMyAdmin. L'opération nécessite une reconfiguration du serveur avec la commande reconfigure.

Des applications web vous sont proposées dont certaines sont **pré-installées** et doivent être activées lors de la configuration du module.

D'autres sont **pré-packagées** et leur installation est laissée à votre initiative. Vous pouvez également ajouter vos propres applications.



La seule procédure valide pour mettre à jour les applications web d'un module EOLE est la procédure proposée par EOLE.

En aucun cas vous ne devez les mettre à jour par les moyens qui sont proposées via le navigateur.

Vous risquez d'endommager vos applications web et d'exposer votre module à des failles de sécurité.

9.1. L'authentification unique avec EoleSSO

L'authentification unique

EOLE propose un mécanisme d'authentification unique par l'intermédiaire d'un serveur SSO^[p.370].

Ce serveur est compatible CAS^[p.361], SAML^[p.369] et OpenID^[p.367].

L'utilisation d'un serveur SSO permet de centraliser l'authentification. En s'authentifiant auprès du serveur SSO, les utilisateurs peuvent se connecter aux différentes applications web sans avoir à se ré-identifier sur chacune d'elles.

Configuration

Dans l'interface de configuration du module, vous pouvez activer le serveur SSO du module ou utiliser un serveur SSO distant dans l'onglet **Services** → Utiliser un serveur EoleSSO

Vous devez ensuite renseigner les paramètres du serveur dont l'adresse IP et le port dans l'onglet **Eole sso** apparu après l'activation du service.

Cette opération nécessite la reconfiguration du module par la commande **reconfigure**.

Comptes utilisateurs pris en compte par le serveur SSO

Le serveur SSO installé sur les modules EOLE peut utiliser plusieurs annuaires LDAP.

Connexion

Une connexion vers une application (http://<adresse_serveur>/application/) redirige le navigateur vers le serveur SSO (https://<adresse_serveur>:8443/) afin d'effectuer l'authentification via un formulaire appelé mire SSO :



Formulaire d'authentification SSO

Lorsque le serveur SSO valide le couple identifiant / mot de passe de l'utilisateur, il délivre au navigateur un *jeton* sous forme de cookie et le redirige vers l'application (https://<adresse_serveur>/application/).

L'application reconnaît le jeton et autorise l'accès à l'utilisateur.

Remarque

Le navigateur doit être configuré pour **accepter les cookies**.

9.2. Applications pré-installées

Il est possible d'ajouter au module Horus des applications web pré-installées.

Il y a 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.

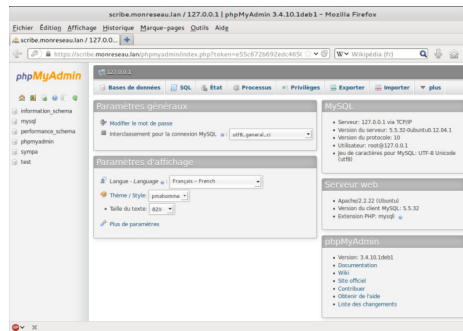
Reconfiguration du module

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**.

9.2.1. phpMyAdmin : gestionnaire de base de données MySQL

Présentation



Vue générale dans phpMyAdmin

phpMyAdmin est une application de gestion de base de données MySQL.

Cette interface pratique permet d'exécuter, très facilement et sans grandes connaissances dans le domaine des bases de données, de nombreuses requêtes comme les créations de table de données, les insertions, les mises à jour, les suppressions, les modifications de structure de la base de données.

<http://www.phpmyadmin.net>

Installation

Cette application est pré-installée sur les modules Scribe, Horus, Seshat ainsi que sur AmonEcole et toutes ses variantes.



Pour désactiver rapidement et temporairement (jusqu'au prochain reconfigure) l'application web il est possible d'utiliser la commande suivante :

```
# a2dissite nom de l'application
```

Le nom de l'application à mettre dans la commande est celui que l'on trouve dans le répertoire `/etc/apache2/sites-available/`

Pour activer cette nouvelle configuration il faut recharger la configuration d'Apache avec la commande :

```
# service apache2 reload
```

Pour réactiver l'application avec cette méthode il faut utiliser les commandes suivantes :

```
# a2ensite nom de l'application
```

```
# service apache2 reload
```

Pour désactiver l'application pour une période plus longue voir définitivement, il faut désactiver l'application depuis l'interface de configuration du module, dans l'onglet `Applications web`.

L'opération nécessite une reconfiguration du module avec la commande `reconfigure`.

Accéder à l'application

Pour accéder à l'application, se rendre à l'adresse : `https://<adresse_serveur>/phpmyadmin/` (ou `https://<adresse_serveur>/myadmin/`).

L'utilisateur peut être l'utilisateur `root` de MySQL ou un utilisateur de la base.



L'accès à l'application ne peut se faire que depuis une adresse IP autorisée dans l'interface de configuration du module (Onglet `Interface-n`, sous-menu `Administration distante sur l'interface`, mettre `Autoriser les connexions pour administrer le serveur` à `oui`, remplir le champ `Adresse IP réseau autorisé` avec l'adresse IP ou la plage d'adresses IP souhaitée).

Rôles de utilisateurs

Les utilisateurs autorisés à se connecter sont **les utilisateurs de MySQL**.

Il est possible de déléguer tout ou une partie des droits d'administration.

Remarques

Le mot de passe root de MySQL est réinitialisé avec une chaîne de caractères aléatoires à chaque reconfiguration du serveur.

Le mot de passe de l'utilisateur `root` de MySQL peut être réinitialisé avec la commande :

```
mysql_pwd.py
```



Si vous prévoyez d'utiliser régulièrement phpMyAdmin, il est préférable de créer un utilisateur MySQL dédié pour l'administration des bases de données.

Celui-ci ne sera pas écrasé après une reconfiguration du module.

9.3. Prise en charge d'applications supplémentaires

Les modules Scribe, Horus, Seshat et AmonEcole fournissent tous les éléments nécessaires à l'installation d'applications web indépendamment de celles pré-configurées.

Les exemples sont basés sur l'installation du logiciel EGroupware mais sont facilement transposables pour l'installation de n'importe quelle application PHP/MySQL.

EGroupware est un logiciel collaboratif professionnel. Il vous permet de gérer vos contacts, vos rendez-vous, vos tâches, et bien plus pour toute votre activité.

<http://www.egroupware.org/>



Mode conteneur

L'installation d'applications sur les modules configurés en mode conteneur est plus complexe.

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.

9.3.1. Téléchargement et mise en place

Installation des fichiers

Pour télécharger une archive sur le module, il faut utiliser la commande `wget` :

```
# wget https://www.sourceforge.net/project/egroupware/eGroupware-14.2/eGroupware-14.2
```

Il faut ensuite décompresser l'archive à l'aide de la commande `tar` (ou `unzip`, pour le format zip) :

```
# tar xzvf egroupware-epl-14.2.20150310.tar.bz2
```

Dans cet exemple, cela créera le répertoire `egroupware`

Ensuite, il faut envoyer les fichiers dans le répertoire de destination, soit :

- sur les modules Scribe ou Horus :

```
# cp -r egroupware /var/www/html/egroupware
```

- sur un module Horus dépourvu d'application web :

```
# mkdir /var/www/html
```

```
# cp -r egroupware /var/www/html/egroupware
```

- sur le module AmonEcole :

```
# cp -r egroupware /opt/lxc/reseau/rootfs/var/www/html/egroupware
```

Affectation de droits

La plupart des applications nécessitent que l'utilisateur utilisé par le service Apache (ici, l'utilisateur système : `www-data`) ait le droit d'écrire en certains endroits du disque.

Le propriétaire d'un fichier ou d'un répertoire se modifie à l'aide de la commande `chown` :

- sur les modules Scribe/Horus :

```
# chown -R www-data: /var/www/html/egroupware
```

```
# chmod 770 /var/www/html/egroupware (le temps de l'installation)
```

- sur le module AmonEcole :

```
# ssh reseau
```

```
# chown -R www-data: /var/www/html/egroupware
```

```
# chmod 770 /var/www/html/egroupware (le temps de l'installation)
```

```
# ctrl + d pour sortir du conteneur
```



Donner trop de droits à l'utilisateur `www-data` diminue la sécurité du serveur.

Consulter la documentation du logiciel pour n'attribuer que les droits nécessaires au fonctionnement de l'application.

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 :

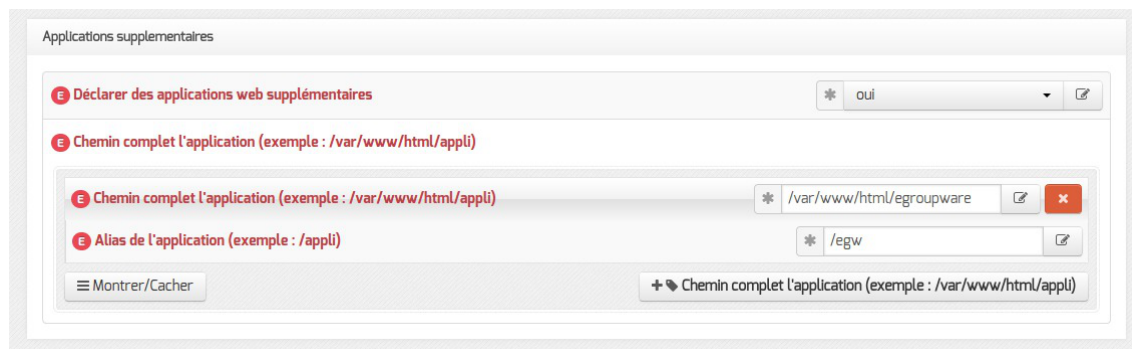
```
# apt-eole install-conteneur web php5-imap
```
- Installation manuelle de paquets (cf. Installation manuelle de paquets)

9.3.2. Configuration Apache

Méthode Creole

Dans l'interface de configuration du module :

- aller dans l'onglet `Apache` en mode expert ;
- indiquer le chemin complet de l'application et l'alias de l'application `/var/www/html/egroupware` ;
- indiquer le chemin de l'alias de l'application `/egw` ;



Déclaration d'une application web dans gen_config

- enregistrer la configuration et quitter ;
- lancer la commande `reconfigure` ;
- le logiciel doit répondre à l'adresse : `http://<adresse_serveur>/egw`



La 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-enabled/egroupware`

- sur le module AmonEcole : `/opt/lxc/reseau/rootfs/etc/apache2/sites-enabled/egroupware`

```
# 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 :

```
# a2ensite egroupware
```

- recharger la configuration d'Apache à l'aide de la commande `CreoleService`^[p.362] :

```
# CreoleService apache2 reload
```

- le logiciel doit répondre à l'adresse : `http://<adresse_serveur>/egw`

Pour obtenir une configuration apache optimale, consulter la documentation de l'application.

En cas de problème, consulter le fichier de journal `/var/log/rsyslog/local/apache2/apache2.err.log`

Dans le cas d'EGroupware, il est nécessaire de supprimer le fichier `.htaccess` situé dans le répertoire racine du logiciel :

```
# rm -f /var/www/html/egroupware/.htaccess
```

La directive `php_admin_flag allow_url_fopen On` est également nécessaire au bon fonctionnement d'EGroupware.

9.3.3. Configuration MySQL

Méthode EOLE

Utiliser le script `mysql_add.py` :

```
Nom de la base de données à créer : egroupware
```

```
Nom de l'utilisateur MySQL administrant la base : egroupware
```

```
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`.

9.3.4. Configuration du logiciel

Vous pouvez maintenant utiliser le système automatique d'installation du logiciel disponible à l'adresse :

`http://<adresse_serveur>/egw`

Un `/install` ou `/config` sera à ajouter au chemin en fonction de l'application à installer.



Sur le module AmonEcole, l'adresse de la base de données à mettre dans l'interface de configuration de l'application est celle du conteneur `bdd` (`192.0.2.50`) et non `localhost`.

Affectation de droits après l'utilisation du système automatique d'installation du logiciel

Changer les droits d'accès :

```
# chmod 750 /var/www/html/egroupware
```

Changer le propriétaire des fichiers :

```
# chown -R root :www-data /var/www/html/egroupware
```

Authentification CAS

Informations utiles à la configuration d'une authentification CAS :

- adresse du serveur CAS : adresse IP (ou nom DNS) de votre module EOLE
- 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.361] 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 ^[p.337]

Définition de filtres d'attributs

10. Réplication LDAP

Avec le module Scribe ou le module Horus, il est possible de mettre en place rapidement une réplication d'annuaire LDAP vers un module Seshat.

La réplication utilise le mécanisme *syncrepl* (LDAP Sync Replication engine).

Syncrepl est plus robuste que son prédécesseur *slurpd* et permet de mettre en place des architectures beaucoup plus complexes.

La configuration actuelle permet au **client** (serveur Seshat) de venir recopier les informations de son **fournisseur** (serveur Scribe ou Horus).



Il est déconseillé de répliquer des serveurs Scribe et des serveurs Horus sur le même client Seshat.

Pré-requis

Serveur Scribe ou Horus

Pour configurer le fournisseur il faut adapter les informations dans l'interface de configuration du module en mode expert dans l'onglet `Openldap`.

- la réplication LDAP du côté fournisseur doit être activée

- par défaut, les communications LDAP ne sont pas chiffrées. Pour mettre en place une communication chiffrée entre le fournisseur et le client, il faut passer la variable `Activer LDAP sur le port SSL` à `oui` ou à `uniquement`.



Selon la configuration mise en place le port 389 et/ou le port 636 doivent être ouverts :

- du serveur Seshat vers le serveur Scribe ou Horus ;
- si possible dans le sens inverse.

Mise en place

Génération du fichier de configuration

Sur le module Scribe ou Horus, exécuter la commande `active_replication.py`.

Cette commande permet de générer dans `/root/` le fichier de configuration propre au serveur nommé : `replication-<numero_etab>.conf`.

La commande permet de paramétrer plusieurs éléments :

- `Répliquer également les groupes` : si la réponse est laissée à `non`, seuls les comptes utilisateurs seront répliqués.

Certains connecteurs EoleSSO disponibles sur le module Seshat nécessitent de répliquer les groupes en plus des utilisateurs ;

- `Ajouter des uid à exclure de la réplication` : en répondant `oui` à cette question, il est possible de saisir une liste de comptes à ne pas répliquer (administrateur locaux, comptes réservés, ...).

Par défaut seul le compte `admin` n'est pas répliqué ;

- `Adresse utilisée pour accéder au module depuis le client` : adresse IP ou nom de domaine que le client de réplication devra utiliser pour interroger l'annuaire du module. L'adresse proposée par défaut est celle de l'interface eth0 du module mais cette valeur dépend de l'architecture réseau mise en place et notamment de la configuration des pare-feu présents entre le module EOLE et le client de réplication ;
- Selon la configuration du serveur OpenLDAP du module, le choix du protocole à utiliser pour la réplication peut être proposé. Si à la question `Utiliser le protocole ldaps (port 636) pour la réplication` la réponse est laissée à `oui`, la réplication utilisera le protocole LDAPS sinon elle utilisera le protocole LDAP.

Mise en place manuelle

Il faut copier le fichier `/root/replication-<numero_etab>.conf` du fournisseur dans le dossier `/etc/ldap/replication` du serveur Seshat.

Puis, sur le module Seshat, il faut exécuter la commande `gen_replication.py`.

Mise en place via Zéphir

Si le serveur fournisseur (Scribe ou Horus) et le serveur Seshat sont enregistrés sur le même serveur Zéphir, celui-ci peut se charger de la mise en place de la configuration sur le serveur Seshat.

La connexion à Zéphir est proposée automatiquement en fin d'exécution du script :

```
Veillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :
```



Il est impératif de connaître l'identifiant Zéphir du serveur Seshat pour finaliser la transaction.

```
Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :
```

Les configurations de réplication envoyées via Zéphir sont consultables dans l'application web Zéphir en utilisant le lien [configurations de réplication LDAP](#) disponible sur la page décrivant l'état du serveur Seshat.

Configurations de réplication LDAP - seshat aca (225)

Fichier(s) de configuration des annuaires à répliquer

| | |
|---------------------------|--------------------------------------|
| replication-0000000A.conf | Supprimer ce fichier |
| replication-0000000M.conf | Supprimer ce fichier |
| replication-0000000N.conf | Supprimer ce fichier |

[Retour à la page d'état du serveur](#)

Consultation des configurations de réplications LDAP dans l'application Zéphir



Les configurations envoyées via Zéphir sont stockées dans le répertoire `/etc/ldap/replication/zephir` du serveur Seshat.

Suivi et débogage



Pour obtenir des informations concernant la réplication, il faut paramétrer slapd avec le *log level* 16384.

Cela se traduit par la ligne de commande suivante :

```
slapd -f /etc/ldap/slapd.conf -u openldap -g openldap -d 16384
```

Attention, ce mode peut être très verbeux.

Chapitre 7

Compléments techniques

Cette partie de la documentation regroupe différentes informations complémentaires : des schémas, des informations sur les services, les ports utilisés sur chacun des modules...

1. Les services utilisés sur le module Horus

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complètement 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 d'entre-eux conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `annuaire (id=10)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.2. eole-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)`.

1.3. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.



Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro

<http://dev-eole.ac-dijon.fr/projects/eole-antivir>

<http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf>

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon et clamav-freshclam.

<http://www.clamav.net/>

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirus (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

```
1 <container name='xxx'>
2   <package>eole-antivirus-pkg</package>
3   <service>clamav-daemon</service>
4   <file filelist='clamav' name='/etc/clamav/clamd.conf' />
5 </container>
```

1.4. 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/downloads/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 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.

1.5. eole-fichier-primaire

Le paquet `eole-fichier-primaire` permet la mise en place d'un serveur de fichiers complet.

Logiciels et services

Le paquet `eole-fichier-primaire` permet de gérer les services suivants :

- `smbd`, `nmbd` et `Scannedonly`^[p.369] (serveur de fichiers) ;
- `nscd` (cache).

<http://www.samba.org/>

Historique

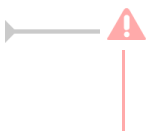
Les services fournis sont spécifiques aux modules Horus et Scribe.

Grâce au paquet `eole-fichier-primaire`, la configuration de base est identique sur les deux modules bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)`.

Sur 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`).

1.6. eole-cups

Le paquet `eole-cups` permet la mise en place d'un serveur d'impressions.

Logiciels et services

Le paquet `eole-cups` permet de gérer le service cups (serveur d'impressions).

<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`).

1.7. 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`).

1.8. eole-mysql

Le paquet `eole-mysql` permet la mise en place d'un serveur de bases 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)`.

1.9. eole-web

Le paquet `eole-web` permet la mise en place d'un serveur web.



L'installation d'`eole-web` entraîne celle d'`eole-mysql`.

Logiciels et services

Le paquet `eole-web` s'appuie principalement sur le service `apache2`.

<http://httpd.apache.org/>

Il permet également d'activer l'application `phpMyAdmin`.

<http://www.phpmyadmin.net/>

Historique

À la base uniquement disponible sur les modules Scribe/AmonEcole, le paquet `eole-web` est désormais installable sur n'importe quel module EOLE.

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.

1.10. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de bases de données Interbase^[p.366].

Logiciels et services

Le paquet `eole-interbase` s'appuie principalement sur le service `xinetd`.

Historique

Historiquement ce service est uniquement utilisé sur le module Horus.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `interbase (id=16)`.

Sur les modules Horus/AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

2. Ports utilisés sur le module Horus

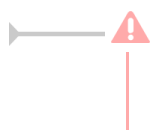
Le module Horus propose de nombreux services.

Ce document donne la liste exhaustive des ports utilisés sur un module Horus standard.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.

Il est possible de lister les ports ouverts sur le serveur par la commande :

```
netstat -ntulp
```



En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 68/udp : dhclient
- 123/udp : ntpd
- 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)
- 8443/tcp : EoleSSO

Ports spécifiques au module Horus

- 21/tcp : ftp (ProFTPD)
- 67/udp : dhcp
- 69/udp : tftp
- 80/tcp : http (Apache2)
- 137/udp : nmbd
- 138/udp : nmbd
- 139/tcp : samba (netbios)
- 389/tcp : ldap (OpenLDAP)
- 443/tcp : https (Apache2)
- 445/tcp : samba (sans netbios)
- 631/tcp+udp : CUPS
- 636/tcp : ldaps (OpenLDAP sur le port SSL)
- 3050/tcp : Xinetd (Interbase)
- 3306/tcp : MySQL
- 7080/tcp : horus_frontend
- 9101/tcp : bacula-director
- 9102/tcp : bacula-filedemon
- 9103/tcp : bacula-storagedemon

Services et numéro de ports

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

3. L'annuaire LDAP du module Horus

L'annuaire LDAP^[p.366] du module Horus est basé sur le logiciel OpenLDAP (version 2.4).

Il est la pièce maîtresse du module puisqu'il est utilisé par quasiment tous les logiciels intégrés sur Horus.

Il fournit les services suivants :

- authentification utilisateur ;
- comptes Samba ;

- définition des groupes et des partages.

Horus utilise l'annuaire LDAP pour stocker la liste des utilisateurs et des groupes ainsi que leurs paramètres. Cet annuaire est initialisé avec un utilisateur et plusieurs groupes spéciaux :

- l'utilisateur dédié à toutes les tâches d'administrations :
 - `admin` (membre du groupe `DomainAdmins`)
- les groupes dédiés à l'environnement Windows :
 - `DomainAdmins`
 - `DomainUsers`
 - `DomainComputers`
 - `PrintOperators`
- les groupes propres à Horus :
 - `minedu`
 - `applidos`

Le groupe `DomainAdmins` correspond au groupe `Administrateurs du domaine`. Les membres de ce groupe sont `Administrateur` des postes Windows et bénéficient d'un **accès en lecture/écriture sur l'ensemble des partages** du module Scribe.

Le groupe `DomainUsers` correspond au groupe `Utilisateurs du domaine`. Il s'agit des utilisateurs standards n'ayant pas de privilèges particuliers.

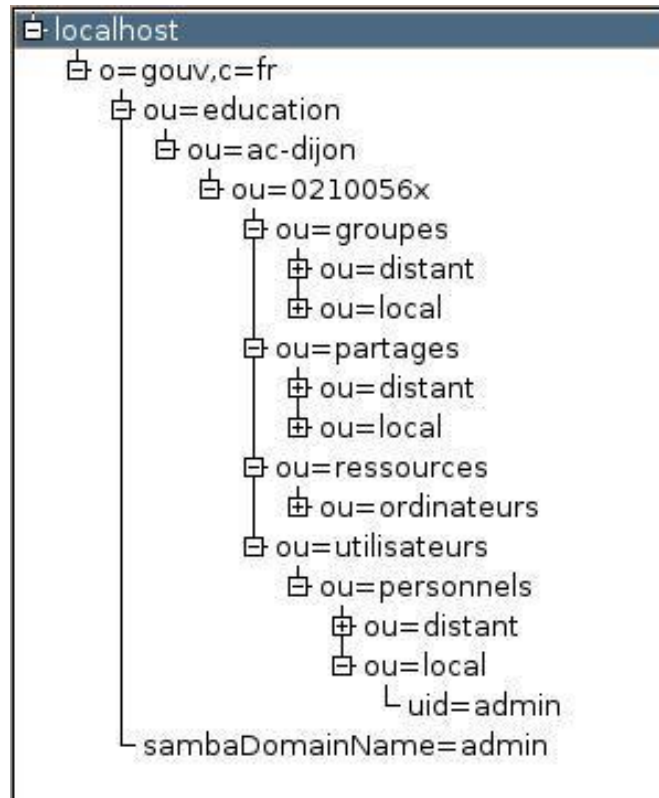
Le groupe `DomainComputers` est le groupe principal pour les stations intégrées au domaine.

Le groupe `PrintOperators` correspond au groupe `Administrateurs des imprimantes`.

Les groupes `minedu` et `applidos` sont des groupes propres à Horus permettant d'appliquer des méthodes de gestion spécifiques.

3.1. Arborescence de l'annuaire

L'arborescence LDAP (Lightweight Directory Access Protocol) du module Horus utilise le **nom de l'académie** et le **numéro de l'établissement** pour offrir à chaque établissement des branches personnalisées.



Arborescence de l'annuaire LDAP d'Horus

3.2. Utilisateurs spéciaux

Le compte d'administration

L'administrateur LDAP^[p.366] de l'application (*rootdn*) est l'utilisateur spécial :

cn=admin,o=gouv,c=fr

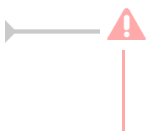
Pour des raisons pratiques et de sécurité, le mot de passe de cet utilisateur est changé régulièrement (mise à jour et reconfiguration du module).

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 du script :

`/usr/share/eole/annuaire/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 leur permettent d'accéder aux attributs LDAP protégés par des ACL^[p.361]. Ces attributs ne sont pas accessibles par des requêtes anonymes et l'utilisation d'un

compte en lecture seule permet de préserver la sécurité de l'annuaire.

Pour faciliter la mise en œuvre d'applications distantes, le mot de passe de cet utilisateur n'est jamais modifié après avoir été généré.

Le mot de passe de cet utilisateur est stocké dans le fichier `/root/.reader`



La validité du mot de passe de l'utilisateur `reader` peut être testée avec la commande suivante :

```
ldapsearch -x -D cn=reader,o=gouv,c=fr -w `cat /root/.reader` uid=admin uid
```

3.3. Entrée ordinateur du domaine

Lors de la jonction au domaine d'ordinateur (pour les versions supérieures ou égales à Windows 2000), un compte de machine est créé dans l'annuaire. Ces comptes sont stockés dans la branche :

```
ou=ordinateurs,ou=ressources,ou=numero_etab,ou=nom_academie,ou=education,o=
```

Classes d'objet

Les ordinateurs héritent des classes d'objet suivantes :

- posixAccount (`nis.schema`)
- sambaSAMAccount (`samba.schema`)
- account (`cosine.schema`)

Attributs

Dans certains cas (formatage ou renouvellement d'une station), il peut être nécessaire de supprimer l'ordinateur de l'annuaire.

Les attributs spécifiques aux machines sont les suivants :

- uid : identifiant, c'est le nom de la machine suivi du caractère \$
- cn : nom de la machine (généralement identique à l'uid)

3.4. Entrée partage

Les partages de l'établissement sont placés dans la branche :

```
ou=local,ou=partages,ou=numero_etab,ou=nom_academie,ou=education,o=gouv,c=fr
```

Classes d'objet

Les partages héritent des classes d'objet suivantes :

- sambaFileShare (`eoleshare.schema`)

Attributs

Les attributs spécifiques aux partages sont les suivants :

- `cn` : chemin samba du partage (`smb://serveur_samba/partage`)
- `sambaShareName` : nom du partage
- `sambaShareGroup` : groupe associé au partage, par convention sur Scribe un partage est toujours associé au groupe du même nom
- `sambaFilePath` : chemin Unix du partage (`/home/workgroups/partage`)
- `sambaShareURI` : URI du partage (`\\serveur_samba\partage`)
- `sambaShareModel` : modèle de partage Samba à utiliser pour déclarer le partage
- `sambaShareDrive` : lettre de lecteur associée au partage (facultatif)
- `sambaShareOptions` : options spécifiques (exemple : *sticky bit* sur les partages Horus, facultatif)

4. La gestion du SID

Le SID est un identifiant de sécurité utilisé pour identifier les ressources et les personnes sur un réseau Microsoft.

Le SID d'un domaine se présente sous la forme `S-1-5-21-nnnnnnnnnn-nnnnnnnnnn-nnnnnnnnnn`

Chaque serveur de fichier 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.369] 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.366] 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 : $2 \times \text{uidNumber} + 1000$

—  | 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
```

Chapitre 8

Questions fréquentes

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



1. Questions fréquentes communes aux modules

CAS Authentication failed !

Le message `CAS Authentication failed ! You were not authenticated.` (ou `Authentification CAS infructueuse ! Vous n'avez pas été authentifié(e).`) peut apparaître si des modifications ont été faites dans l'interface de configuration.

—💡 **Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module**

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
# /usr/share/creole/gen_certif.py -f ou #
/usr/share/creole/gen_certif.py -f nom du certificat pour la régénération
d'un certificat en particulier.
# reconfigure
```

Vous avez ajouté un nom DNS alternatif ou une adresse IP alternative sur le serveur

Il faut ajouter le nom alternatif ou l'adresse IP alternative dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet **Certifs-ssl** en mode expert il faut remplir les champs **Nom DNS alternatif du serveur** et/ou l'adresse **IP alternative du serveur**.

Le bouton **+** permet d'ajouter autant d'alternatives que vous voulez. Il faut ensuite **Valider le groupe** et enregistrer la configuration.

L'opération doit être suivie de la reconfiguration du module, cela va régénérer le certificat **/etc/ssl/certs/eole.crt**

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande **gen_certif.py** avec l'option **-f** pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

```
# /usr/share/creole/gen_certif.py -f ou #
/usr/share/creole/gen_certif.py -f nom du certificat pour la régénération
d'un certificat en particulier.
```

```
# reconfigure
```

Attention, les adresses suivantes ne sont pas définies comme sujet du certificat...

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

```
# /usr/share/creole/gen_certif.py -f ou #  
/usr/share/creole/gen_certif.py -f nom_du_certificat
```

pour la régénération d'un certificat en particulier.

```
# reconfigure
```



Consulter la documentation dédiée aux certificats. (cf. Gestion des certificats SSL)

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 réseaux

Cette erreur provient certainement du masque des variables d'autorisation d'accès à SSH sur l'une des interfaces réseaux.

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 **Systeme / Mise à jour** de l'EAD.

► Dans un terminal

```
python -c "from creole import maj; print maj.get_maj_day()"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un terminal.

► Via l'EAD

Pour l'afficher il faut se rendre dans la section **Systeme / 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.

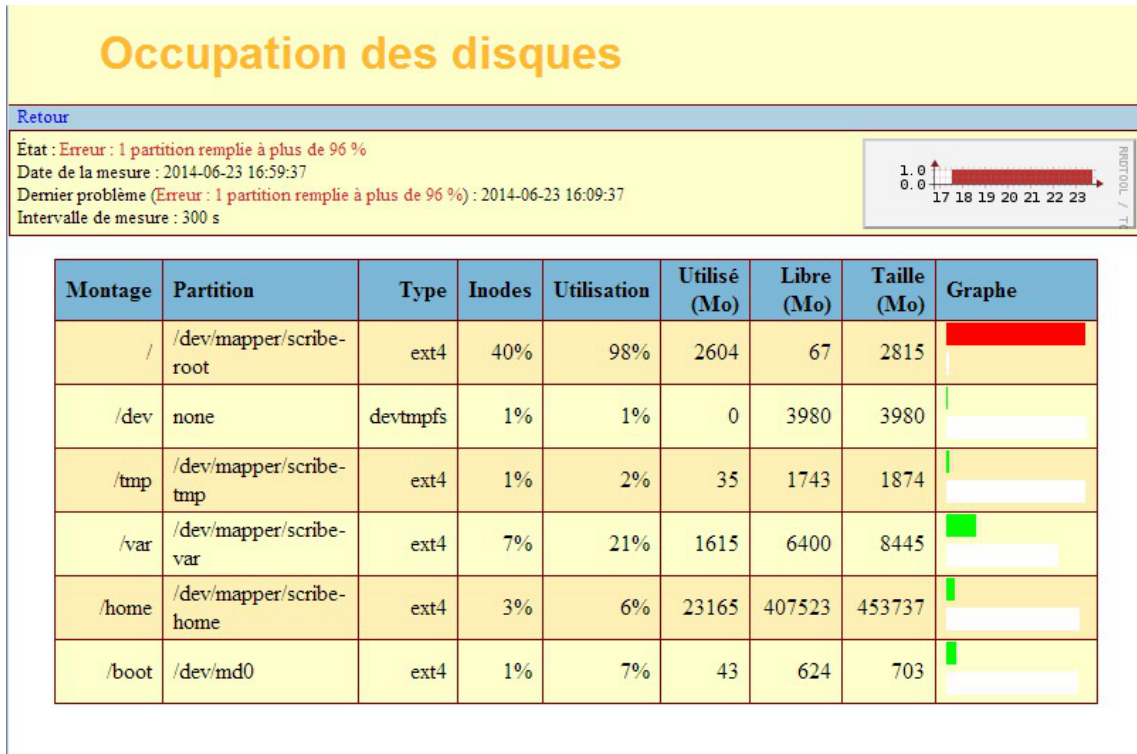
(Code d'erreur : sec error reused issuer and serial)

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

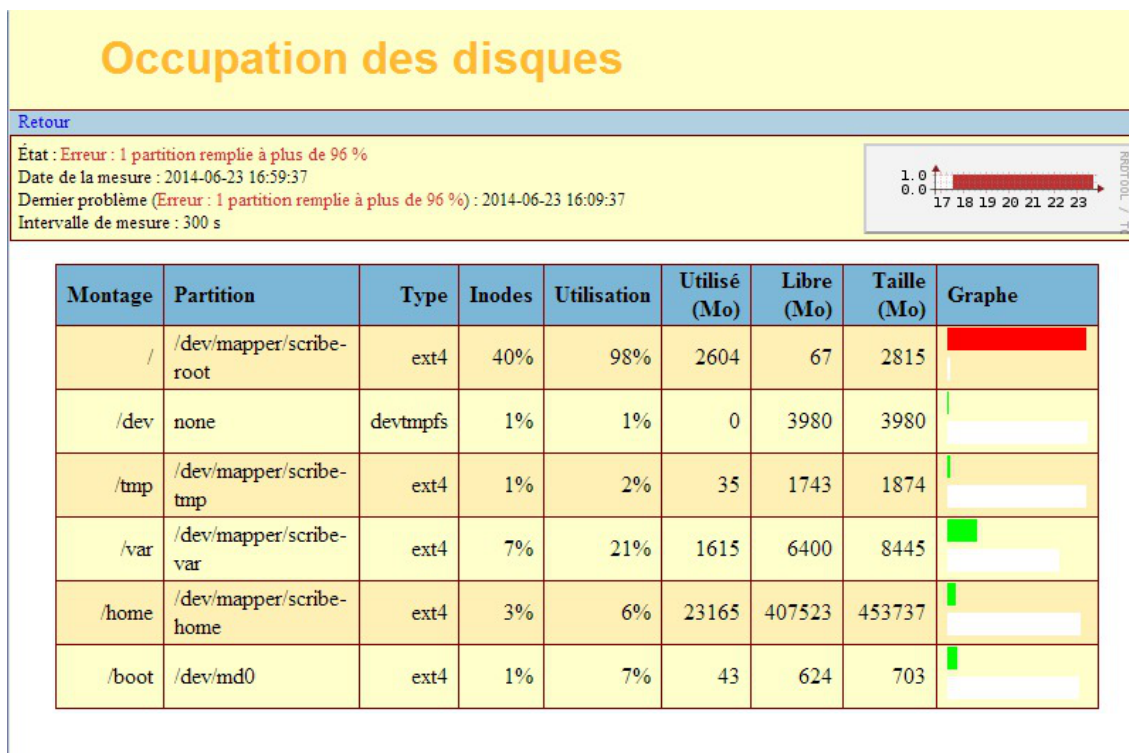


Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- 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



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 de la sauvegarde bacula par exemple.



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 :

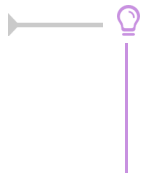
```
root@scribe:/# du -h --max-depth=1 /media /mnt/
4,0K /media 4,0K /mnt/
```



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).

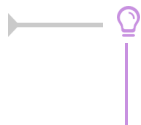
Partition `/var` saturée

Cette partition contient entre autres les journaux systèmes du serveur.

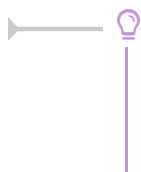


La commande suivante affiche l'espace occupé par chaque répertoire et les classe par taille, le plus grand nombre en dernier (sans tenir compte de l'unité) :

```
# du -smh /var/* | sort -n
```



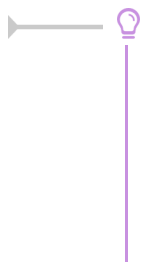
Un service mal configuré génère une quantité importante de journaux. Si le problème n'est pas résolu la partition va de-nouveau saturer.



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. 366]).

Partition /var saturée en inode

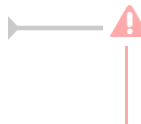
Un nombre important de fichier peut être du à un service mal configuré mais peut aussi être du à un fonctionnement normal. Il faut identifier le répertoire dans lequel il y a le plus de fichier.



La commande suivante affiche le nombre de fichiers par répertoire et les classe par taille, le plus grand nombre en dernier :

```
# for i in $(find /var -type d); do f=$(ls -A $i | wc -l); echo "$f : $i"; done | sort -n
```

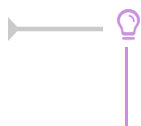
Selon les circonstances il faudra soit supprimer des fichiers soit agrandir la partition.



La suppression de fichier ne doit pas être effectué sans connaissances solides du système d'exploitation.

Liste d'arguments trop longue

La commande `# rm -rf /var/<rep>/*` renvoie `Liste d'arguments trop longue`.

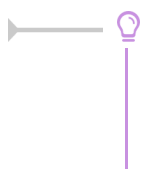


Préférez l'utilisation d'une autre commande :

```
# find /var/<rep>/* -type f -name "*" -print0 | xargs -0 rm
```

Le démarrage reste figé à l'étape de vérification des disques

Le serveur est virtualisé avec une solution basée sur l'émulateur qemu.



Seul l'affichage est figé, la machine démarre en fait normalement et est certainement accessible par SSH. Cela vient du support de la carte graphique. Il faut forcer la carte graphique à utiliser une autre carte graphique que celle par défaut (cirrus).

Sous Proxmox, indiquez carte `VGA_standard` à la place de `par_défaut`.

Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.



Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :

1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet `Eoleflask`.
2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.

Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

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

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.



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

À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.

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

Impossible de trouver la base des matériels maintenue par EOLE

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

Changer le disque dur du serveur

Il est possible entre autre de faire une image avec le logiciel Clonezilla.



L'UUID^[p.372] 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 http://scenari-platform.org/deb precise main
```

Il faut ensuite mettre la liste des paquets disponibles à jour avec la commande `apt-get update`.

Dysfonctionnement des agents suite à un changement d'architecture

En allant sur la page des statistiques de surveillance d'un serveur (EAD ou Application Zéphir), j'obtiens un message du type `rrdtool.error: This RRD was created on another architecture`

Ce problème peut survenir en cas de réinstallation des données d'un serveur 32 bits sur un serveur 64 bits (ou inversement).



Une solution consiste à supprimer les fichiers de statistiques :

- Statistiques propres au serveur Zéphir

Concerne les statistiques de Zéphir lui-même, pour les statistiques des serveurs clients, l'erreur doit être corrigée sur le client (voir cas suivant).

```
# service zephir stop
# rm -rf /var/lib/zephir/data/0/*
# service zephir start
```

- Sur un module EOLE autre que Zéphir

```
# service z_stats stop
# rm -rf /usr/share/zephir/monitor/data/*
# rm -rf /usr/share/zephir/monitor/stats/*
# service z_stats start
```



Si perdre les statistiques pose problème, il est possible de convertir les fichiers `.rrd` avec l'outil `rrdtool`.

Depuis l'ancien serveur, pour convertir les fichiers RRD vers des fichiers XML avec la commande `dump` :

```
# rrdtool dump stats.rrd > stats.xml
```

Après les avoir transférés sur le nouveau serveur il faut les convertir en RRD avec la commande `restore` :

```
# rrdtool restore -f stats.xml stats.rrd
```

Le serveur peut maintenant lire le fichier. Vous pouvez le tester avec la commande `info` :

```
# rrdtool info stats.rrd
```

Attention, il y a un (ou plusieurs) fichier par agent.

Exemple sur un serveur Zéphir :

```
root@zephir:~# ls -l /var/lib/zephir/data/0/*/*.rrd -rw-r--r-- 1
root root 11464 août 31 14:51
/var/lib/zephir/data/0/bastion/status.rrd -rw-r--r-- 1 root root
17032 août 31 15:27 /var/lib/zephir/data/0/bilan/status.rrd
-rw-r--r-- 1 root root 13576 août 31 15:26
/var/lib/zephir/data/0/debsums/status.rrd -rw-r--r-- 1 root root
1000 août 31 14:51 /var/lib/zephir/data/0/diag/status.rrd
-rw-r--r-- 1 root root 13576 août 31 15:26
/var/lib/zephir/data/0/diskspace /status.rrd
[...]
```

Si vous voulez convertir un répertoire entier en XML, utilisez ce petit script bash :

```
# for f in *.rrd; do rrdtool dump ${f} > ${f}.xml; done
```

S o u r c e :

<http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite>

Comment débloquent 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.

2. Questions fréquentes propres au module Horus

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.

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 :

```
U P D A T E          u s e r          S E T
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
```

- 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 :

```
U P D A T E                               u s e r                               S E T
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
```

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:
```

```
#
```

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.

Comment effectuer un changement de nom de domaine académique

Le changement du nom de domaine académique entraîne un dysfonctionnement de l'annuaire LDAP car la construction de l'annuaire utilise cette valeur et n'a lieu qu'une fois au moment de l'instance.

Pour connaître le nom de domaine utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep -E 'dn: ou=[^,]+,ou=education'
```

Le nom utilisé ici est `ac-test` :

```
dn: ou=ac-test,ou=education,o=gouv,c=fr
```

Le nom de domaine `Nom de domaine académique` se change dans l'interface de configuration du module dans l'onglet `Général`.

Le suffixe peut être changé dans le même onglet à la ligne `Suffixe du nom de domaine académique`.

Pour connaître la valeur de ces variables en ligne de commande :

```
# CreoleGet nom_academie
ac-test
# CreoleGet suffixe_domaine_academie
fr
```

La solution consiste à extraire l'annuaire, à faire la modification souhaitée dans tous le `.ldif`, puis à injecter l'annuaire modifié.

Extraire l'annuaire :

Arrêt du service

```
# service slapd stop
```

Extraction vers `~root/full-ldap-old.ldif` :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no >
~root/full-ldap-old.ldif
```

Remplacer toutes les occurrences de `ou=ac-test` par `ou=ac-dijon` et toutes les occurrences de `ou : ac-test` par `ou : ac-dijon` avec la commande :

```
# sed -e 's/ou=ac-test,/ou=ac-dijon,/g' -e 's/ou:
ac-test,/ou=ac-dijon,/g' ~root/full-ldap-old.ldif >
~root/full-ldap-fixed.ldif
```

Vérifier l'absence (hors messagerie -i) de la chaîne `ac-test` dans le nouveau fichier :

```
# grep 'ac-test' ~root/full-ldap-fixed.ldif
```

Injection du nouvel annuaire avec les commandes suivantes :

- Supprimer les anciens fichiers d'annuaire, sauf le fichier `/var/lib/ldap/DB_CONFIG`

```
# rm -f /var/lib/ldap/[^D]*
```

- Injecter l'annuaire corrigé

```
# slapadd -f /etc/ldap/slapd.conf -l ~root/full-ldap-fixed.ldif
-##### 47.59% eta 04s elapsed 03s spd 307.1 k/s
Closing DB...
```

- Corriger le propriétaire des fichiers de la base de données

```
# chown -R openldap: /var/lib/ldap/
```

- Redémarrer l'annuaire

```
# service slapd start
```



Vérifier le bon fonctionnement du service avec la commande `diagnose`.

Comment effectuer un changement de nom du serveur de fichier

Le changement du nom du contrôleur de domaine et/ou du nom du domaine Samba entraîne un dysfonctionnement de l'annuaire LDAP car la construction de l'annuaire utilise cette valeur et n'a lieu qu'une fois au moment de l'instance.

Pour connaître le nom du domaine Samba utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep
"^sambaDomainName"
```

Le nom utilisé ici est `dompedago` :

```
sambaDomainName: dompedago
```

Pour connaître le nom du contrôleur de domaine utilisé dans l'annuaire :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no | grep -m1
'sambaShareURI'
```

Le nom utilisé ici est `scribe` :

```
sambaShareURI: \\scribe\icones$
```

Le nom du contrôleur de domaine et le nom du domaine Samba sont configurés dans l'interface de configuration du module dans l'onglet `Samba`.

Pour connaître la valeur de ces variables en ligne de commande :

```
# CreoleGet smb_netbios_name
```

```
scribe
```

```
# CreoleGet smb_workgroup
```

```
dompedago
```

La solution consiste à extraire l'annuaire, à faire la modification souhaitée dans tous le `.ldif`, puis à injecter l'annuaire modifié.

Extraire l'annuaire après arrêt du service :

Arrêt du service

```
# service slapd stop
```

Extraction vers `~root/full-ldap-old.ldif` :

```
# slapcat -f /etc/ldap/slapd.conf -o ldif-wrap=no >
~root/full-ldap-old.ldif
```

Remplacer toutes les occurrences de **scribe** par **nomnetbios** avec la commande :

```
# sed -e 's/scribe/nomnetbios/g' ~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'
~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-fixed.ldif
```

Injection du nouvel annuaire avec les commandes suivantes :

- Supprimer les anciens fichiers d'annuaire, sauf le fichier `/var/lib/ldap/DB_CONFIG`

```
# rm -f /var/lib/ldap/[^D]*
```

- Injecter l'annuaire corrigé

```
# slapadd -f /etc/ldap/slapd.conf -l ~root/full-ldap-fixed.ldif
-##### 47.59% eta 04s elapsed 03s spd 307.1 k/s
Closing DB...
```

- Corriger le propriétaire des fichiers de la base de données

```
# chown -R openldap: /var/lib/ldap/
```

- Redémarrer l'annuaire

```
# service slapd start
```

Vider le cache de Samba :

```
# net cache flush
```

Si cela ne suffit pas il faut supprimer les fichiers `/var/lib/samba/wins.dat` et

```
/var/cache/samba/browse.dat :  
# service samba stop  
# rm -f /var/lib/samba/wins.dat /var/cache/samba/browse.dat  
# service samba start
```



Vérifier le bon fonctionnement du service avec la commande `diagnose`.

3. Questions fréquentes propres à la sauvegarde

La sauvegarde programmée est en échec



Relancer les services

Il faut en premier lieu enlever le verrou :

```
# bareosconfig.py --unlock
```

Si tout n'est pas passé au vert dans l'EAD, il faut relancer les services :

```
# service bareos-dir stop
```

```
# service bareos-sd stop
```

```
# service bareos-fd stop
```

```
# service bareos-dir start
```

```
# service bareos-sd start
```

```
# service bareos-fd start
```

Modification de la configuration de Bareos non prise en compte

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

Afin de prendre en compte la nouvelle valeur, il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et ré-initialiser la base de données Bareos.



Ré-initialisation de la base Bareos

```
# bareosregen.sh
```

```
Le catalogue Bareos a déjà été initialisé, voulez-vous le  
réinitialiser ? [oui/non]
```

```
[non] : oui
```

Réinitialisation de la sauvegarde

Pour réinitialiser la sauvegarde il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et surtout il faut ré-initialiser la base de données de Bareos.

⚡ Ré-initialisation de la base Bareos

```
# bareosregen.sh
Le catalogue Bareos a déjà été initialisé, voulez-vous le
réinitialiser ? [oui/non]
[non] : oui
```

Supprimer le verrou de sauvegarde

⚡ Il faut utiliser la commande suivante :

```
# bareosconfig.py --unlock
```

Paramètres de la commande bareosconfig.py

⚡ Pour afficher la liste des paramètres de la commande `bareosconfig.py` :

```
# bareosconfig.py --help
```

Problème de droit sur le point de montage des sauvegardes

Il peut survenir un problème de droit sur le point de montage des sauvegardes dans les cas où la configuration du support choisie est `Configuration manuelle du support` ou sur `Disque USB local`.

👁

```
# bareosmount.py --mount
Échec du montage : point de montage : OK
montage : OK
permissions : Erreur
```

⚡ Appliquer les bons droits sur le point de montage

Tester la configuration du support et rendre l'utilisateur `bacula` et le groupe `tape` propriétaires du point de montage

```
# bareosmount.py -t -o
```

```
. Test OK .
```

Monter le support

```
# bareosmount.py --mount
```

```
Montage OK
```

Démontage du support

```
# bareosmount.py --umount
```

```
Démontage OK
```

Comment restaurer avec l'outil bconsole

Comment restaurer avec `bconsole`, dans le cas où la sauvegarde complète s'effectue le week-end puis des incrémentales en semaine ?



Pour faire une restauration partielle, il n'est pas nécessaire de passer par la restauration complète.

`bconsole` reconstruit l'arborescence et prend les fichiers dans le jeux de sauvegarde adéquat.

Arrêter une sauvegarde en cours

Dans certains cas (saturation du support de sauvegarde,...), il peut arriver qu'une sauvegarde reste bloquée.

Dans ce cas, il faut utiliser l'instruction `cancel` de la console Bareos : `bconsole`.

Voici un aperçu des manipulations à réaliser :

```
# bconsole
(pour lancer la console de bareos)
*status dir
(pour voir les jobs en cours)
JobId Level Name Status
=====
23 Full Complet.2010-09-03 23.00.00 02 is waiting for a mount request
24 Full BackupCatalog.2010-09-03 23.00.00 03 is waiting execution
*cancel JobId=23
(pour annuler le job en question)
*quit
```

Tester le support de sauvegarde

Pour tester le support de sauvegarde USB local ou SMB, il est possible d'utiliser le script `bareosmount.py`.



```
1 root@scribe:~# bareosmount.py -t
2 Test de montage OK
3 root@scribe:~#
```



```
1 root@scribe:~# bareosmount.py -t
2 Problème de montage (1 essais restants)
3 ERREUR : périphérique /dev/sda1 non reconnu
4 Problème de montage (0 essais restants)
5 ERREUR : périphérique /dev/sda1 non reconnu
6 Échec du test de montage :
7 point de montage : Erreur
8 permissions : Erreur
9 montage : Erreur
```

```
10 root@scribe:~#
```

```
1 root@scribe:~# bareosmount.py -t
2 Problème de montage (1 essais restants)
3 [Errno 32] mount error(13): Permission denied
4 Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
5
6 Problème de montage (0 essais restants)
7 [Errno 32] mount error(13): Permission denied
8 Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)
9
10 Échec du test de montage :
11 point de montage : Erreur
12 permissions : Erreur
13 montage : Erreur
14 root@scribe:~#
```

Options de montage du support de sauvegarde

Le fichier `/etc/eole/bareos.conf` permet de personnaliser les options de montage du support de stockage de la sauvegarde. L'intérêt est que ce fichier ne sera pas écrasé lors de la prochaine mise à jour.

Le fichier `/etc/eole/bareos.conf` a une syntaxe du type fichier INI^[p.365] : 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 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 `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 -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 créer le fichier `/etc/eole/bareos.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}'
```

Glossaire

| | |
|---|---|
| <p>.REG = <i>abréviation de registry</i></p> | <p>Un fichier portant l'extension .REG est un fichier contenant des instructions permettant d'apporter des modifications locales à la base de registre.</p> |
| <p>AAF = <i>Annuaire Académique Fédérateur</i></p> | <p>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.</p> |
| <p>ACL = <i>Access Control List</i></p> | <p>Le terme ACL désigne deux choses en sécurité informatique :</p> <ul style="list-style-type: none"> • 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. |
| <p>Anti-spoofing = <i>Anti-usurpation d'adresse IP</i></p> | <p>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.</p> <p>L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.</p> |
| <p>ARENA = <i>Accès aux Ressources de l'Éducation Nationale et Académiques</i></p> | <p>Les portails d'applications ARENA vous donnent accès aux applications en ligne du ministère de l'Éducation nationale et de l'Académie.</p> |
| <p>Backbone.js</p> | <p>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.</p> <p>http://backbonejs.org/</p> |
| <p>CAS = <i>Central Authentication Service</i></p> | <p>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.</p> |

| | |
|---|---|
| Classe de caractères | <p>Une classe de caractères définit un ensemble de caractères ayant un sens commun :</p> <ul style="list-style-type: none"> • caractères alphabétiques ; • caractères non-alphabétiques ; • les caractères numériques ; • les caractères alphanumériques ; • les caractères grecs. |
| Conteneur = LXC | <p>Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés.</p> <p>Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.</p> |
| Contrôleur de domaine NT | <p>Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire.</p> <p>Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "ADMINISTRATIF" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service administratif, et les comptes utilisateur qui sont autorisés à s'y connecter.</p> <p>Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.</p> <p>Cette base de données est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003), appelés Contrôleurs de Domaine.</p> |
| CreoleService | <p><code>CreoleService</code> est un nouvel outil qui vient remplacer avantageusement la fonction <code>Service()</code> de <code>FonctionsEoleNg</code>.</p> <p>Pour l'utiliser : <code>CreoleService apache2 reload</code></p> <p>S'il existe le même service dans plusieurs conteneurs il est possible de spécifier le conteneur.</p> <p>Exemple : <code>CreoleService -c fichier smbdc restart</code></p> |
| CSV = <i>Comma-separated values</i> | <p>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.</p> |
| CUPS = <i>Common Unix Printing System</i> | <p>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</p> |

| | |
|---|--|
| | <p>des tâches d'impression d'autres ordinateurs (les clients) et de les répartir sur les imprimantes qui sont paramétrées.</p> <p>CUPS met à disposition une interface de gestion accessible avec un navigateur web.</p> |
| <p>DHCP = <i>Dynamic Host Configuration Protocol</i></p> | <p>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.</p> |
| <p>DNS = <i>Domain Name System</i></p> | <p>Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types. L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP.</p> <p>Source : http://fr.wikipedia.org/wiki/Dns</p> |
| <p>Durée de rétention</p> | <p>La durée de rétention désigne le temps de conservation des sauvegardes avant leur effacement.</p> |
| <p>e2guardian</p> | <p>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.</p> <p>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.</p> <p>http://e2guardian.org</p> |
| <p>ELF = <i>Executable and Linkable Format</i></p> | <p>ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé</p> |
| <p>Envole</p> | <p>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.</p> <p>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 ...</p> <p>Envole est adapté pour mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Établissement (PIE) ou un Espace Numérique de Travail (ENT).</p> <p>http://envole.ac-dijon.fr/</p> |
| <p>EPLE</p> | <p>En France, un établissement public local d'enseignement (EPL) est un établissement scolaire d'enseignement secondaire (ou,</p> |

| | |
|--|--|
| <p>= <i>Établissement Public Local d'Enseignement</i></p> | <p>exceptionnellement, primaire) :</p> <ul style="list-style-type: none"> • collège • lycée d'enseignement général et technologique (LGT) • lycée professionnel (LP) • établissement régional d'enseignement adapté (EREA) • école régionale du premier degré (ERPD) |
| <p>ESU = <i>Environnements Sécurisés des Utilisateurs</i></p> | <p>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.</p> <p>ESU propose de nombreuses fonctions :</p> <ul style="list-style-type: none"> • 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. |
| <p>FAI = <i>Fournisseur d'Accès à Internet</i></p> | <p>Le FAI est un organisme (une entreprise ou une association) qui met à disposition une connexion au réseau informatique nommé Internet.</p> |
| <p>Fichiers métadatas</p> | <p>Les fichiers métadatas 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 :</p> <ul style="list-style-type: none"> • 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 ; • <p>La description complète du format de ces fichiers et des éléments possibles est disponible sur le site du consortium OASIS.</p> |
| <p>Flask</p> | <p>Flask est un framework d'application web léger écrit en Python et basé sur le toolkit Werkzeug (une librairie Python WSGI) et sur le</p> |

| | |
|---|--|
| | <p>moteur de template Jinja2.</p> <p>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.</p> <p>Il existe des extensions pour utiliser les objets relationnels, valider des formulaires, le téléchargement, diverses technologies d'authentification ouvertes, et plus encore.</p> <p>Flask est sous licence BSD.</p> <p>http://flask.pocoo.org/</p> |
| <p>GTK = <i>The GIMP Toolkit</i></p> | <p>GTK est un ensemble de bibliothèques logicielles, c'est-à-dire un ensemble de fonctions permettant de réaliser des interfaces graphiques. Cette bibliothèque a été développée originellement pour les besoins du logiciel de traitement d'images GIMP. GTK est maintenant utilisé dans de nombreux projets, dont les environnements de bureau GNOME, Xfce, Lxde et ROX.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/GTK+</p> |
| <p>Gunicorn = <i>Green Unicorn (Licorne Verte)</i></p> | <p>Gunicorn est un serveur Web HTTP WSGI écrit en Python et disponible pour Unix. Son modèle d'exécution est basé sur des sous-processus créés à l'avance, adapté du projet Ruby Unicorn. Le serveur Gunicorn est compatible avec un large nombre de frameworks Web, repose sur une implémentation simple, légère en ressources et relativement rapide.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Gunicorn_(HTTP_server)</p> |
| <p>ICMP = <i>Internet Control Message Protocol</i></p> | <p>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.</p> |
| <p>INI</p> | <p>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 « <code>.ini</code> ». Les fichiers INI sont des fichiers texte qui peuvent être manipulés avec un logiciel courant de type éditeur de texte.</p> <p>La valeur de chaque paramètre de configuration est indiquée par une formule : paramètre = valeur.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Fichier_INI</p> |
| <p>instance = <i>instanciation, instancier</i></p> | <p>Instancier un serveur correspond à la troisième étape de mise en 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</p> |

| | |
|---|---|
| | 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 <code>instance</code> . |
| InterBase | InterBase est un moteur de base de données. Il a été choisi par le ministère de l'Éducation nationale pour supporter les bases de données utilisées par les logiciels nationaux (comme GFC et SELENE, par exemple). Source Wikipédia : http://fr.wikipedia.org/wiki/InterBase |
| IPv6 <i>= Internet Protocol version 6</i> | L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4. Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire. IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés. |
| LDAP <i>= Lightweight Directory Access Protocol</i> | À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires. |
| LVM <i>= Logical Volume Management</i> | La gestion par volumes logiques est à la fois une méthode et un logiciel. Elle permet le découpage, la concaténation, le redimensionnement et l'utilisation des espaces de stockage. Le logiciel permet de gérer, de sécuriser et d'optimiser de manière souple les espaces de stockage sur les systèmes d'exploitation de type UNIX. |
| man in the middle <i>= homme du milieu</i> | 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/ |
| MTU = <i>Maximum Transmission Unit</i> | <p>La MTU définit la taille maximum du paquet (en octet) pouvant être transmis sur le réseau sans fragmentation.</p> <p>Pour plus d'information : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit</p> |
| NAS = <i>Network Attached Storage</i> | <p>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.</p> |
| NetBIOS | <p>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.</p> |
| NSCD = <i>Name Service Caching Daemon</i> | <p>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.</p> |
| NTP = <i>Network Time Protocol</i> | <p>NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.</p> |
| NUT = <i>Network UPS Tools</i> | <p>NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments :</p> <ul style="list-style-type: none"> • le démon <code>nut</code> lancé au démarrage du système ; • le démon <code>upsd</code> qui permet d'interroger l'onduleur, il est lancé sur le PC relié à l'onduleur ; • le démon <code>upsmon</code> 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. <p><code>upsd</code> peut communiquer avec plusieurs onduleurs si nécessaire. <code>upsmon</code> interroge à intervalle régulier la machine du réseau sur laquelle est lancée <code>upsd</code>.</p> |
| OpenID | <p>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</p> |

| | |
|--|---|
| | <p>informations déjà disponibles. Ce système permet à un utilisateur d'utiliser un mécanisme d'authentification forte.</p> |
| <p>OSCAR = <i>Outil Système Complet d'Assistance Réseau</i></p> | <p>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.</p> <p>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.</p> <p>http://oscar.crdp-lyon.fr</p> |
| <p>OTP = <i>One-time password</i></p> | <p>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 mémorisés par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir.</p> <p>Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique</p> |
| <p>PAM = <i>Pluggable Authentication Modules</i></p> | <p>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.</p> <p>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.</p> <p>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 être stockés sous différentes formes.</p> |
| <p>Patch</p> | <p>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.</p> |

| | |
|--|---|
| | <p>Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch.</p> <p>La procédure pour réaliser des patches 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.</p> |
| <p>PDC = <i>Primary Domain Controller</i></p> | <p>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.</p> |
| POSIX | <p>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.</p> |
| <p>PUA = <i>Potentially Unwanted Applications</i></p> | <p>Applications potentiellement indésirables.</p> |
| Restauration | <p>La restauration c'est la réutilisation de données sauvegardées. C'est l'opération inverse de la sauvegarde.</p> |
| <p>Samba = <i>SaMBa : Server Message Block</i></p> | <p>Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du protocole SMB, protocole standard de Microsoft.</p> <p>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.</p> |
| <p>SAML = <i>Security assertion markup language</i></p> | <p>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.</p> |
| <p>Sauvegarde = <i>Backup</i></p> | <p>La sauvegarde est l'opération qui consiste à dupliquer dans un lieu sûr les données contenues dans un système informatique.</p> |
| Scannedonly | <p>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</p> |

| | |
|--|---|
| | à l'utilisateur final. http://olivier.sessink.nl/scannedonly/ |
| SecurID | SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID |
| 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 = <i>Simple Mail Transfer Protocol</i> | SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique. |
| Squid | Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites. |
| SSH = <i>Secure Shell</i> | 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 = <i>Single Sign On, Authentification unique</i> | 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 : <ul style="list-style-type: none"> • 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. |
| timeout | Le timeout est la durée de validité d'une donnée avant son expiration. |
| Tiramisu <i>= Outil de gestion de configuration</i> | <p>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.</p> <p>La documentation technique du projet : http://tiramisu.labs.libre-entreprise.org</p> <p>Les sources du projet Tiramisu : http://labs.libre-entreprise.org/projects/tiramisu/</p> |
| TLS <i>= Transport Layer Security</i> | 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 | <p>Twisted est un framework d'application réseau écrit en Python et sous licence MIT.</p> <p>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.</p> <p>http://twistedmatrix.com</p> |
| UAC <i>= User Account Control</i> | <p>UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7.</p> <p>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).</p> <p>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.</p> |
| UAC <i>= User Account Control</i> | <p>UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7.</p> <p>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).</p> |

| | |
|---|---|
| | <p>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.</p> |
| <p>UNC = <i>Universal Naming Convention ou Uniform Naming Convention</i></p> | <p>UNC est une convention sur une manière de définir l'adresse d'une ressource sur un réseau.</p> <p>Plutôt que de spécifier une lettre de lecteur et un chemin d'accès (par exemple, <code>D:\lecteur</code>), on utilise la syntaxe suivante</p> <pre>\\serveur\partage\répertoire\nomFichier</pre> |
| <p>UUID = <i>Universally Unique Identifier</i></p> | <p>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 ».</p> <p>Source : http://fr.wikipedia.org/wiki/Universal_Unique_Identifier</p> |
| <p>WINS = <i>Windows Internet Name Service</i></p> | <p>WINS est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.</p> |
| <p>XML = <i>Extensible Markup Language</i></p> | <p>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 :</p> <ul style="list-style-type: none"> • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. <p>Source : http://fr.wikipedia.org/wiki/XML</p> |
| <p>XML-RPC = <i>XML Remote procedure call</i></p> | <p>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.</p> <p>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.</p> <p>Cela permet de fournir un Service web utilisable par tout le monde</p> |

| | |
|--|--|
| | <p>sans restriction de système ou de langage.</p> <p>Source : http://fr.wikipedia.org/wiki/XML-RPC</p> |
| <p>XMPP = <i>Extensible Messaging and Presence Protocol</i></p> | <p>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.</p> <p>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.</p> <p>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).</p> <p>XMPP est en développement constant et ouvert au sein de l'IETF.</p> |
| <p>YAML = <i>YAML Ain't Markup Language</i></p> | <p>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.</p> <p>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.</p> <p>Symfony 2, Drupal 8 et phpMyAdmin, entre autres, l'utilisent pour leurs formats d'entrée et de sortie.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/YAML</p> |
| <p>ZéphirLog</p> | <p>ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.</p> |