Installation et mise en œuvre du module Horus

EOLE 2.3

révisé : Mai 2014

Version du document révisé : Mai 2014

Date de création : Mars 2013

Editeur Pôle de compétence EOLE

Licence

Il est développé par le pôle de compétences EOLE du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information et des Infrastructures de L'académie de Dijon (DS2i).

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-DS2i - 2G, rue du Général Delaborde - 21000 DIJON

- Le site du pôle de compétences EOLE : http://eole.orion.education.fr

Sommaire

I Présentation et historique du projet EOLE

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

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

1 Les objectifs d'EOLE

Les objectifs du projet EOLE sont les suivants :

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

2 Logiciel Libre

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

Le logiciel libre garantit quatre niveaux de libertés :

- utilisation : la liberté d'utiliser/exécuter le logiciel pour quelque usage que ce soit ;

- étude : la liberté d'étudier le fonctionnement du programme, et de l'adapter à vos besoins ;
- redistribution : la liberté de redistribuer des copies ;
- modification : la liberté d'améliorer le programme, et de rendre publiques vos améliorations de telle sorte que la communauté tout entière en bénéficie.

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

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

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

Remarque

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

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

Pour ses développements internes, EOLE a choisi la licence libre CeCILL*.

3 Méta-distribution EOLE

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

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

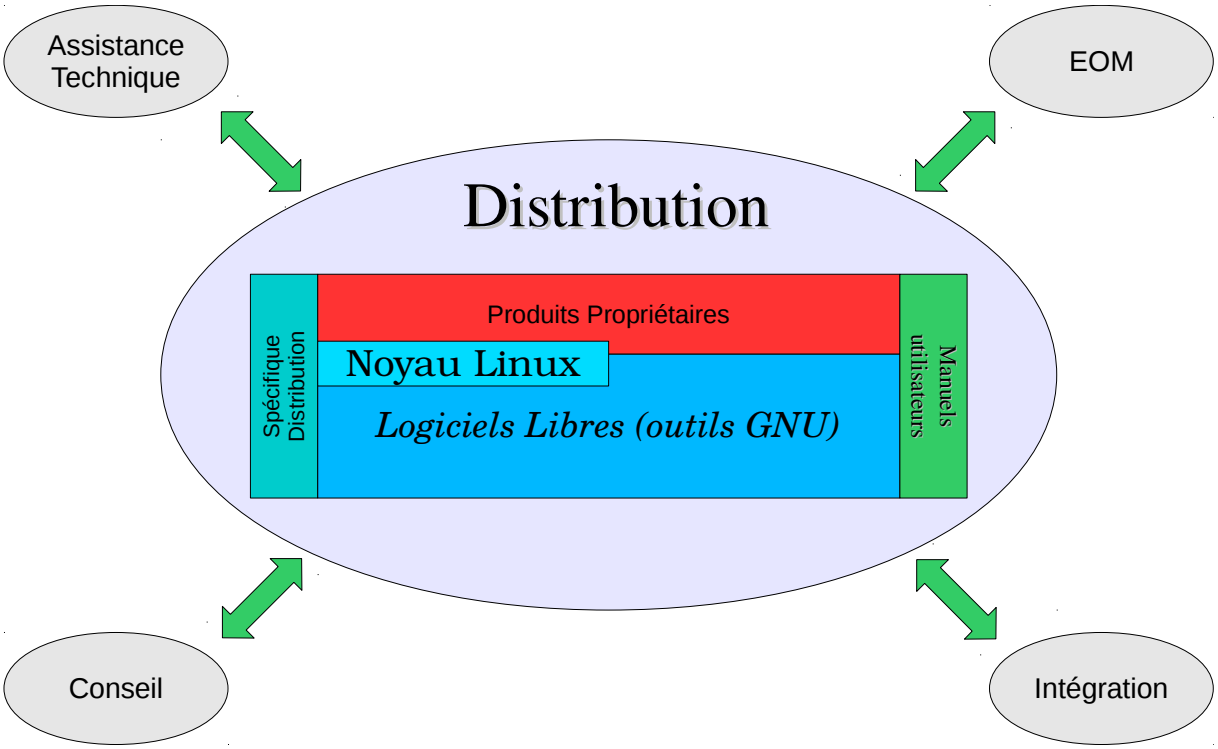
Une distribution GNU/Linux

Une distribution* GNU/Linux* est un ensemble cohérent de logiciels groupés autour d'un noyau (ou kernel) Linux.

Elle comporte :

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

- une procédure simple pour la mise à jour des logiciels.



Les modules EOLE

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

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

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

4 Panorama des modules 2.3

4.1. Le module eCDL

Le module eCDL est un contrôleur de domaine qui répond aux besoins propres de Ministère de l'Écologie mais qui peut, moyennant quelques adaptations, être utilisé partout où il est nécessaire d'avoir un contrôleur de domaine.

4.1.1. Qu'est ce que le module eCDL ?

Le module eCDL est un contrôleur de domaine de compte Samba 3*.

Il peut être interfacé avec un annuaire LDAP*, le plus souvent commun avec la messagerie.

Principales fonctionnalités

Contrôleur de domaine :

- plusieurs contrôleurs peuvent coopérer pour gérer un domaine de compte ;
- des relations d'approbation peuvent être établies entre des domaines Samba3, NT4 ou Active Directory ;
- de nombreux types de clients sont supportés. On peut intégrer dans un domaine de comptes géré par des eCDL des serveurs membres samba3 ou Windows (NT, 2000, 2003, 2008) et postes XP, Vista, Seven, Windows 8 ;
- support des scripts d'ouverture de sessions (partages netlogon).

L'eCDL comporte un mode dit de « secours » où il travaille avec une copie locale de la base LDAP du domaine en cas de perte de la liaison avec l'annuaire LDAP de l'organisation.

La gestion des comptes et des groupes n'est pas gérée directement par l'eCDL. Une application spécifique est à mettre en place pour alimenter la base LDAP interfacée avec l'eCDL.

Intégration native dans la chaîne de supervision Ministère

4.1.2. À qui s'adresse ce module ?

Le module eCDL s'adresse aux réseaux administratifs du Ministère de l'Écologie. Sous réserve d'adaptations, il peut toutefois être utilisé partout où il est nécessaire d'avoir un contrôleur de domaine.

4.1.3. Les services eCDL

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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module eCDL

- *Samba* : Contrôleur de domaine (primaire ou secondaire) serveur de fichiers permettant le partage des répertoires netlogon ;
- *supervision-psin* : client de supervision pour le Pôle de Supervision Informatique National.

4.2. Le module eSBL

Le module eSBL est un serveur de fichiers, d'impression et de sauvegarde. Il peut fonctionner de manière autonome ou être intégré dans un domaine (NT, Active Directory, LDAP).

4.2.1. Qu'est ce que le module eSBL ?

Le module eSBL est un serveur de fichiers, d'impression et de sauvegarde. Il peut fonctionner de manière autonome ou être intégré dans un domaine (NT, Active Directory, LDAP).

Principales fonctionnalités

Serveur de fichiers et d'impression :

- intégration possible dans un domaine de compte Samba 3, NT4, LDAP ou Active Directory

- partage de fichiers et de répertoires
  - un certain nombre de partages prédéfinis optionnels ont vocation à harmoniser les pratiques entre services
  - ménage automatique de partages spécifiques à des échéances définies (journalier, hebdomadaire et mensuel)
- support des ACLs ;
- support des quotas disques ;
- détection de virus;
- partage d'imprimantes et télédistribution de drivers;
- gestion des files d'attente des imprimantes connectées au serveur.

Serveur Web et FTP :

- des applications validées : OCS/GLPI/GRR
- des applications métiers : GEO-IDE base, GEO-IDE distribution
- des applications spécifiques : dépôt de signatures anti-virus (selon l'éditeur en cours au Ministère de l'Écologie)

Intégration native dans la chaîne de supervision Ministère

4.2.2. À qui s'adresse ce module ?

Le module eSBL s'adresse principalement aux réseaux administratifs du Ministère de l'Écologie. Il peut toutefois être utilisé, sans adaptation, partout où il est nécessaire d'avoir un serveur de fichiers Samba proche des standards.

Dimensionné pour 10 à 300 utilisateurs, il peut se substituer à un serveur membre d'un domaine de compte pour la gestion des droits sur les partages.

4.2.3. Les services eSBL

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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module eSBL

- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateurs, des comptes ainsi que des accès, des quotas disques et des ACL ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de bases de données ;
- *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 le courrier, les partages du serveur et les échanges FTP ;
- *Apache* : serveur web ;
- *OCS Inventory* : gestion de parc matériel ;
- *GLPI* : service helpdesk ;
- *GRR* : gestionnaire de réservations et de ressources ;
- *Arkeia* : logiciel de sauvegarde (selon l'éditeur en cours au Ministère de l'Écologie) ;
- *supervision-psin* : client de supervision pour le Pôle de Supervision Informatique National.

Service optionnel

- *dhcp3-server* : serveur DHCP.

4.3. Le module Amon

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

Il s'adresse à toutes les structures pourvues d'un réseau interne communiquant avec l'extérieur.

Un pare-feu permet de faire respecter la politique de sécurité du réseau, les types de communication autorisés.

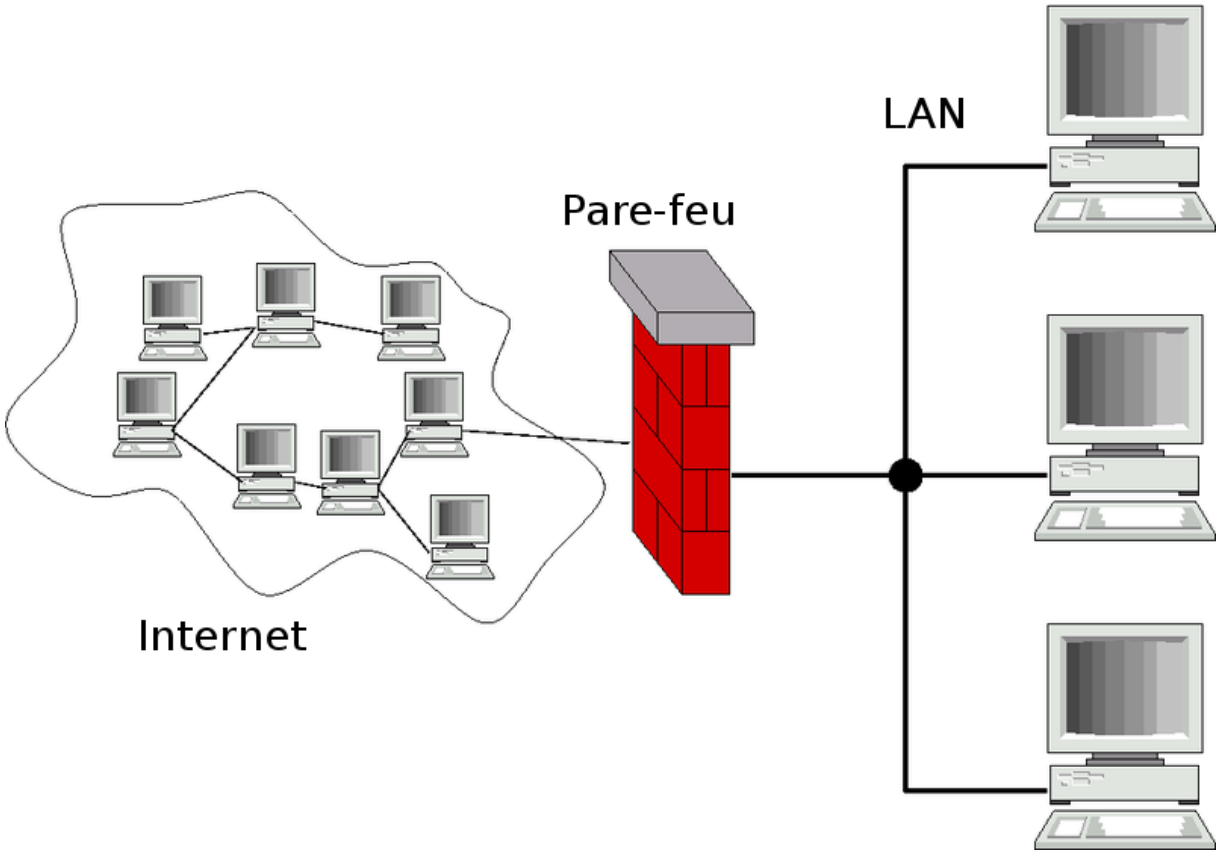
Il a pour principale tâche de contrôler le trafic entre différentes zones : Internet et le réseau interne.

Le filtrage se fait selon plusieurs critères :

- l'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.) ;

- les options contenues dans les données (fragmentation, validité, etc.) ;
- les données elles-mêmes (taille, correspondance avec un motif, etc.).

Un pare-feu permet de se prémunir des attaques extérieures.



Un pare-feu fait office de routeur, il permet donc de partager un accès Internet en toute sécurité entre les sous-réseaux d'un réseau local. Il crée un véritable intranet fédérateur au sein de votre établissement (entreprise, établissements scolaires, collectivités territoriales, association) et de n'importe quel réseau local (usage domestique).

4.3.1. Qu'est ce que le module Amon ?

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

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

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

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, Era*, est à votre disposition pour effectuer ce travail.

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

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES* .

Attention

Le module Amon assure uniquement des services liés à la sécurité : il doit être installé sur un serveur dédié.

Pour installer plusieurs modules sur un même serveur il est possible d'utiliser les modules AmonEcole, AmonHorus et AmonEcole+.

Principales fonctionnalités :

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

4.3.2. À qui s'adresse ce module ?

Le module Amon s'adresse à toutes les structures pourvues d'un réseau interne communiquant avec l'extérieur :

- entreprises ;
- établissements scolaires ;
- collectivités territoriales ;
- associations ;
- etc.

Le module Amon s'adresse à toutes les structures désireuses d'accroître la sécurité de leurs réseaux :

- de protéger leur réseau interne et/ou le découper en sous-réseaux ;
- de réguler les accès réseau vers l'extérieur ;
- de sécuriser la navigation sur le web.

Le module Amon peut être utilisé pour un usage domestique.

4.3.3. Les services Amon

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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Amon

- *Bind* : implémentation la plus répandue du DNS (résolution des noms de machine en adresse IP) ;
- *iptables* : filtrage d'adresses IP ;
- *Squid* : proxy cache qui permet d'accélérer les connexions Internet ;

- *Dansguardian* : outil de filtrage syntaxique des adresses web ;
- *LightSquid* : générateur de statistiques pour le proxy Squid ;
- *Strongswan* : version libre d'IPSec. Permet la création de réseaux virtuels privés ;
- *NginX* : reverse proxy ;
- *FreeRADIUS* : service d'authentification réseau ;
- *Era* : outil de génération de règles iptables.

4.4. Le module Eclair

Le module Eclair est un serveur de clients légers GNU/Linux.

Il permet de faire fonctionner, depuis le réseau, un grand nombre de machines clientes avec ou sans système d'exploitation installé.

Que se soit sur des machines obsolètes pour accueillir un système d'exploitation et/ou sans disque dur ou que se soit sur des machines basse consommation, les clients légers exécutent leur système d'exploitation ainsi que toutes leurs applications directement sur le serveur.

Le module Eclair s'appuie sur la technologie LTSP*, sur le projet LTSP et intègre LTSP-Cluster.

4.4.1. Qu'est ce que le module Eclair ?

Le module Eclair est un serveur de clients légers GNU/Linux qui s'appuie sur la technologie LTSP* et le projet LTSP.

Grâce à LXC tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.

En pratique le serveur Eclair est la seule machine ayant un système d'exploitation installé, il exporte son système vers les clients légers.

Le système et toutes les applications disponibles sur les clients légers (les terminaux) sont en fait installés sur le serveur, il n'y a donc qu'une seule machine à administrer.

Si vous installez une application sur le serveur, elle sera immédiatement disponible pour tous les clients légers.

Tout ceci est complètement transparent pour l'utilisateur qui utilise le client léger (le terminal) exactement comme s'il utilisait un poste de travail ordinaire.

Les avantages sont multiples :

- économie de maintenance, seul le serveur est à maintenir ;
- économie d'administration, seul le serveur est à administrer ;
- pas besoin de passer derrière chaque machine pour propager une modification ;
- possibilité de contrôler n'importe lequel des terminaux ;
- possibilité d'exécuter la même application sur chacun d'eux ;
- les clients sont faciles à changer quand ils deviennent défectueux.

Principales fonctionnalités

- démarrer des machines à travers le réseau ;
- fournir des applications embarquées ;
- gérer les sessions graphiques (bloquer une application, bloquer la session, envoi de messages, …) ;
- diffusion de la session graphique de l'enseignant ;
- prise en main à distance ;
- partager son poste de travail.

Attention

Les modules AmonEcole, AmonEcole+, AmonHorus et Eclair sont fournis exclusivement en mode conteneur.

4.4.2. À qui s'adresse ce module

Le module Eclair intègre LTSP-Cluster. C'est une extension de LTSP qui ajoute les composants nécessaires pour des déploiements à grande échelle. Il rend possible et facile le déploiement et la gestion de milliers de clients légers se connectant à un cluster de serveurs d'applications GNU/Linux et/ou Windows.

Cette extension rend le module évolutif en lui permettant d'augmenter sa capacité, notamment sa montée en charge, tout en conservant ses fonctionnalités et ses performances.

Le serveur de clients légers Eclair s'adresse donc :

- aux structures gérant un grand nombre de postes, qui souhaitent mettre à disposition des stations en libre service (mode kiosque), qui ne veulent ou ne peuvent pas administrer un parc de machines entier, ou qui ont beaucoup de machines obsolètes qu'elles souhaitent réutiliser etc ...
- aux structures gérant un petit nombre de postes comme une école par exemple. La solution serveur de clients légers Eclair permet de mettre à disposition des machines hétérogènes, tous les ordinateurs de l'école ont un même système d'exploitation et ce à partir d'une machine unique.

Le module Eclair répond aussi bien aux besoins de ceux qui souhaiteraient réduire leur budget d'achat d'ordinateurs qu'à ceux qui souhaiteraient s'affranchir d'une grosse partie de la tâche d'administration en limitant celle-ci au serveur.

4.4.3. Les services Eclair

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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Eclair

- *PXE/TFTP* : serveur de démarrage réseau ;
- *tftpd-hpa* : serveur TFTP ;
- *ltsp-cluster* : service de Load Balancing ;
- *Apache* : serveur web ;
- *PostgreSQL* : système de gestion de bases de données
- *Alsa* : serveur son ;
- *Epoptes* : gestion des clients légers ;
- *NDB* : montage d'une image d'un système de fichiers et des applications embarquées.

4.5. Le module Horus

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

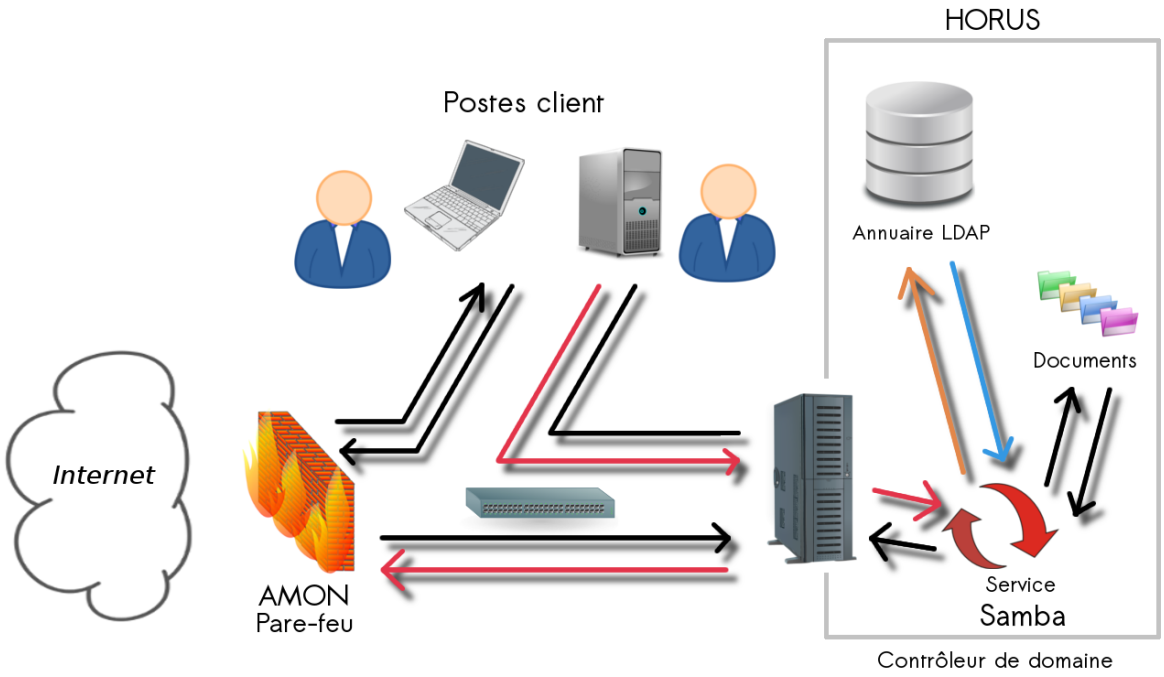
Il est également utilisable dans n'importe quelle autre structure nécessitant un contrôleur de domaine.

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.

4.5.1. 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*, 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*. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP* pour l'attribution dynamique d'adresse IP.

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

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

Complément

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-personnels-de-direction/detail-d-une-fiche/?a=74&cHash=a2e9902743

Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL* ;
- 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*, CSV*, ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- un service de messagerie instantanée (standard XMPP*) ;

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).

4.5.2. 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.

4.5.3. 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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *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* ;
- *CUPS* : serveur d'impression ;
- *InterBase* : système de gestion de bases de données utilisé pour les anciennes applications nationales ;
- *MySQL* : système de gestion de bases 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 ;
- *dhcp3-server* : serveur DHCP.

4.6. Le module Scribe

Le module Scribe est un contrôleur de domaine dotée de fonctions évoluées. Il optimise la gestion de votre parc de stations clientes.

Il intègre un serveur de fichiers et d'impression, un système de messagerie et une gestion avancée des utilisateurs et des postes clients.

Le module Scribe héberge de nombreuses applications web au sein d'un portail Web 2.0 et offre la possibilité d'en rajouter.

Le tout est articulé autour d'un annuaire performant qui référence, élèves, responsables légaux, personnels enseignant et administratif.

4.6.1. Qu'est ce que le module Scribe ?

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

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

Grâce à LXC tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.

Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL* ;
- quotas disques ;
- partage d'imprimantes ;
- gestion des comptes utilisateurs et des accès ;
- exécution d'applications utilisateur ;

- gestion des devoirs élève.

Serveur de messagerie articulé autour d'un annuaire performant :

- l'annuaire est initialisé à partir d'importations de comptes (SIECLE*, BE1D, AAF*, CSV*,...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseaux ;
- la messagerie gère deux domaines distincts (l'Internet et l'intranet académique) ;
- utilisation au choix d'une interface web multilingue ou d'un client de messagerie (standards IMAP* et POP*) ;
- un service de listes de diffusion ;
- un service de messagerie instantanée (standard XMPP*) ;
- une sécurité anti-spam, un anti-virus, une gestion de quotas (taille des boites aux lettres), ...

Serveur web :

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

4.6.2. À qui s'adresse ce module ?

Le module Scribe s'adresse principalement aux réseaux pédagogiques des établissements scolaires.

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

4.6.3. Les services Scribe

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 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Scribe

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL* ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de bases de données ;
- *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 le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Exim4* : serveur de messagerie ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;
- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

4.7. Le module Seshat

Le module Seshat permet la centralisation de l'authentification et la réplication d'annuaires LDAP*.

4.7.1. Qu'est ce que le module Seshat ?

Seshat permet de mettre en place une **réplication d'annuaire centralisée** et un système d'**authentification centralisé**.

La fonctionnalité de **relais de messagerie** est optimisée pour relier les serveurs Scribe d'une même académie.

4.7.2. À qui s'adresse ce module ?

À toutes les structures désirant mettre en place un relais de messagerie et des applications centralisées (rectorat, collectivités territoriales, entreprises).

4.7.3. Les services Seshat

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

Chacune de ces services peut évoluer indépendamment des autres et faire l'objet d'une actualisation ou d'une intégration par l'intermédiaire des procédures de mise à jour, et ce afin d'ajouter de nouvelles fonctionnalités ou d'augmenter la sécurité.

Services communs à tous les modules

- *Noyau Linux 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffré et sécurisé) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *Rsyslog* : service de journalisation. Il permet également la centralisation des logs ;
- *Pam* : Gestion des authentifications ;
- *EAD* : l'outil d'administration du serveur ;
- *EoleSSO* : gestion de l'authentification centralisée ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Seshat

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *MySQL* : système de gestion de bases de données ;

- *ClamAV* : anti-virus, il peut être activé pour surveiller le courrier, les partages du serveur et les échanges FTP ;
- *Apache* : serveur web ;
- *Exim4* : serveur de messagerie ;
- *Spamassassin* : anti-spam.

4.7.4. Pré-requis

Cette partie n'est pas encore documentée #fixme

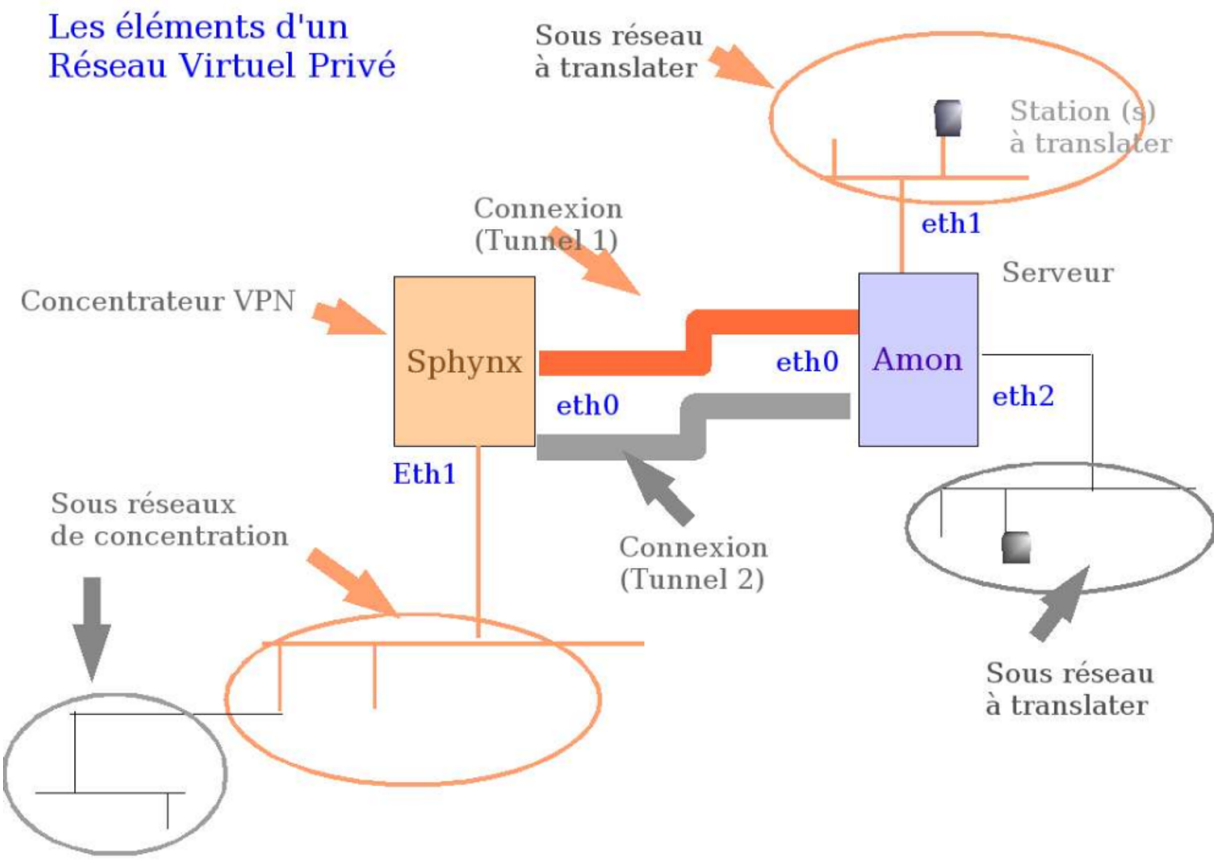
4.7.5. Les différences entre les versions 2.2 et 2.3

La nouvelle version du module Seshat apporte un certain lot de changements, loin d'être exhaustive voici une liste des points les plus importants :

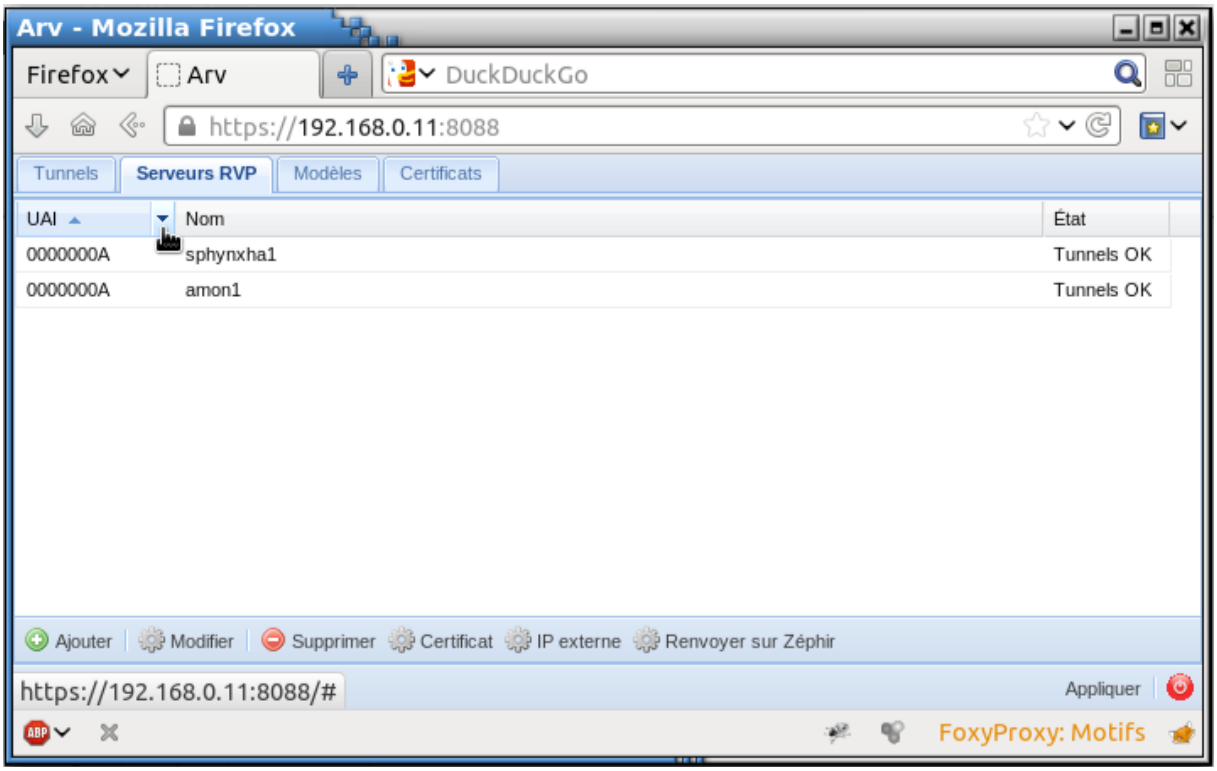
- l'annuaire LDAP du module Seshat dispose de son propre utilisateur en lecture seule (`cn=reader`) ;
- la déclaration des hôtes à relayer (relayhosts) s'effectue dans l'interface de configuration du module et plus dans l'interface d'administration EAD.

4.8. Le module Sphynx

Le serveur Sphynx est un concentrateur de Réseaux Virtuels Privés (RVP* ou VPN). Il permet de relier des stations, des sous-réseaux, ou des réseaux entre eux, au travers d'Internet et ce de manière sécurisée. Le serveur Sphynx fait partie des éléments constitutifs du réseau AGRIATES*.



L'outil ARV*, pré-configuré dans le module Sphynx, permet de construire un modèle de configuration RVP. Il permet de générer des configurations RVP pour strongSwan*.



4.8.1. Qu'est ce que Sphynx ?

Sphynx est un concentrateur de Réseau Virtuel Privé (RVP*). Il vous permet de relier en réseau vos serveurs pour former un RVP entre le module pare-feu Amon des établissements distants et le module Sphynx en entrée de votre réseau académique.

Principales fonctionnalités

- possibilité de travailler avec des certificats auto-signés ou signés par une PKI* externe simultanément ;
- le concentrateur académique Sphynx comprend un pare-feu pour se protéger des attaques ;
- communications chiffrées entre les réseaux des établissements et le réseau académique ;
- préparation des configurations établissement sur le serveur Sphynx grâce à l'outil ARV* ;
- mise à jour opérée sur le serveur Sphynx au moyen des outils livrés dans la distribution.

4.8.2. À qui s'adresse ce module ?

Le concentrateur de Réseaux virtuels privés Sphynx s'adresse à toutes les structures souhaitant prolonger leur réseau au travers d'Internet.

4.8.3. Les services Sphynx

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

Chacune de ces services peut évoluer indépendamment des autres et faire l'objet d'une actualisation ou d'une intégration par l'intermédiaire des procédures de mise à jour, et ce afin d'ajouter de nouvelles fonctionnalités ou d'augmenter la sécurité.

Services communs à tous les modules

- *Noyau Linux 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffré et sécurisé) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *Rsyslog* : service de journalisation. Il permet également la centralisation des logs ;
- *Pam* : Gestion des authentifications ;
- *EAD* : l'outil d'administration du serveur ;
- *EoleSSO* : gestion de l'authentification centralisée ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Sphynx

- *Iptables* : filtrage d'adresses IP ;
- *Strongswan* : version libre d'IPSec. Permet la création de réseaux virtuels privés ;
- *ARV* : interface d'administration des réseaux virtuels (VPN) ;
- *Pacemaker* : haute disponibilité ;
- *Quagga* : routage dynamique.

4.9. Le module Zéphir

Le module Zéphir propose une solution normalisée pour faciliter le **déploiement**, la **surveillance** et la **maintenance** des modules EOLE.

Ce module permet une gestion centralisée des serveurs EOLE tout en autorisant certaines divergences de configuration.

4.9.1. Qu'est ce que le module Zéphir ?

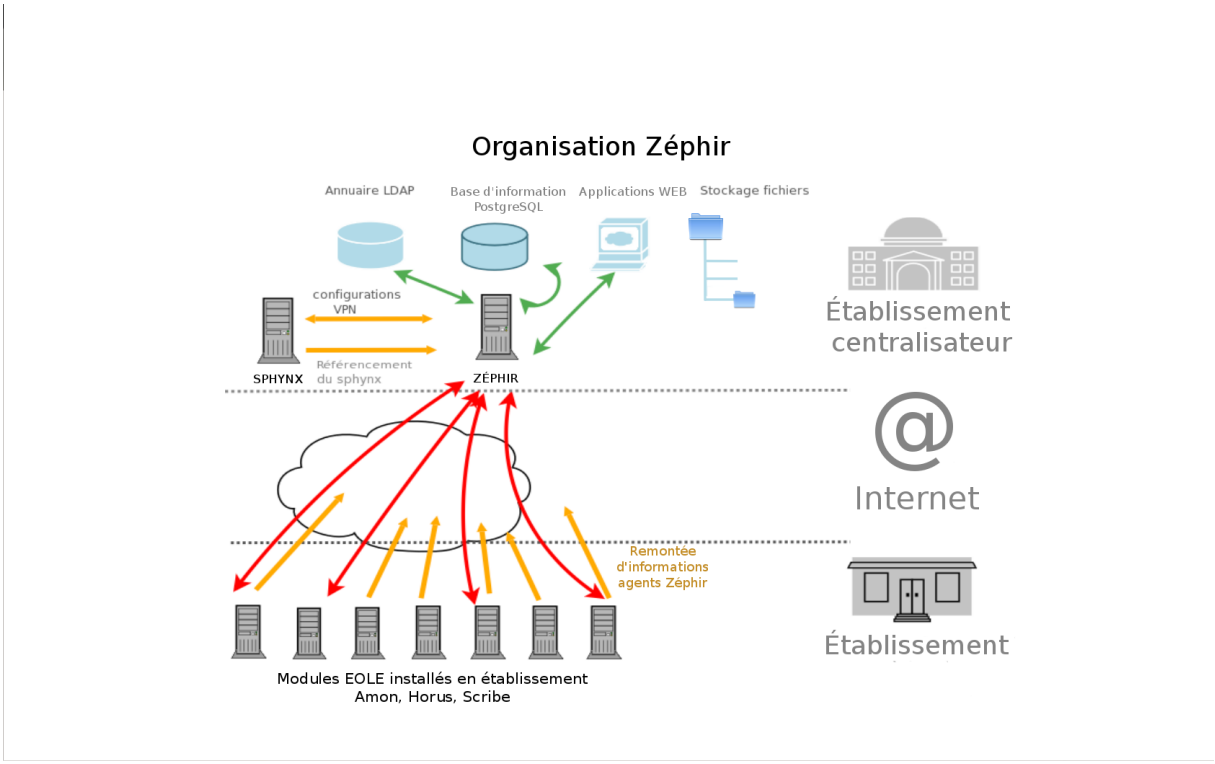
Le module Zéphir permet de déployer et gérer un parc de serveurs. Il héberge une base de données des établissements et des serveurs installés dans ces établissements. Cette base de données peut être pré--initialisée à partir du fichier national des établissements. L'ensemble constitue un inventaire de votre parc matériel.

Le module permet la gestion des différentes configurations serveur.

Il prend en charge :

- la génération des configurations serveurs (création du dictionnaire) ;
- le stockage de ces configurations ;
- la distribution de ces configurations sur les serveurs à travers le réseau ;
- la mise à jour des configurations avec une gestion des différentes versions et un historique des modifications effectuées.

Le module Zéphir permet également la surveillance des serveurs déployés en établissements. Il permet la remontée d'alertes à intervalles réguliers et le lancement d'actions à distance.



Principales fonctionnalités

- gestion centralisée des configurations ;
- travail sur des groupes de serveurs ;
- possibilité de spécialiser un module en variante ;

- aide à l'installation des serveurs clients ;
- actions à distance sur les clients ;
- surveillance des serveurs ;
- actions automatiques des agents ;
- possibilité de changer l'adresse IP du module Zéphir ;
- création d'actions personnalisées ;
- sauvegarde de fichiers dans une variante ;
- gestion des serveurs de mise à jour ;
- gestion centralisée d'identifiants pour les ENT.

4.9.2. À qui s'adresse ce module ?

Le module Zéphir s'adresse aux **administrateurs** et aux **équipes d'intervention** des réseaux informatiques académiques ou de toute autre structure (collectivités territoriales) ayant en charge l'installation, la configuration et le suivi de parcs de serveurs.

Le module Zéphir peut travailler par profils (rôles) ce qui permet des vues et des actions différentes sur les différents serveurs gérés.

Le module permet d'administrer et de surveiller plusieurs centaines de serveurs.

4.9.3. Les services Zéphir

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

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

Services communs à tous les modules

- *Noyau Linux 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Services spécifiques au module Zéphir

- *PostgreSQL* : base de donnée relationnelle pour le stockage des informations du serveur ;
- *OpenLDAP* : service d'annuaire utilisé pour l'authentification des utilisateurs (annuaire local ou externe) ;
- *Ulog* : stockage des logs ;
- *Zephir-Web* : application web pour gérer les serveurs EOLE déployés.

4.10. Le module AmonEcole

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

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

Ce module intègre donc les fonctionnalités des 2 modules :

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

4.10.1. Qu'est ce que le module AmonEcole ?

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

Grâce à LXC tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.

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

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

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

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, Era*, est à votre disposition pour effectuer ce travail.

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

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES*.

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

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

Principales fonctionnalités

Service réseau :

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

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL* ;
- quotas disque ;

- partage d'imprimantes ;
- gestion des comptes utilisateur et des accès ;
- exécution d'applications utilisateur ;
- gestion des devoirs élève.

Serveur de messagerie articulé autour d'un annuaire performant :

- l'annuaire est initialisé à partir d'importations de comptes (SCONET*, BE1D, AAF*, CSV*,...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- la messagerie gère deux domaines distincts (l'Internet et l'intranet académique) ;
- utilisation au choix d'une interface web multilingue ou d'un client de messagerie (standards IMAP et POP) ;
- un service de listes de diffusion ;
- un service de messagerie instantanée (standard XMPP*) ;
- une sécurité anti-spam, un anti-virus, une gestion de quotas (taille des boites aux lettres), ...

Serveur web :

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

Gestion avancée des utilisateurs et des postes client :

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

Attention

Ce module est fourni exclusivement en mode conteneur.

4.10.2. À qui s'adresse ce module ?

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

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

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

4.10.3. Les services AmonEcole

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

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

Services communs à tous les modules

- *Noyau Linux 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

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

Services spécifiques au module Amon

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

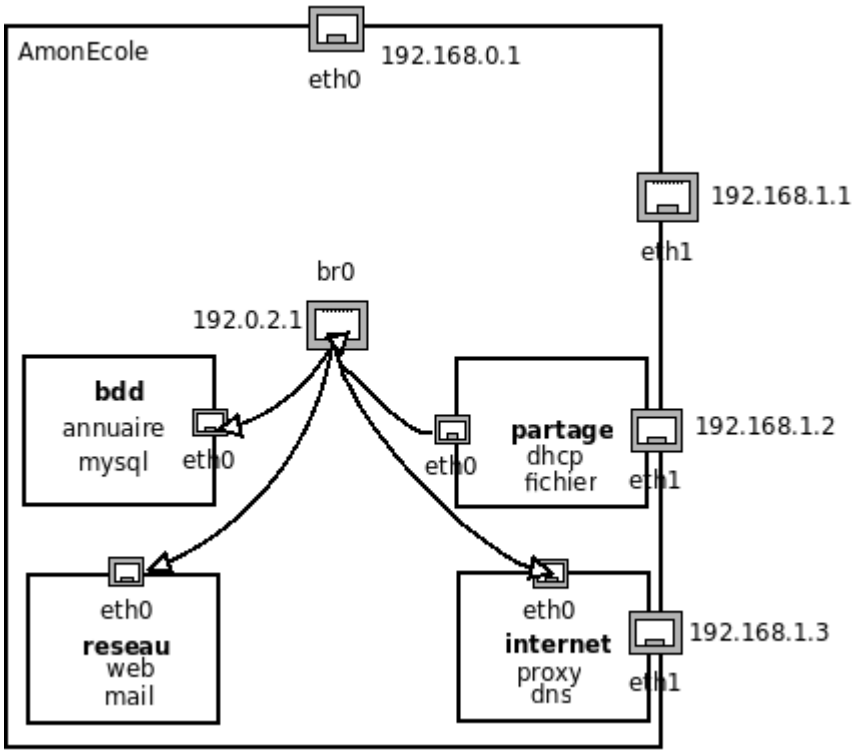
- *Era* : outil de génération de règles iptables.

Services spécifiques au module Scribe

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL* ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de bases de données ;
- *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 le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Exim4* : serveur de messagerie ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;
- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

4.10.4. Les conteneurs

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



Deux conteneurs ont une adresse IP sur le réseau eth1 :

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

4.11. Le module AmonEcole+ (AmonEcole-Eclair)

Le module **AmonEcole+**, également dénommé **AmonEcole-Eclair**, est un pare-feu pédagogique facile à installer et à utiliser.

Il est l'association des modules Amon, Scribe et Eclair.

Ce module intègre donc les fonctionnalités des 3 modules :

- il vous permet de partager votre sortie Internet en toute sécurité, et de créer un intranet fédérateur au sein de votre établissement ou de n'importe quel réseau local (entreprise, association, domestique, etc.) ;
- il intègre un serveur de fichiers et d'impression, un système de messagerie articulé autour d'un annuaire performant, des services web et une gestion avancée des utilisateurs et des postes client ;
- il permet de faire démarrer, depuis le réseau, des machines sans système d'exploitation installé (clients légers GNU/Linux).

4.11.1. Qu'est ce que le module AmonEcole+ ?

AmonEcole+ est un module qui intègre les fonctionnalités du module **Amon** (pare-feu), les fonctionnalités du module **Scribe** (serveur pédagogique) ainsi que les fonctionnalités du module **Eclair** (serveur de clients légers GNU/Linux).

Grâce à LXC tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.

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

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

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

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, Era*, est à votre disposition pour effectuer ce travail.

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

Pour l'Éducation Nationale, ce réseau est nommé réseau AGRIATES* .

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

Il fournit également un serveur de clients légers GNU/Linux permettant d'utiliser des machines sans système d'exploitation.

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

Principales fonctionnalités

Service réseau :

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

Serveur de fichiers et d'impression :

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

Serveur de messagerie articulé autour d'un annuaire performant :

- l'annuaire est initialisé à partir d'importations de comptes (SCONET, BE1D, AAF, CSV,...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- la messagerie gère deux domaines distincts (l'Internet et l'intranet académique) ;
- utilisation au choix d'une interface web multilingue ou d'un client de messagerie (standards IMAP et POP) ;
- un service de listes de diffusion ;
- un service de messagerie instantanée (standard XMPP*) ;
- une sécurité anti-spam, un anti-virus, une gestion de quotas (taille des boites aux lettres), ...

Serveur web :

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

Serveur de clients légers GNU/Linux :

- démarrer des machines à travers le réseau ;
- fournir des applications embarquées ;
- gérer les sessions graphiques (bloquer une application, bloquer la session, envoi de messages, …) ;
- diffusion de la session graphique de l'enseignant ;
- prise en main à distance ;
- partager son poste de travail.

Attention

Les modules AmonEcole, AmonEcole+, AmonHorus et Eclair sont fournis exclusivement en mode conteneur.

4.11.2. À qui s'adresse ce module ?

Le module AmonEcole+ permet d'avoir un pare-feu Amon, un serveur pédagogique Scribe et un serveur de clients légers Eclair.

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

De ce fait, le module AmonEcole+ est adapté aux grandes structures (résistance à la charge, minimisation des moyens) et s'avère très pratique pour les plus petites (minimisation de la maintenance).

4.11.3. Les services AmonEcole+

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

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

Services communs à tous les modules

- *Noyau Linux 2.6* : Noyau Linux Ubuntu ;
- *OpenSSH* (équivalent à la commande telnet* chiffrée et sécurisée) : cet outil permet une prise en main à distance moyennant une demande d'authentification sur la machine cible ;
- *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 ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

Le module **AmonEcole+** reprend les services des modules Amon, Scribe et Eclair.

Services spécifiques au module Amon

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

Services spécifiques au module Scribe

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL* ;
- *CUPS* : serveur d'impression ;

- *MySQL* : système de gestion de bases de données ;
- *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 le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Exim4* : serveur de messagerie ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;
- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

Services spécifiques au module Eclair

- *PXE/TFTP* : serveur de démarrage réseau ;
- *tftpd-hpa* : serveur TFTP ;
- *ltsp-cluster* : service de Load Balancing ;
- *Apache* : serveur web ;
- *PostgreSQL* : système de gestion de bases de données
- *Alsa* : serveur son ;
- *Epoptes* : gestion des clients légers ;
- *NDB* : montage d'une image d'un système de fichiers et des applications embarquées.

4.11.4. Structure des conteneurs

Le module AmonEcole+ reprend la structure des conteneurs du module AmonEcole et y ajoute les conteneurs du module Eclair.

De ce fait sur le module AmonEcole+ les fonctionnalités sont distribuées dans 6 conteneurs.

4.12. Le module AmonHorus

4.12.1. Qu'est ce que le module AmonHorus ?

AmonHorus intègre les fonctionnalités du module **Amon** (pare-feu) et celles du module **Horus** (serveur administratif).

Grâce à LXC tous les services seront installés sur une seule machine mais séparés grâce à l'usage de conteneurs.

Un conteneur est une zone isolée à l'intérieur du système et qui a un espace spécifique du système de fichier, un réseau, des processus, des allocations mémoires et processeurs. Cette technique permet de faire fonctionner de multiples environnements GNU/Linux isolés les uns des autres sur un seul et même système hôte.

Contrairement à d'autres techniques de virtualisation, il n'y qu'une seule instance du noyau présente pour l'ensemble des conteneurs et du maître.

LXC limite le nombre de serveurs nécessaires, tout en continuant à séparer les environnements et en conservant un haut degré de sécurité.

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

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

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

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, Era*, est à votre disposition pour effectuer ce travail.

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

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES*.

Le module offre un **serveur de fichiers administratif**, il peut également se substituer à un contrôleur de domaine NT*, 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.

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*. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP* pour l'attribution dynamique d'adresse IP.

Principales fonctionnalités

Service réseau :

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

Serveur de fichiers et d'impression :

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

Annuaire :

- l'annuaire est initialisé à partir d'importation de comptes (AAF, CSV, ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseaux ;
- un service de messagerie instantanée (standard XMPP*) ;

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).

Attention

Les modules AmonEcole, AmonEcole+, AmonHorus et Eclair sont fournis exclusivement en mode conteneur.

4.12.2. A qui s'adresse-t'il ?

AmonHorus permet d'avoir un pare-feu Amon et un serveur administratif Horus.

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

De ce fait, AmonHorus est particulièrement adapté aux petites structures en termes d'effectif ou de moyens comme les collèges. AmonHorus est également adapté à des structures plus importantes comme les cités scolaires.

4.12.3. Structure des conteneurs

De la même manière que le module AmonEcole qui reprend les fonctionnalités des modules Scribe et Amon, le module AmonHorus reprend les fonctionnalités des modules Horus et Amon en les distribuant dans 4 conteneurs.

La structure des conteneurs du module AmonHorus est quasiment identique à celle du module AmonEcole, les services de messagerie avancée en moins.

5 Les Grandes Dates

2000 :

Projet local à l'Académie de Dijon pour répondre à un besoin identifié.

2001 :

Projet National à la demande du Ministère National de l'Enseignement Supérieur et de la Recherche (MENESR).

Les buts étaient :

- protéger les élèves ;
- protéger les données administratives.

La version 1.0 du module pare-feu Amon voit le jour.

2002 :

Études de contenu nationales & développement par le Centre d'Études et de Traitements Informatiques de l'Académie de Dijon (CETIAD) :

- généralisation du module Amon dans les collèges et lycées ;
- 2 nouveaux modules :
  - concentrateur de réseaux privés virtuels : module Sphynx 1.0 ;
  - serveur de fichiers administratif : module Horus 1.0.

2003 :

Équipe EOLE devient Pôle de compétence EOLE :

- Module Amon 1.5.

2004 :

- Module Sphynx 1.1 ;
- Module Scribe 1.0 : serveur de fichiers pédagogique ;
- Écriture d'un éditeur de règles pour le module Amon nommé Era.

2005 :

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

2006 :

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

2007 :

- intégration de @SSR sur le module Scribe (sécurité routière) ;
- EOLE NG 2.0 Stable (en octobre).

2008 :

- EOLE NG 2.1 Stable (en mai) ;
- nouveau module : serveur de clients légers Linux Eclair.

2009 :

- EOLE NG 2.2 LTS Stable (en janvier) ;
- nouveaux modules :
  - le serveur virtualisé AmonEcole ;

- la console de visualisation de l'IDS Prélude (fonctionnant avec ZéphirLog) ;
- le relais de messagerie pour le domaine intra-académique nommé module Seshat.

2011 :

- EOLE NG 2.3 LTS Stable (en juin) ;
- ajout du mode conteneur.

2012 :

- nouveau module : AmonEcole+ (AmonEcole-Eclair)

2013 :

- EOLE 2.4 LTS alpha-1 (septembre) ;
- EOLE 2.4 LTS alpha2 (octobre) ;
- nouveau module 2.4 : Thot.

2014 :

- EOLE 2.4 LTS RC (février) ;
- EOLE 2.4 LTS Stable (mai).

6 Quelques références

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

II 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 offre toutes les fonctionnalités de partage de fichiers et d'imprimantes.

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*, 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*. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP* pour l'attribution dynamique d'adresse IP.

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

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

Complément

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-personnels-de-direction/detail-d-une-fiche/?a=74&cHash=a2e9902743

Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL* ;
- 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*, CSV*, ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- un service de messagerie instantanée (standard XMPP*) ;

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.

III Fonctionnement du module Horus

Cette partie n'est pas encore documentée #fixme

IV Mise en œuvre

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

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

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

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

- La **phase de configuration** s'effectue au moyen de l'outil de configuration [gen_config].

  Cet outil permet de renseigner et de stocker en un seul fichier (**<fichier>.eol**) tous les paramètres nécessaires à l'utilisation du serveur dans son environnement (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 est plus ou moins important.

  Cette phase d'adaptation peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid, DansGuardian, etc.

- La **phase d'instanciation** s'effectue au moyen de la commande [instance] suivie du chemin et du nom d'un fichier de configuration généré lors de la phase d'adaptation.

  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

  A l'issue de cette phase, le serveur est utilisable en exploitation.

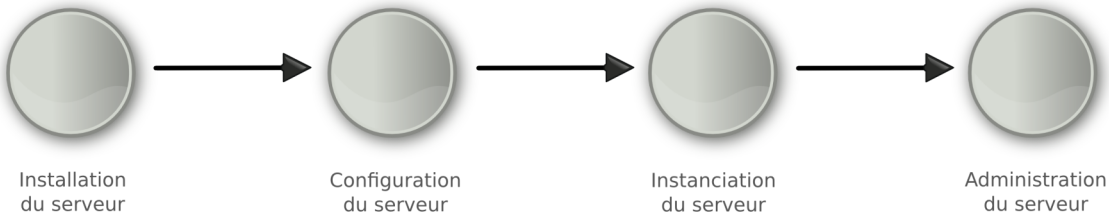
  Cette phase doit être complétée par un diagnostique du serveur (commande **diagnose [-L]**).

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

  Chaque module possède des fonctionnalités propres, souvent complémentaires.

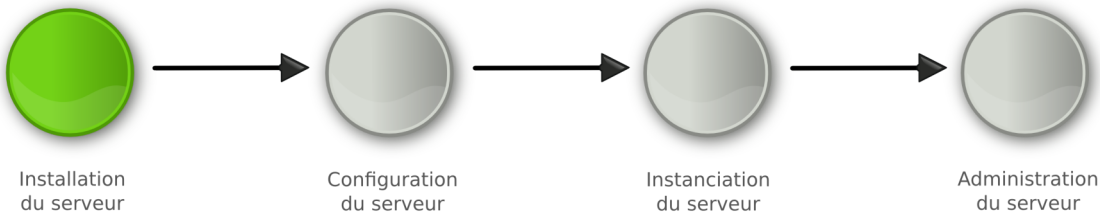
  Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

Pour suivre ces différentes étapes, nous utiliserons un fil rouge des phases de la mise en œuvre :



V Installation

La première des quatre phases



1 Pré-requis

Choix du matériel

Il est recommandé de vérifier la compatibilité matérielle en s'assurant que le serveur est compatible avec Ubuntu serveur 10.04 (lucid lynx).

Une base des matériels, enrichie automatiquement par les installations de modules EOLE, est disponible à l'adresse : http://eole.orion.education.fr/materiel/.

Cette base indique seulement qu'un utilisateur a réussi à installer et instancier un module, cela ne garantit pas son fonctionnement.

Choix de l'architecture

Deux architectures sont supportés par EOLE :

- la version 32 bits (x86) ;
- la version 64 bits (AMD64).

Remarque

AMD64 est le nom d'une architecture processeur développée par la société AMD.

Cette architecture est compatible avec le standard 32 bits x86 d'Intel.

Elle est utilisée, entre autres, par les AMD *Athlon 64*, *Athlon FX*, *Athlon X2*, *Sempron 64*, *Turion* et *Opteron*.

Intel a par la suite adopté cette architecture pour ses processeurs récents de type *Pentium 4*, *Pentium D*, *Pentium Extreme Edition*, *Celeron D*, et *Xeon*.

2 Médias d'installation

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

- http://eoleng.ac-dijon.fr/pub/iso
- ftp://eoleng.ac-dijon.fr/pub/iso

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

```
$ md5sum -c MD5SUMS
eole-2.3.5-alternate-i386.iso: OK
```

Différents types de média sont utilisables pour installer les modules.

CD-ROM

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

USB

1. installer le paquet `usb-creator` sur une distribution GNU/Linux Ubuntu ;
2. lancer l'interface `usb-creator-gtk`, cliquer sur Autre... et choisir l'image ISO préalablement téléchargée ;
3. insérer une clé USB et cliquer sur Effacer le disque (les données seront perdues) ;
4. cliquer sur Créer un disque de démarrage ;
5. démarrer le serveur cible sur la clé USB.

PXE

Le document suivant décrit la mise en place d'une configuration PXE pour installer les modules EOLE :

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

3 Déroulement de l'installation

Pour installer un module, il suffit de :

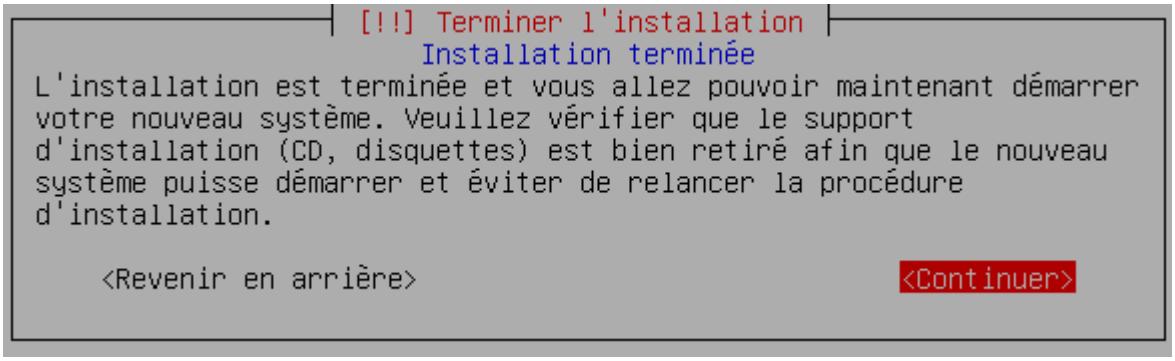
- démarrer le serveur cible sur le média choisi ;
- sélectionner le module à installer parmi ceux proposés ;
- valider.

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

Les différentes phases de l'installation sont :

1. détection du matériel ;
2. charger des composants supplémentaires ;
3. configuration du réseau avec DHCP ;
4. démarrage de l'outil de partitionnement ;
5. partitionnement assisté ;
6. formatage des partitions ;
7. configuration de l'outil de gestion des paquets (apt) ;
8. choisir et installer des logiciels ;
9. installation du programme de démarrage GRUB ;
10. fin de l'installation.

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



En validant Continuer, le système redémarre automatiquement.

Cas particuliers

Seule l'installation d'**Eolebase**, aiguille systématiquement vers un partitionnement manuel et nécessite une intervention.

Cependant, si l'installeur rencontre deux disques durs ou plus, dans l'ordinateur il passe également en partitionnement manuel quelque soit le module.

Si le partitionnement proposé n'est pas satisfaisant ou pour des partitionnements particuliers (RAID), la procédure est la suivante :

- lancer une installation **Eolebase** qui vous proposera de partitionner manuellement (anciennement partitionnement PRO) ;
- installer ensuite le module souhaité au moyen du programme en ligne de commande : [apt-get install nomdumodule-pkg]

Truc & astuce

Si vous n'avez qu'un seul disque dur mais que vous désirez partitionner vous même ce disque, connectez une clé (ou un disque) USB à l'ordinateur. Cette clé (ou ce disque) sera détectée comme un second disque dur et déclenchera le partitionnement manuel.

Attention, les clés USB ne sont pas toujours vues comme des disques en fonction des paramètres du BIOS.

Veillez à ne créer des partitions que sur le disque dur de l'ordinateur. La clé USB pourra être retirée au prochain démarrage.

Une fois le système redémarré, vous devez ouvrir une session avec l'utilisateur **root** et le mot de passe **$eole&123456$** par défaut.

4 Le mode conteneur

EOLE propose un système évolué et cohérent de conteneurs*.

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

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

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

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

Modules en "mode non conteneur"

La quasi totalité des modules des images 2.3 sont installables en *mode non conteneur* :

- `Amon` ;
- `Horus` ;
- `Scribe` ;
- `Seshat` ;
- `Sphynx` ;
- `Zéphir`.

Modules en "mode conteneur"

Contrairement à ceux cités précédemment, les modules `AmonEcole`, `AmonHorus` et `Eclair` installables depuis les images 2.3 sont **obligatoirement** en *mode conteneur*.

Sur ces modules, certains services installés dans différents conteneurs ne sont pas compatibles entre eux, ce qui rend leur installation en *mode non conteneur* impossible.

Le mode conteneur et la virtualisation

Lorsque le module est virtualisé il faut activer le mode promiscuité* pour que les clients puissent communiquer avec le serveur.

Virtualbox 3

Il suffit de lancer le serveur virtualisé et de passer l'interface en mode promiscuité.

Exemple si l'adresse est attaché au réseau sur l'interface `eth1` :

```
#ifconfig eth1 promisc ou ip link set eth1 promisc on
```

Virtualbox 4

Le serveur virtualisé doit être arrêté.

Choisir dans la configuration réseau le driver `e1000` et en cliquant sur avancé, choisir *Mode promiscuité* / *Autoriser tous*.

Il est possible de changer les paramètres dans la console :

```
VBoxManage setextradata <VBOX_NAME> "VBoxInternal/Devices/e1000/1/LUN#0/Config/IfPolicyPromisc" "allow-all"
```

Remplacer `<VBOX_NAME>` par le nom du serveur virtuel, la configuration ne concerne ici que l'interface `eth1`.

Plus d'informations : http://forums.virtualbox.org/viewtopic.php?f=7&t=41036

Démarrer le serveur virtuel et passer l'interface en mode promiscuité.

Exemple si l'adresse est attaché au réseau sur l'interface `eth1` :

```
# ifconfig eth1 promisc ou ip link set eth1 promisc on
```

VMWare

Vswitch de VMware ne prend pas en compte les adresses MAC additionnelles.

Pour contourner ce problème il faut passer le mode promiscuité du Vswitch à Enable dans ses propriétés.

Démarrer le serveur virtuel et passer l'interface en mode promiscuité.

Exemple si l'adresse est attaché au réseau sur l'interface `eth1` :

```
# ifconfig eth1 promisc ou ip link set eth1 promisc on
```

Forcer le "mode conteneur"

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

La procédure recommandée actuellement est la suivante :

- installer un module `Eolebase`
- mettre à jour la liste des paquets :

  [Maj-Auto -i] ou [Maj-Cd -i]
- installer le paquet eole-conteneur :

  [apt-eole install eole-conteneur]
- supprimer le fichier verrou du mode conteneur :

  [rm -f /etc/eole/.VirtDisabled.lock]
- installer le paquet "-pkg" du module souhaité (exemple : scribe-pkg, eclair-pkg) :

  [apt-eole install scribe-pkg]

Les mises à jour

Attention

Si vous avez installé un module (hors `EoleBase`) en *mode non conteneur*, il est fortement déconseillé de tenter de le faire passer en *mode conteneur*.

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

Le partitionnement doit également prendre en compte le fait que les conteneurs sont mis en place dans le répertoire `/opt/lxc`.

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

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

Mise à jour du module

Pour effectuer la mise à jour du module sans prendre en compte le fichier de configuration **config.eol**, utiliser la commande : [Maj-Auto -i]

Installation des conteneurs

La génération des conteneurs se fait à l'aide de la commande suivante :

[gen_conteneurs]

Des logs sont disponibles durant la génération des conteneurs dans le fichier **/var/log/isolation.log**

Remarque

Le fichier **/var/log/isolation.log** est supprimé après que la commande [gen_conteneurs] se soit correctement terminée. Il ne reste en place que si la procédure ne s'est pas déroulée correctement.

Par défaut, les conteneurs seront installés sur le réseau "**192.0.2.0/24**".

Si ce réseau est déjà utilisé dans votre architecture, il est possible de le changer.

Pour installer les conteneurs sur un réseau différent, il est impératif d'ajouter l'option `-n` à la commande [gen_conteneurs].

Par exemple :

[gen_conteneurs -n 192.168.10.0]

Le nouveau réseau défini ne doit pas être utilisé dans votre architecture (et surtout pas sur les adresses physiques du serveur).

Par contre, le masque sera obligatoirement 255.255.255.0.

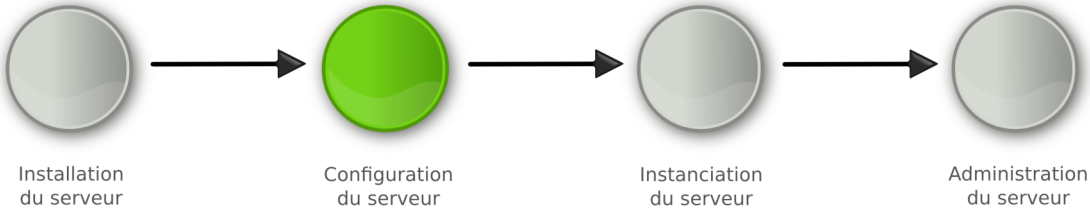
Attention

Attention, si vous utilisez cette fonctionnalité, les configurations générées sur Zéphir ne seront pas correctes (sur Zéphir, les adresses des différents conteneurs sont pré-calculées avec le réseau par défaut et ne sont pas modifiables dans l'interface).

Par conséquent : **n'utilisez pas cette option si vous comptez récupérer la configuration depuis un serveur Zéphir**.

VI Configuration

La deuxième des quatre phases



1 Configuration généralités

La configuration suit la phase d'installation du serveur.

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

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

À tout moment vous pouvez enregistrer la configuration pour l'effectuer en plusieurs temps.

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

Remarque

La configuration porte sur les paramètres propres à EOLE, mais également sur les paramètres des logiciels tiers contenus dans le module (ex : **squid.conf**).

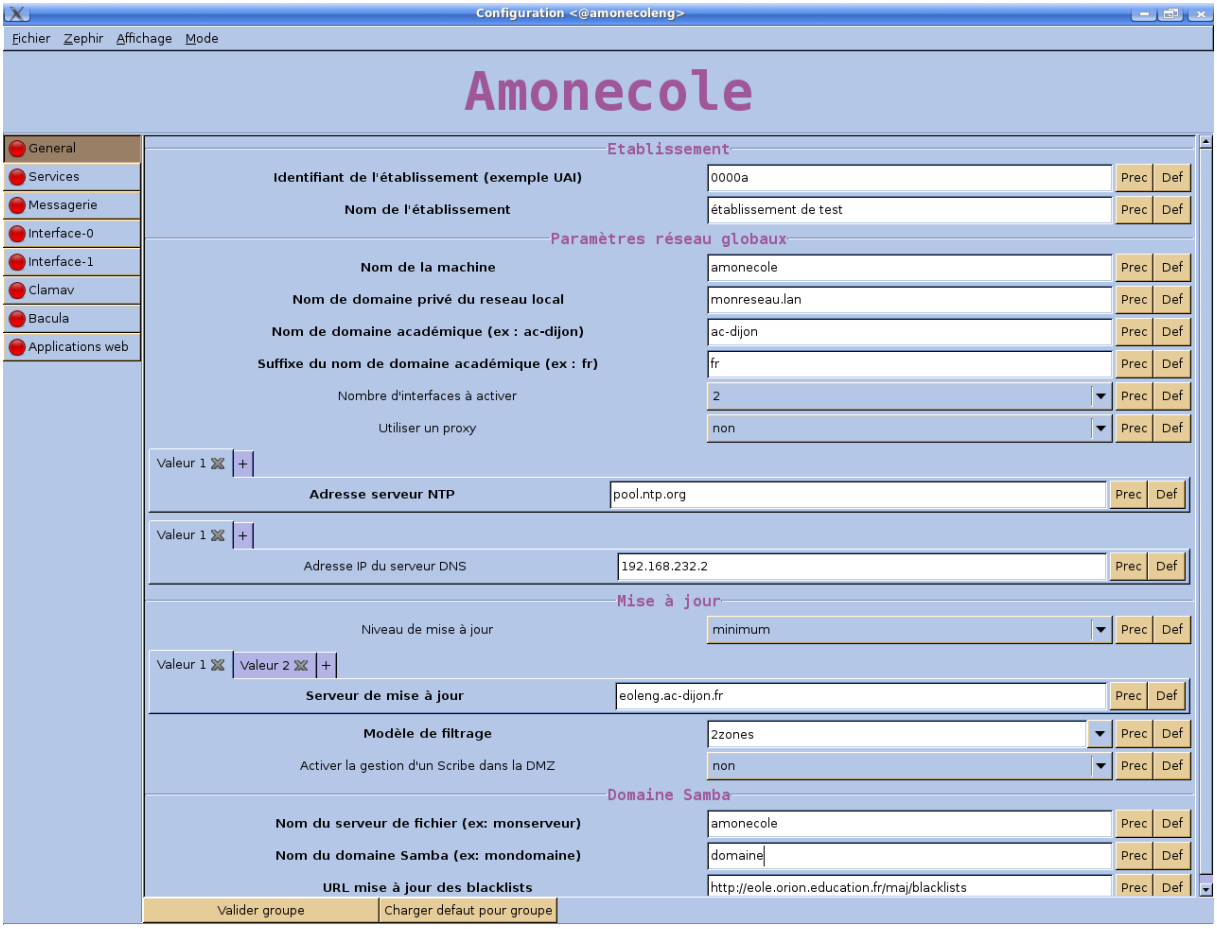
Il est possible de configurer le serveur en mode autonome par l'intermédiaire de l'outil [gen_config].

Au lancement, [gen_config] récupère dans les différents dictionnaires (**/usr/share/eole/creole/dicos**), les variables, leur valeur par défaut et les libellés qui seront affichés dans l'interface.

Mais il est également possible d'utiliser le mode Zéphir qui consiste à configurer le module avec l'application Zéphir depuis le module du même nom. Module qui permet de mettre en place un serveur de gestion de parc des serveurs EOLE. Par le mécanisme de variante, vous pouvez avoir des configurations pré-définies pour un ensemble de serveurs.

1.1. Interface de configuration du module

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



Elle se découpe en quatre zones :

- la zone *menu* ;
- la zone *formulaire* ;
- la zone *onglet* ;

- la zone *validation*.

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

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

1.1.1. La zone menu

Sous-menu Fichier

- *Ouvrir*

  Ce sous-menu permet d'ouvrir un fichier déjà enregistré sur le disque dur du serveur. Par défaut seuls les fichiers possédant l'extension *.eol* sont affichés.

- *Enregistrer*

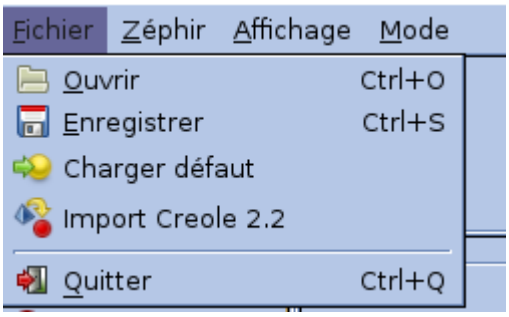
  Ce sous-menu permet d'enregistrer la configuration dans un fichier. Il est généré par défaut dans **/root** et s'appelle **zephir.eol**. Il est possible de donner un autre nom à ce fichier de configuration.

- *Charger défaut*

  Permet de charger les valeurs implicites des différents paramètres lorsqu'elles existent.

- *Import Creole2.2*

  L'importation d'un fichier de configuration de type EOLE 2.2 s'effectue en activant le menu Import Creole2.2. Le programme récupère les paramètres communs à EOLE 2.2 et à EOLE 2.3, il ne reste plus qu'à compléter les tableaux et enregistrer le fichier pour obtenir un fichier de configuration EOLE 2.3.



Sous-menu Zéphir

- *Connexion*

  Permet d'activer une connexion sur le serveur Zéphir, et ainsi de récupérer une configuration existante (renseigner l'adresse IP du serveur Zéphir ainsi que les login et mot de passe).

- *Choisir un serveur*

  La connexion avec le serveur Zéphir établie, il est possible de choisir le serveur sur lequel on doit récupérer la configuration.

- *Récupérer la configuration*

Permet de récupérer sur Zéphir un fichier de configuration déjà renseigné.

- *Envoyer la configuration*

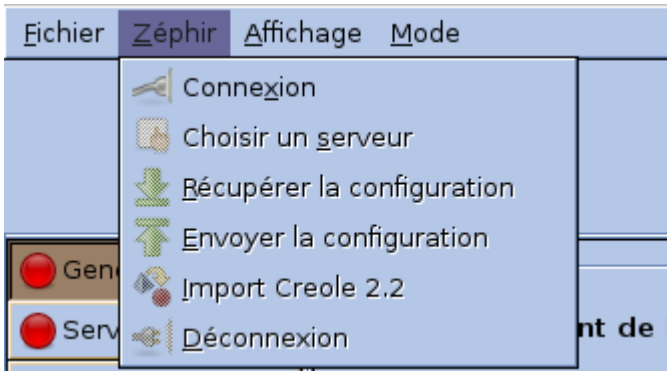
  Après saisie du fichier, permet d'envoyer celui-ci sur le Zéphir.

- *Import Creole 2.2*

  Permet de récupérer sur Zéphir un fichier de configuration de type EOLE 2.2.

- *Déconnexion*

  Ferme la connexion au serveur Zéphir.



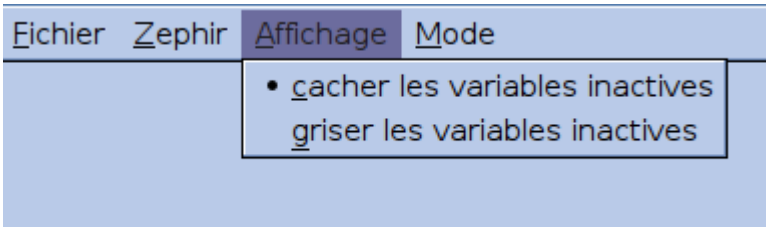
Sous-menu Affichage

- *cacher les variables inactives*

  Permet de cacher les variables inactives.

- *griser les variables inactives*

  Permet d'afficher en grisé les variables inactives.



Sous-menu Mode

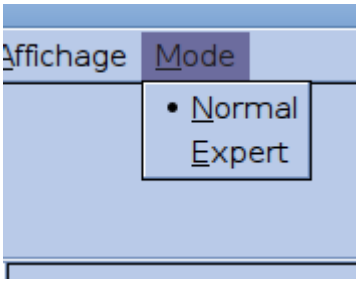
- *Normal :*

Ne présente que les onglets et variables standards (option par défaut).

- *Expert :*

Active les onglets, et variables du mode expert.

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



1.1.2. La zone formulaire

Présentation générale

Elle regroupe les paramètres de l'onglet activé.

Le bouton Prec récupère la valeur saisie précédemment.

Le bouton Def charge la valeur par défaut.

Regroupement des paramètres par bloc

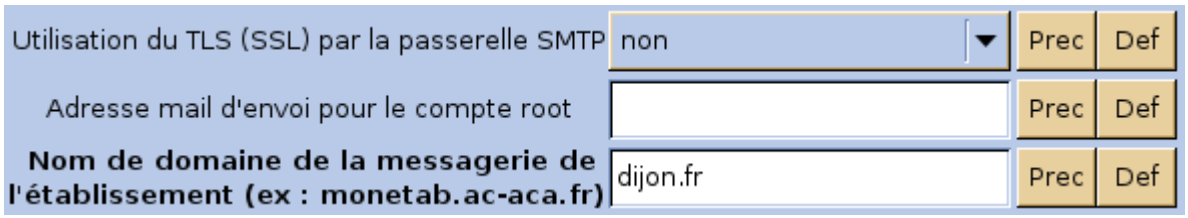
Les paramètres de chaque onglet sont répartis dans des blocs thématiques.

Chaque bloc regroupe un ou plusieurs paramètres.

Les variables obligatoires

Les variables obligatoires sont des variables pour lesquelles il est nécessaire de spécifier une valeur.

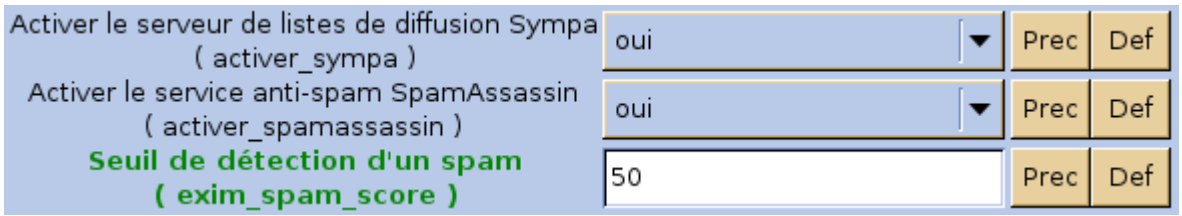
Leur libellé apparaît en gras dans l'interface.



Les variables expertes

Lorsque l'on passe en mode expert, un ensemble de nouvelles variables peuvent apparaître.

Ces variables sont identifiables à la couleur verte de leur libellé.



Les variables multiples

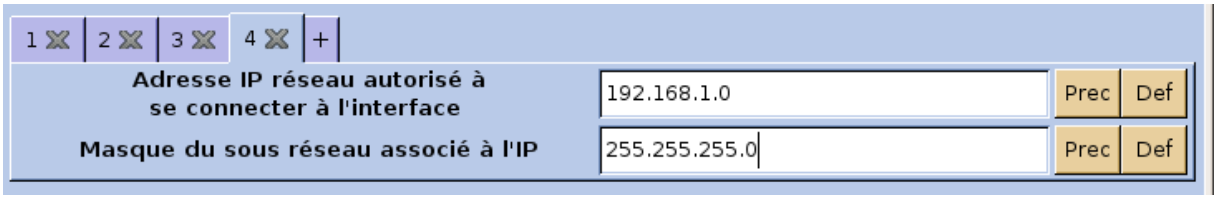
Certains paramétrages peuvent accueillir plusieurs valeurs. Nous parlons alors de variable multiple.

Ces variables multiples sont représentées sous forme d'onglet à l'intérieur de la zone de formulaire.

Pour supprimer une valeur, cliquer sur la croix à côté de l'onglet.

Pour ajouter un nouvel onglet, cliquer sur l'onglet [+].

Les valeurs de l'onglet courant seront alors reportées dans le nouvel onglet.

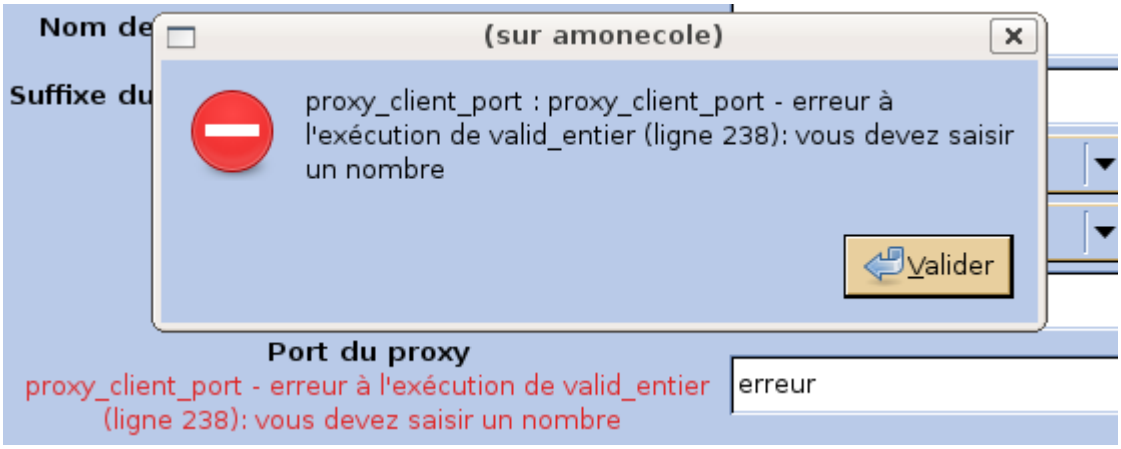


Validation des variables

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

Le cas le plus courant concerne les variables obligatoires. Si aucune valeur n'est spécifiée, une erreur avertira l'utilisateur.

Mais il existe de nombreuses autres vérifications : le type de valeur, leur construction (séparateur), etc.



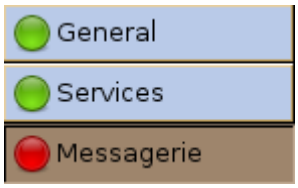
1.1.3. La zone onglet

Il existe trois types d'onglets :

- **les onglets de base**, présents systématiquement au lancement de l'outil [gen_config] ;
- **les onglets optionnels** présents si un paramètre du formulaire est activé. Exemple : si le paramètre DHCP est activé, l'onglet DHCP sera généré dynamiquement au même niveau que les onglets de base ;
- **les onglets experts** correspondent essentiellement au paramétrage de fichiers de configuration d'outils spécifiques. Ils sont disponibles si le mode « expert » est activé.

Les onglets non validés ont un marqueur rouge et les onglets validés ont un marqueur vert.

Les modifications dans les onglets non validés seront perdues lors de l'enregistrement des données.



Les onglets ajoutés par le passage en mode expert sont identifiables par le caractère * à la fin de leur libellé.

1.1.4. La zone validation

Cette zone permet de valider ou d'invalider, formulaire par formulaire, les modifications apportées sur celui-ci.

1.2. Interface de configuration console

Différentes situations peuvent empêcher d'utiliser l'interface graphique. Si le système détecte que son lancement n'est pas possible, il lance l'interface console.

Elle est également accessible directement par la commande [gen_config txt].

Liste des actions disponibles dans l'interface console :

- afficher l'aide de la console : taper [?] ;
- charger un fichier : taper [open], puis indiquer le nom du fichier **<fichier>.eol** ;
- lister les groupes de variables Créole : [showgroups] ;
- modifier des variables du groupe : [choosegroup] puis indiquer le numéro du groupe ;
- passer en mode expert : taper [expert] ([normal] pour en sortir) ;
- enregistrer la configuration : [save] ;
- quitter la console : [exit].

```
root@eolebase:~# gen_config txt
    ***************************
Outil de génération de la configuration
(tapez help ou ? pour la liste des commandes)
    ***************************
=>> choosegroup
0 : general
1 : services
2 : messagerie
3 : Interface-0
Choisissez un numéro : 2
Passerelle SMTP
[] : smtp.ac-acad.fr
Utilisation du TLS (SSL) par la passerelle SMTP (non, port 25, port 465)
[non] :
Adresse mail d'envoi pour le compte root
[] : amon@ac-acad.fr
Adresse mail de réception pour les comptes système
[postmaster] :

-- fin du groupe --
```

Remarque

Si vous sortez prématurément de la console ([Ctrl-D] ou [exit]), et qu'il y a eu des modifications, il vous est demandé de sauvegarder la configuration.

1.3. Configuration en mode autonome

La configuration en mode autonome signifie que la configuration est réalisée directement sur le serveur et qu'elle n'est pas centralisée avec l'application Zéphir.

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

Truc & astuce

La méthode autonome n'oblige pas à configurer exclusivement le module sur lequel est lancé l'interface de configuration du module. Il est possible de lancer l'interface de configuration du module (commande [gen_config]) sur un autre serveur (déjà en production par exemple),d'enregistrer le fichier, de le copier sur une clé USB et de l'utiliser pour *instancier* un nouveau serveur.

De cette manière, le fichier **<fichier>.eol** peut être préparé avant l'installation du serveur et peut être confié à une personne tierce, par exemple la personne chargée d'installer le serveur dans l'établissement. Celui-ci n'aura plus qu'à instancier le serveur.

1.4. Configuration en mode Zéphir

La configuration en mode Zéphir se fait en deux temps :

- il faut déjà créer le serveur au niveau académique sur le Zéphir, utiliser éventuellement un variante, le configurer, ... ;
- dans l'établissement, il ne reste qu'à enregistrer le serveur.

Cette procédure n'est pas obligatoirement dans cet ordre. Il est possible de configurer le serveur en mode autonome et d'enregistrer ensuite le serveur dans Zéphir.

La procédure d'enregistrement est requise pour tous les serveurs à administrer dans Zéphir. Elle permet de créer les données nécessaires dans la base de données et de configurer la transmission sécurisée entre Zéphir et le serveur. Cette tâche est obligatoire et doit être effectuée manuellement sur le module.

Pour enregistrer un serveur sur Zéphir, il faut utiliser la commande [enregistrement_zephir].

Truc & astuce

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

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

- le serveur doit être connecté au réseau pour pouvoir fonctionner voulez-vous établir une configuration réseau minimale (O/N), il est possible de configurer sommairement le réseau en répondant "oui" à la question ;
- entrer l'adresse du serveur Zéphir, ainsi qu'un nom d'utilisateur (et un mot de passe) autorisé en écriture dans l'application Zéphir ;

- si le serveur n'a pas été pré-créé sur le Zéphir, répondre "oui" à la question Créer le serveur dans la base Zéphir ? ;
- saisir ensuite les informations demandées (vous devez entrer un numéro RNE existant dans l'application Zéphir) ;
- choisir un numéro parmi les modules proposés ;
- même chose pour les variantes ;
- choisir enfin ce qu'on fait de la configuration :
  - si la configuration a été faite en mode autonome au préalable choisir Sauver la configuration actuelle sur Zephir,
  - si la configuration a été défini sur Zéphir choisir Récupérer les fichiers de variante sur Zéphir ;
- un message indiquera que la configuration est bien sauvegardée et que les communications avec Zéphir sont configurées. Dans le cas où des paramètres du serveur ne seraient pas renseignés (paramètres provenant d'une variante), un message vous préviendra que ceux-ci doivent être saisis.

Une fois la procédure terminée, lancer **`gen_config`**. Une fenêtre de login apparaît alors.

Elle permet de s'identifier sur le serveur Zéphir.

Remarque

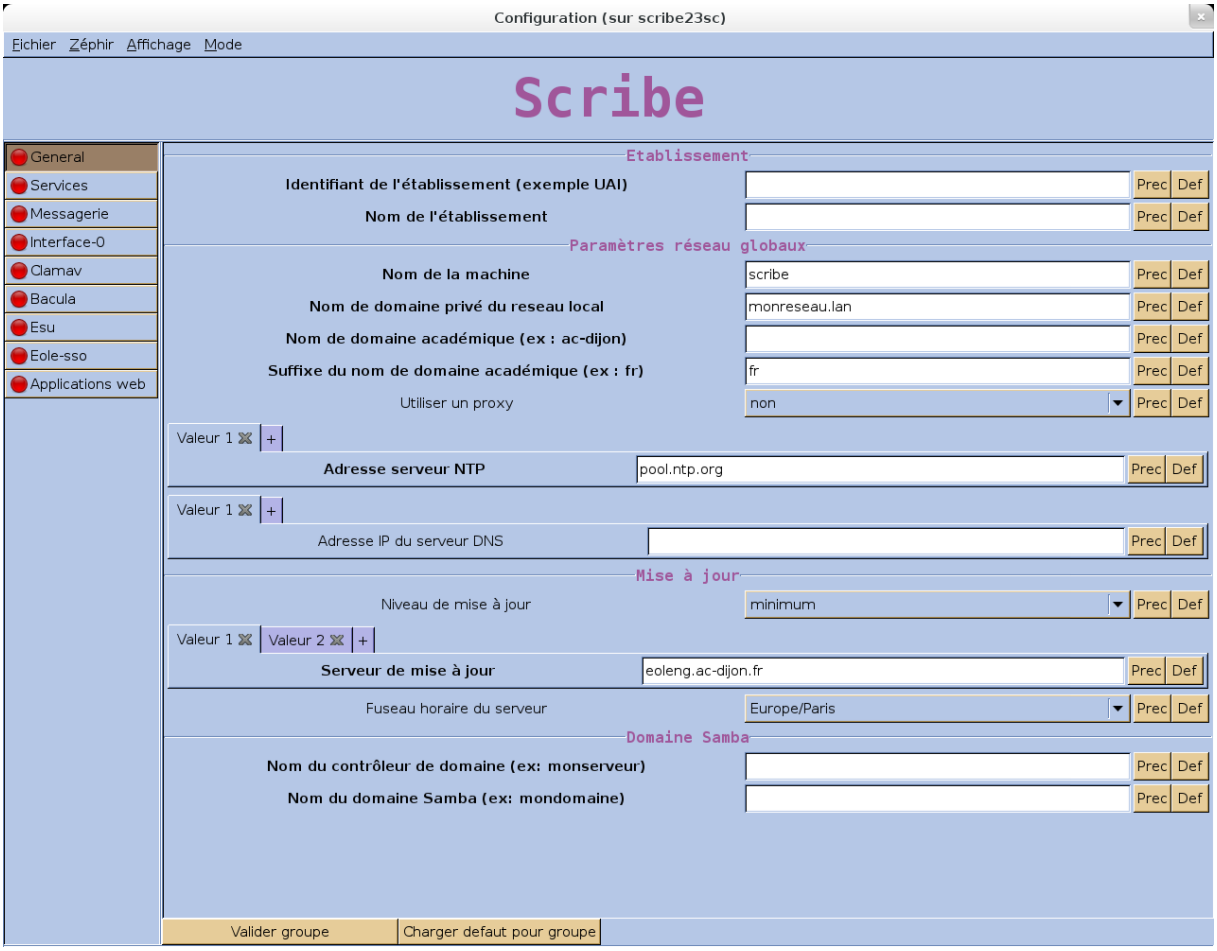
Un numéro vous sera indiqué (id du serveur). Ce numéro vous permettra d'accéder directement aux informations de ce serveur dans l'application Zéphir.

2 Configuration commune

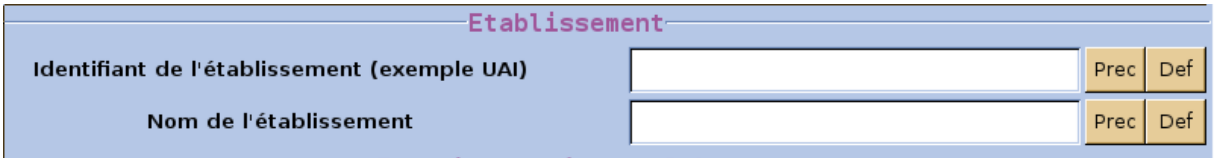
Une partie de la configuration se retrouve sur chacun des modules EOLE.

2.1. Onglet Général

Présentation des différents paramètres de l'onglet *`General`*.



Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

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

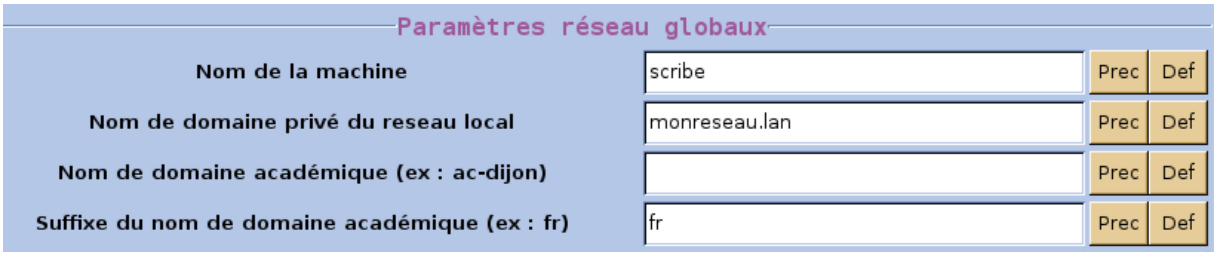
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP* local, ces variables sont utilisées pour créer l'arborescence.

Attention

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

Paramètres réseau globaux



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

Cette information est découpée en plusieurs champs :

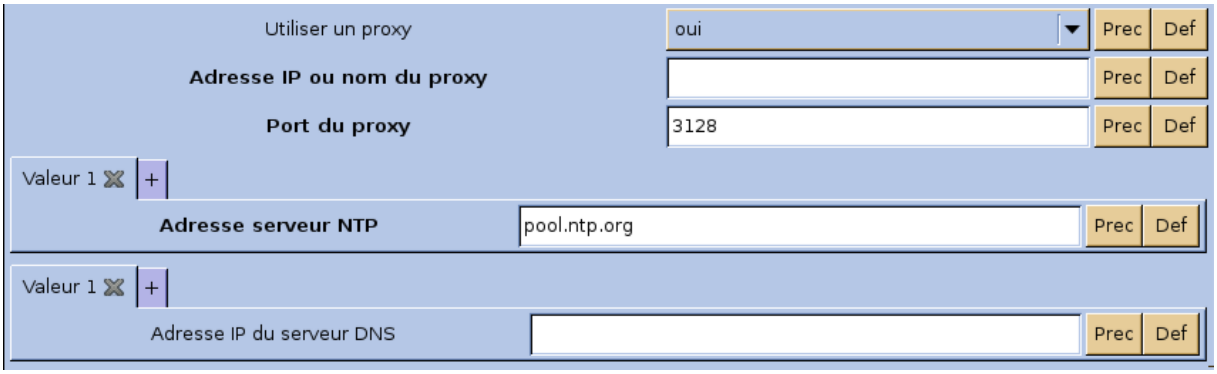
- le nom de la machine dans l'établissement ;
- le nom du domaine privé utilisé à l'intérieur de l'établissement ;
- le nom de domaine académique et son suffixe.

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 mais on utilise fréquemment le domaine de premier niveau .lan ou .local.

L'usage de ces autres domaines de premier niveau n'est pas recommandé, car il existe un risque de collision avec des domaines de premier niveau d'Internet, et donc de fragmentation du réseau.

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 LDAP.



Une suite de paramètres concerne la configuration réseau de la machine :

- l'adresse IP ou le nom de domaine du proxy ;

Pour renseigner la valeur de l'adresse ou du nom de domaine, il faut passer la variable **Utiliser un Proxy** à **oui**.

- adresse serveur du ou des serveur(s) de temps NTP* ;
- adresse IP du ou des serveur(s) de nom DNS*.

Mise à jour

Pour paramétrer les mises à jour, il faut au minimum choisir entre la mise à jour minimum et complète.

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

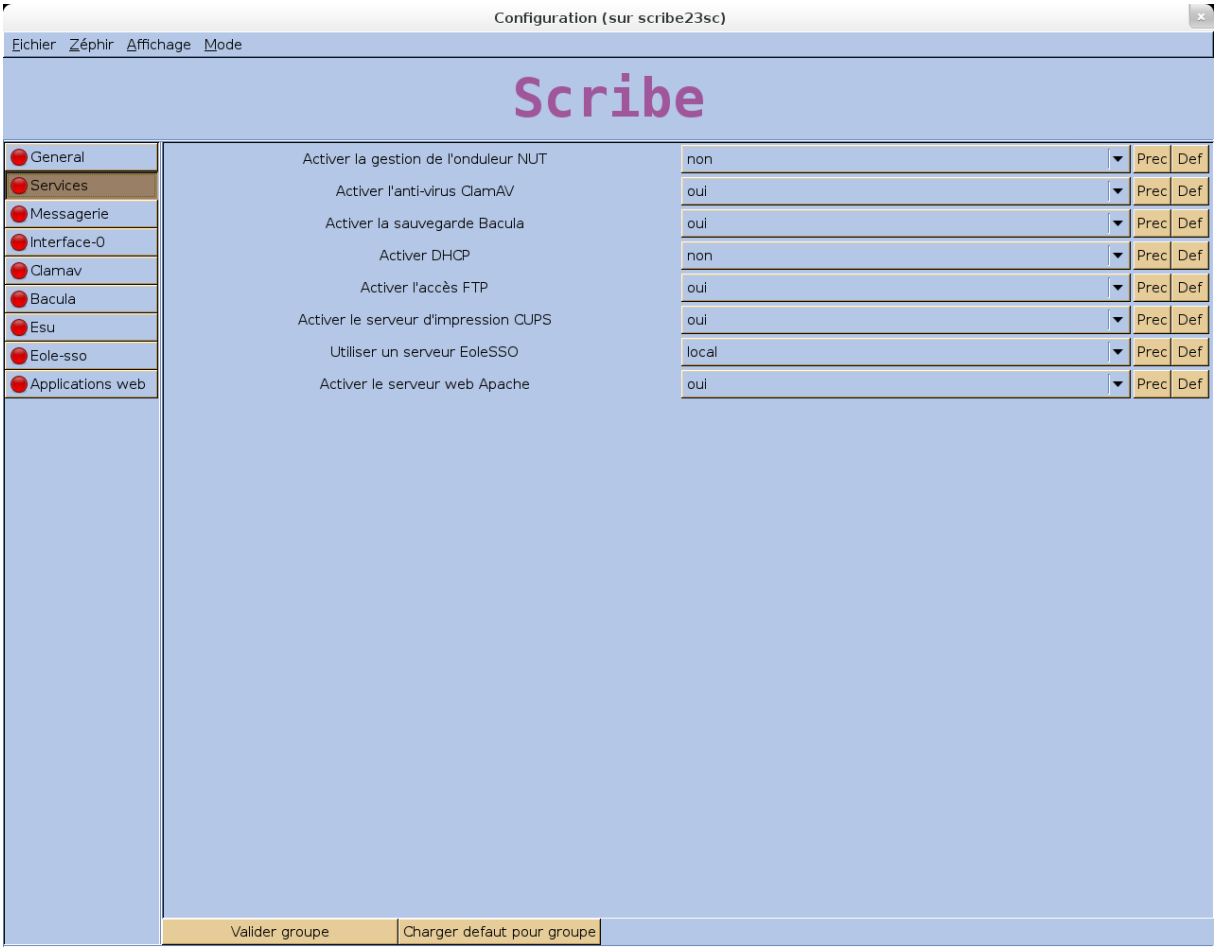
Les différentes mises à jour

Fuseau Horaire

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

2.2. Onglet Services

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



Les services de base communs à tous les modules sont les suivants :

- gestion de l'onduleur NUT* ;
- utilisation d'un serveur EoleSSO ;
- gestion des logs centralisés (mode expert) ;
- interface web de l'EAD (mode expert).

2.3. Onglet Messagerie

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

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

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

Les paramètres communs à renseigner sont les suivants :

Passerelle SMTP	Adresse IP ou nom DNS de la passerelle SMTP à utiliser.
Utilisation du TLS (SSL) par la passerelle SMTP	Permet de forcer l'utilisation du TLS.
Adresse mail d'envoi pour le compte root	Adresse de l'expéditeur : certaines passerelles n'acceptent que des adresses de leur domaine.
Adresse mail de réception pour les comptes système	Permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.

Remarque

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

2.4. Onglet Interface-x

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

Le nombre d'interfaces se défini dans l'onglet *Général* de l'interface de configuration du module.

Attention

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

Adresse de l'interface

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

Dans le cas de la configuration statique, l'adresse IP, le masque, l'adresse réseau et le broadcast vous seront demandés.

La configuration DHCP ne nécessite aucun paramétrage particulier.

En mode PPPoE, l'identifiant et le mot de passe de la connexion sont à renseigner.

Truc & astuce

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

Attention

Le PPPoE n'est disponible que pour le module Amon, AmonEcole et ses variantes.

Mode de connexion

Le paramètre "mode de connexion", en mode expert, 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 -> forcer la vitesse à 100Mbits/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- autoneg on -> activer l'auto-négociation (mode par défaut) :
- speed 10 duplex half autoneg off -> forcer la vitesse à 10Mbits/s en half duplex et désactiver l'auto-négociation ;
- speed 1000 duplex full autoneg off > forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.

Plus d'informations : http://fr.wikipedia.org/wiki/Auto-n%C3%A9gociation_%28ethernet%29.

Alias et VLAN

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 et configurer l'ensemble des paramètres utiles (l'adresse IP, ...).

Il est possible de configurer une passerelle particulière pour cet alias.

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

Pour cela, il faut activer son support et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

Il est possible de configurer une passerelle particulière pour ce VLAN.

Administration à distance

Par défaut les accès à ssh et aux interfaces d'administration (EAD, CUPS, ...) sont bloqués.

Pour chaque interface réseau activée (onglets *Interface-X*), 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.

Truc & astuce

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

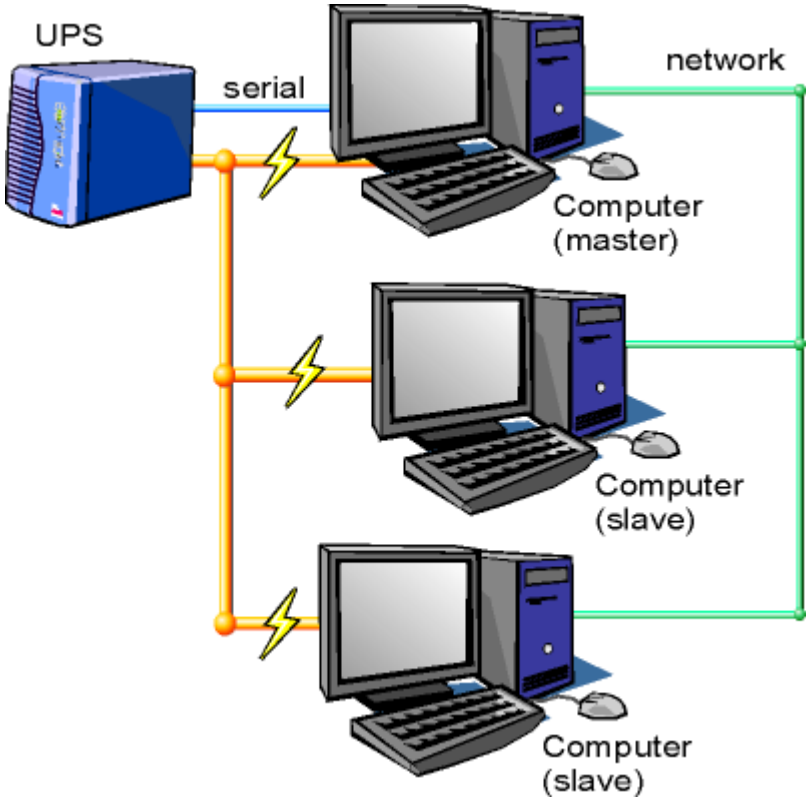
Complément

Des restrictions supplémentaires au niveau des connexions ssh sont disponibles dans l'onglet l'onglet expert : *Sshd*.

2.5. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT*. 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.



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

Truc & astuce

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

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

ou encore :

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

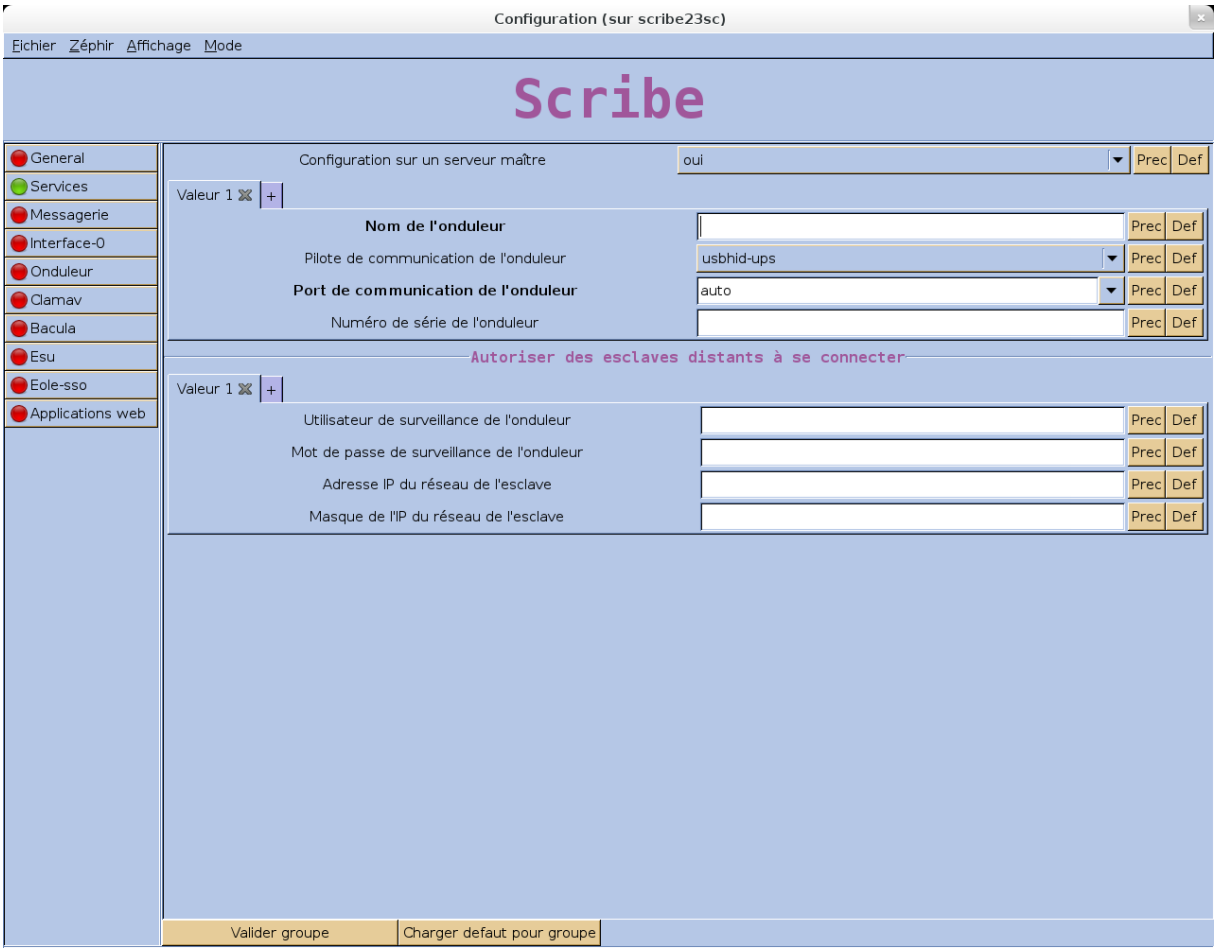
Si la version retournée est 2.4.3 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

http://www.networkupstools.org/source/2.4/new-2.4.3.txt

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

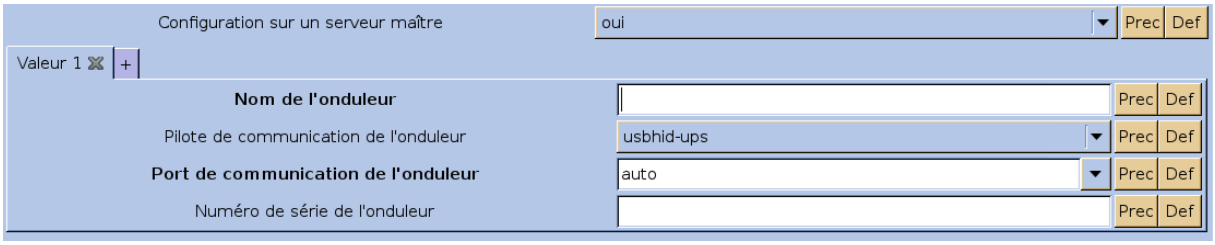
http://www.networkupstools.org/source/2.6/new-2.6.5.txt

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



Si l'onduleur est branché directement sur le module il faut laisser la variable **`Configuration sur un serveur maître`** à **`oui`** 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.

Le champ **Numéro de série de l'onduleur** est facultatif 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.

Remarque

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 à un onduleur différent.

Il faut cliquer sur + 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`.

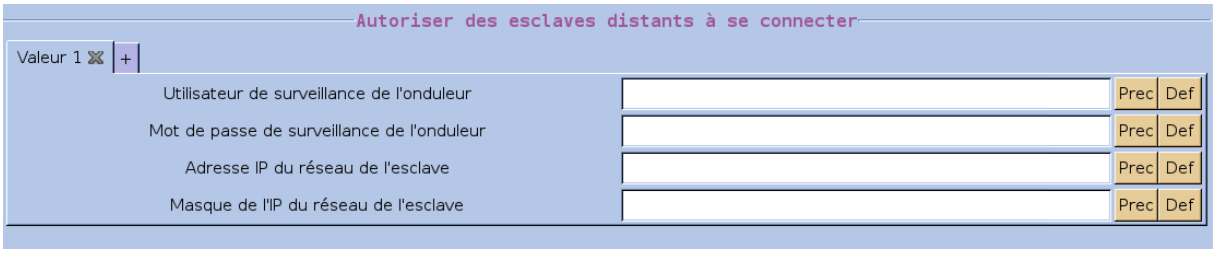
La majorité des onduleurs USB sont détectés automatiquement.

Attention

Attention, seul le premier onduleur sera surveillé.

Autoriser des esclaves distants à se connecter

Avant d'ajouter un serveur esclave il faut ajouter un utilisateur sur le serveur maître pour autoriser l'esclave a se connecter avec cet utilisateur.



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

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)

Remarque

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.

Attention

Chaque utilisateur doit avoir un nom différent.

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

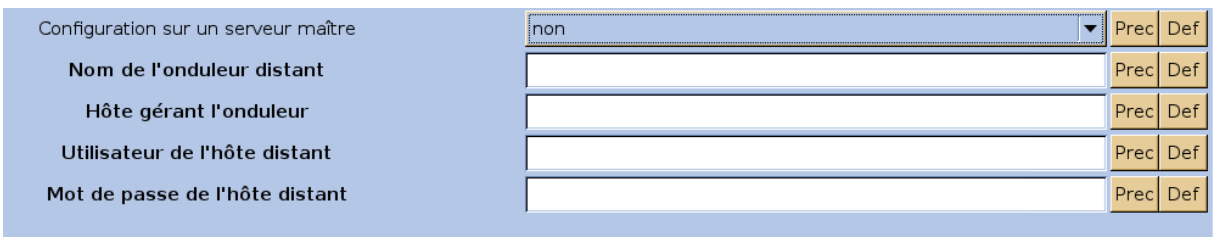
Complément

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

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il faut configurer le ou les serveurs esclaves. Après avoir activé le service dans l'onglet *Services*, il faut, 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

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 : **99JJUE2EZOAI2IZI1OIIZ93I187UZ8** ;
- 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 : **99JJUE2EZOAI2IZI1OIIZ93I187UZ8**.

3 Configuration commune avancée

Certains onglets déjà disponibles comportent de nouvelles variables.

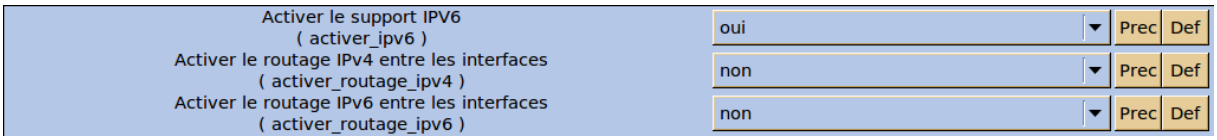
Certains onglets ne sont disponibles qu'après avoir activé le mode expert de l'interface de configuration du module.

3.1. Onglet Réseau avancé

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

La section **Ajout d'hôtes** n'est pas disponible dans cet onglet sur les modules Amon, AmonEcole, AmonHorus et AmonEcole+ mais dans l'onglet expert *Zones-dns*.

3.1.1. Configuration IP



Si la variable **Activer le support IPv6** est à **oui**, alors le support de l'IPv6* est activé au niveau du noyau.

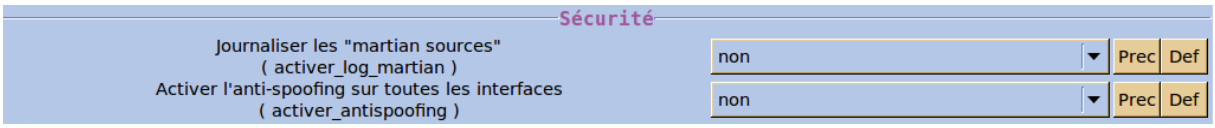
Cette variable est également utilisée pour désactiver explicitement le support de l'IPv6 dans la configuration de certains logiciels (Bind, Proftpd).

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** (une validation groupe peut s'avérer nécessaire).

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

3.1.2. Sécurité

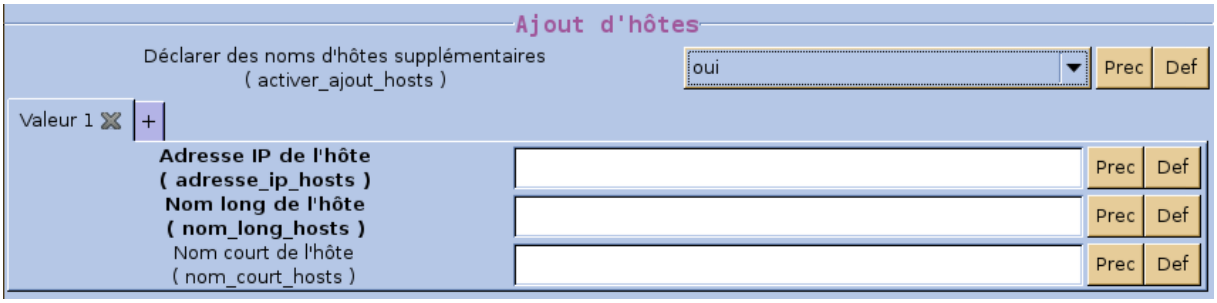


Si la variable **Journaliser les "martian sources"** est à **oui**, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.

Par défaut, l'anti-spoofing* est activé sur l'interface-0 des modules EOLE.

Il est possible de demander son activation sur les autres interfaces en passant la variable **Activer l'anti-spoofing sur toutes les interfaces** à **oui**.

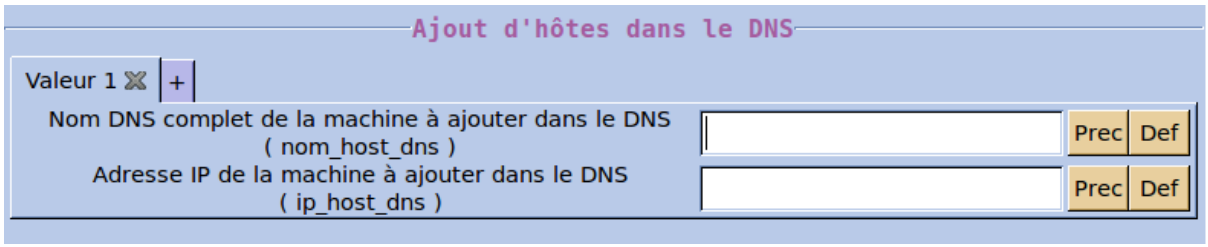
3.1.3. Ajout d'hôtes



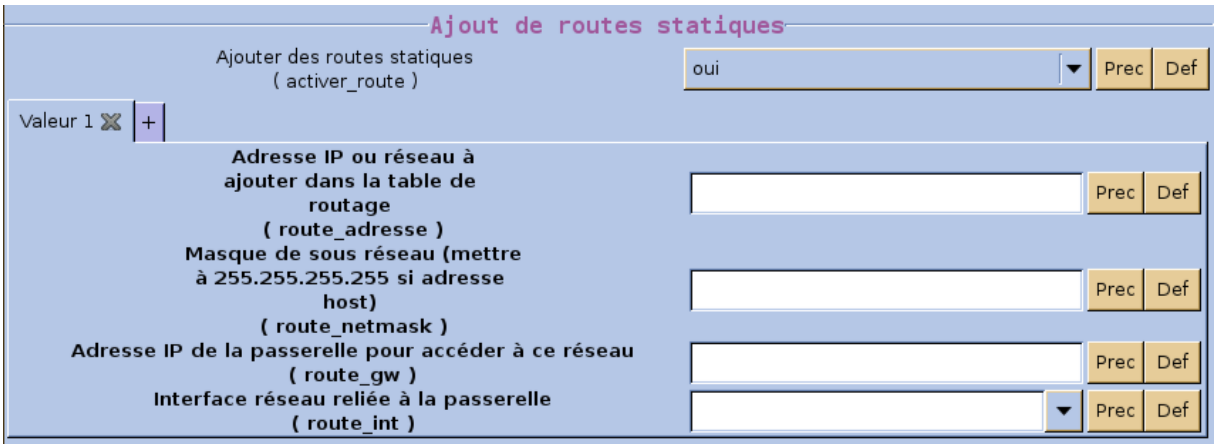
En passant la variable **Déclarer des noms d'hôtes supplémentaires** à **oui** il est possible de déclarer des noms d'hôtes qui seront ajoutés au fichier **/etc/hosts**.

Attention

La section **Ajout d'hôtes** n'est pas disponible dans cet onglet sur les modules Amon, AmonEcole, AmonHorus et AmonEcole+ mais dans l'onglet expert *Zones-dns*.



3.1.4. Ajout de routes statiques



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 que celui par défaut (défini par le routeur par défaut).

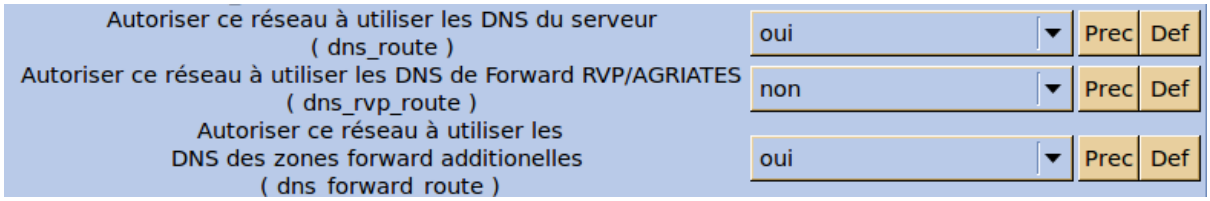
Après avoir passé la variable **Ajouter des routes statiques** à **oui** il faut ajouter les paramètres suivants :

- **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 (si cette valeur n'est pas renseignée à 0.0.0.0, alors la route se fera par l'interface) ;
- **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**).

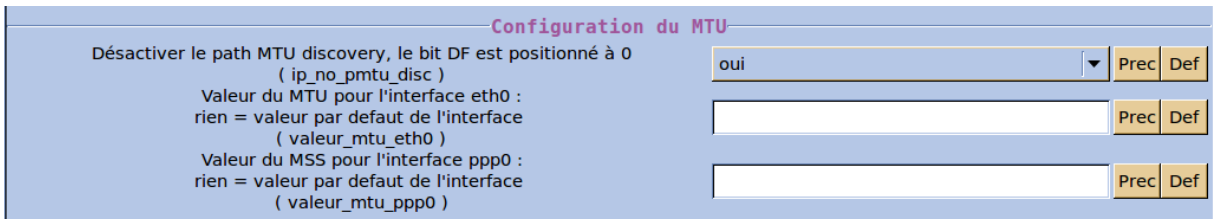
Remarque

Dans cet onglet sur les modules Amon, AmonEcole, AmonHorus et AmonEcole+, des champs supplémentaire sont disponibles pour autoriser chaque nouveau réseau déclaré dans les routes statiques à interroger le serveur DNS.



- **Autoriser ce réseau à utiliser les DNS du serveur** : autorise globalement ou non les requêtes DNS pour le réseau de la route renseignée.
- **Autoriser ce réseau à utiliser les DNS de Forward RVP/AGRIATES** : Si le service RVP est activé (onglet *Services*) et que le serveur est membre du réseau AGRIATES (onglet *Rvp*) la variable est disponible pour autoriser ou non le réseau de la route renseignée à résoudre les noms d'hôte de la zone AGRIATES.
- **Autoriser ce réseau à utiliser les DNS des zones forward additionnelles** : permet d'autoriser le réseau de la route renseignée à résoudre les noms d'hôte des domaines déclarés dans la section **Forward de zone DNS** de l'onglet *Zones-dns*.

3.1.5. Configuration du MTU



La variable **Désactiver le path MTU discovery** permet d'activer ou non le path MTU discovery* (/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* de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

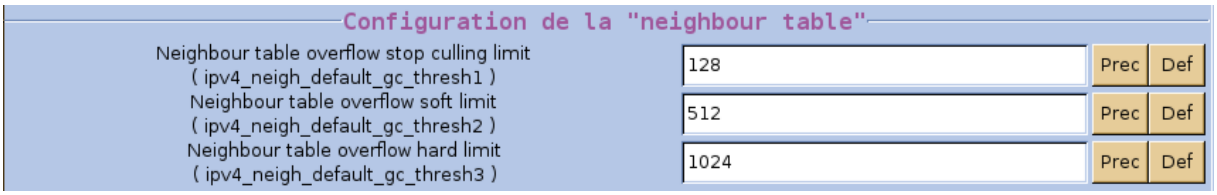
Un des phénomène permettant de diagnostiquer un problème lié au PMTU discovery est que l'accès à certains sites (ou certaines pages d'un site) n'aboutit pas (la page reste blanche) ou que les courriels n'arrivent pas dans le client messagerie.

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* pour l'interface externe.

- Si le champ n'est pas renseigné, la valeur par défaut 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* (module Amon, AmonEcole et ses variantes) et que vous souhaitez forcer une valeur de MSS* différente, il faut renseigner le second champ : **Valeur du MSS pour l'interface ppp0**.

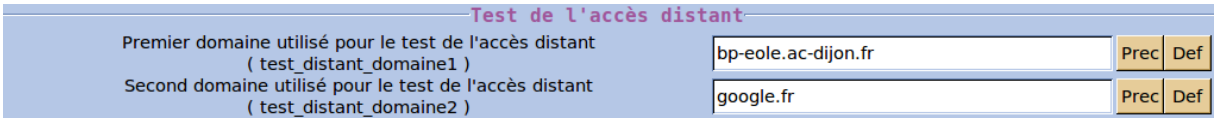
3.1.6. Configuration de la "neighbour table"



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

- gc_thresh1 : stop culling limit, once you drop to this point stop culling ;
- gc_thresh2 : soft limit, if you pass this limit start culling crud ;
- gc_thresh3 : hard limit, limite dure, is a hard limit, don't ever grow past this limit.

3.1.7. Test de l'accès distant



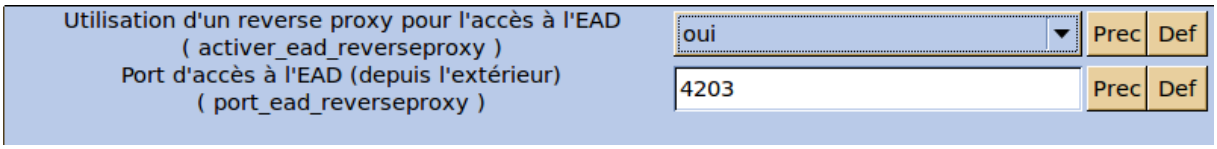
Les deux variables permettent de définir les domaines qui sont utilisés lorsque le module EOLE a besoin de tester son accès à Internet.

En pratique, seul l'accès au premier domaine est testé sauf dans le cas où il n'est pas accessible.

Les domaines définis sont utilisées dans les outils [diagnose] et dans l'agent Zéphir.

3.2. EAD et proxy inverse

Si l'interface web de l'EAD est activée sur le module, les paramètres de l'onglet *Ead-web* (mode expert) 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.

3.3. Configuration système

Les paramètres de l'onglet *Systeme* (mode expert) 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 déactiver cette fonctionnalité.

Validation des mots de passe

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

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

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

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

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

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

Attention

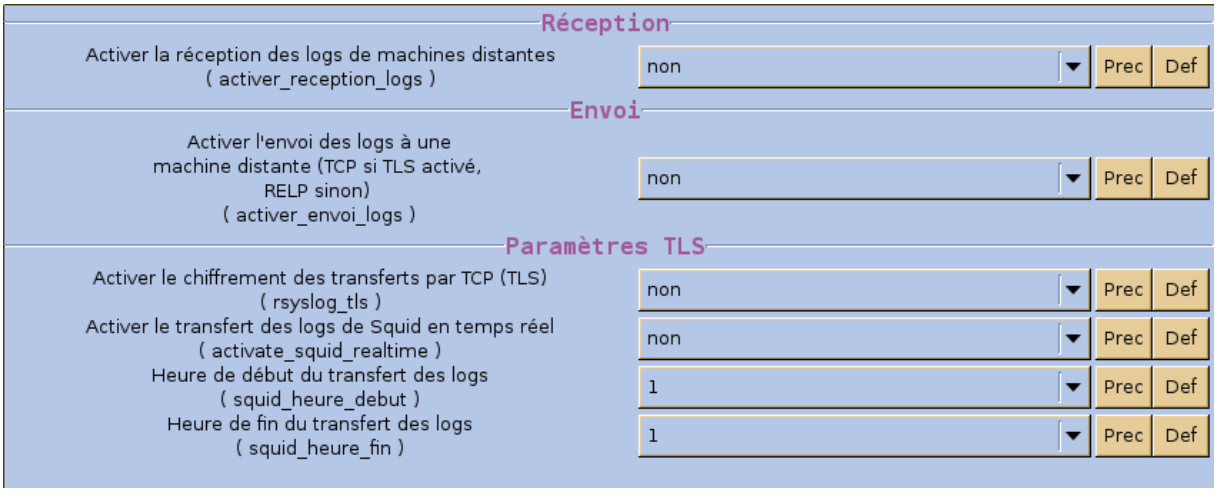
Ce paramétrage ne concerne que les comptes locaux. Les utilisateurs LDAP ne sont pas soumis aux mêmes restrictions.

> "cf Les mots de passe", page 130.

3.4. Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog.

Le support des logs centralisés peut être activé dans l'onglet *Service* en mode expert. Cette activation affiche 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 utilisé est contraint par l'activation ou non du chiffrement ;
- la configuration du chiffrement comprend les emplacements des certificats et de l'autorité de certification.

3.5. 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 Certifs-ssl de l'interface de configuration du serveur (mode expert) :

- **`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).

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.

Afin d'éviter des problèmes de compatibilité avec certaines applications, les certificats doivent être au format *PEM* . Dans le cas contraire, vous pouvez les convertir à l'aide de la commande **openssl**.

Conversion d'un certificat au format *DER* :

```
# openssl x509 -inform DER -outform PEM -in /etc/ssl/certs/mon_certif.der
-out /etc/ssl/certs/mon_certif.pem
```

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**.

L'IGC fournis un fichier qui certifie les mêmes services que le fichier **/etc/ssl/certs/eole.crt**.

Il faut créer un nouveau fichier **nom-etab.crt** dans **/etc/ssl/certs/** avec ce que fournis l'IGC.

Pour identifier correctement le certificat fournit par l'autorité il est recommandé de le renommer, par exemple en utilisant le nom de l'établissement et l'extension `.crt`.

Exemple : **/etc/ssl/certs/mon-etab.crt**

Le fichier **/etc/ssl/certs/eole.key** doit être renommé pour porter le même nom de fichier que le certificat.

Exemple : **/etc/ssl/certs/mon-etab.key**

Pour la prise en charge du nouveau certificat il faut renseigner l'interface de configuration du module.

Les chemins du certificat **/etc/ssl/certs/mon-etab.crt** et de la clé privée **/etc/ssl/certs/mon-etab.key** doivent être renseignés dans les onglets *`Certifs-ssl`* et *`Eole-sso`*.

Attention

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

Attention l'IGC signe les certificats avec l'ACInfraEducation et non avec la racine, mais certains navigateurs ne disposent que de la racine ce qui fait qu'ils considèrent votre certificat comme non valide même lorsqu'il viens de l'IGC.

Pour palier au problème il faut concaténer le fichier **/etc/ssl/certs/ACInfraEducation.pem** dans votre tout nouveau certificat **/etc/ssl/certs/mone-etab.crt**.

Attention ce fichier doit être un fichier de type "Unix" et toujours édité en mode binaire il ne doit pas contenir de `\n` sur la dernière ligne.

Exemple d'édition avec `vim`, utilisez les commandes suivantes :

```
:set binary
```

```
:set noeol
```

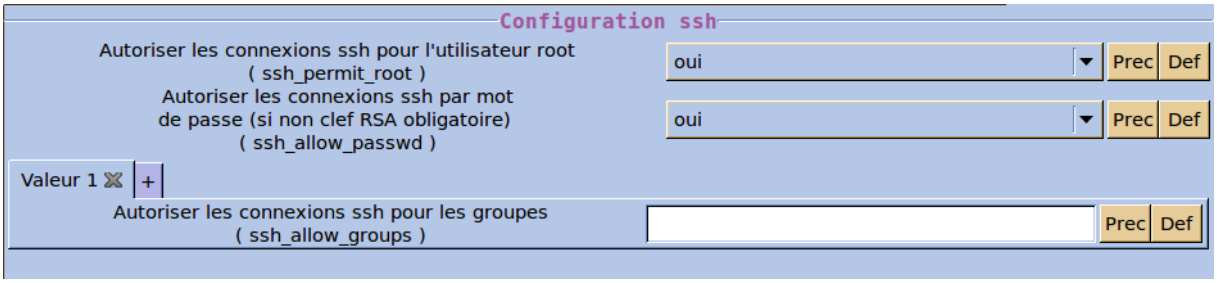
Puis sauvegarder votre fichier avec la commande :

```
:x
```

Utilisation d'un certificat signé par une autorité

Il faut suivre la même démarche que pour le certificat signé par l'IGC de l'Éducation Nationale (ci-dessus), en copiant la chaîne de l'autorité de certification dans le certificat si elle n'y est pas déjà. Il faut également copier cette chaîne dans le répertoire **/etc/ssl/local_ca** avec une extension `.pem` ou `.crt` pour qu'elle soit ajoutée au fichier `ca.crt` du serveur (cette action est réalisée automatiquement au reconfigure).

3.6. Gestion SSH avancée



Les paramètres disponibles dans l'onglet *Sshd* 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-X*).

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.

Remarque

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).
```

Complément

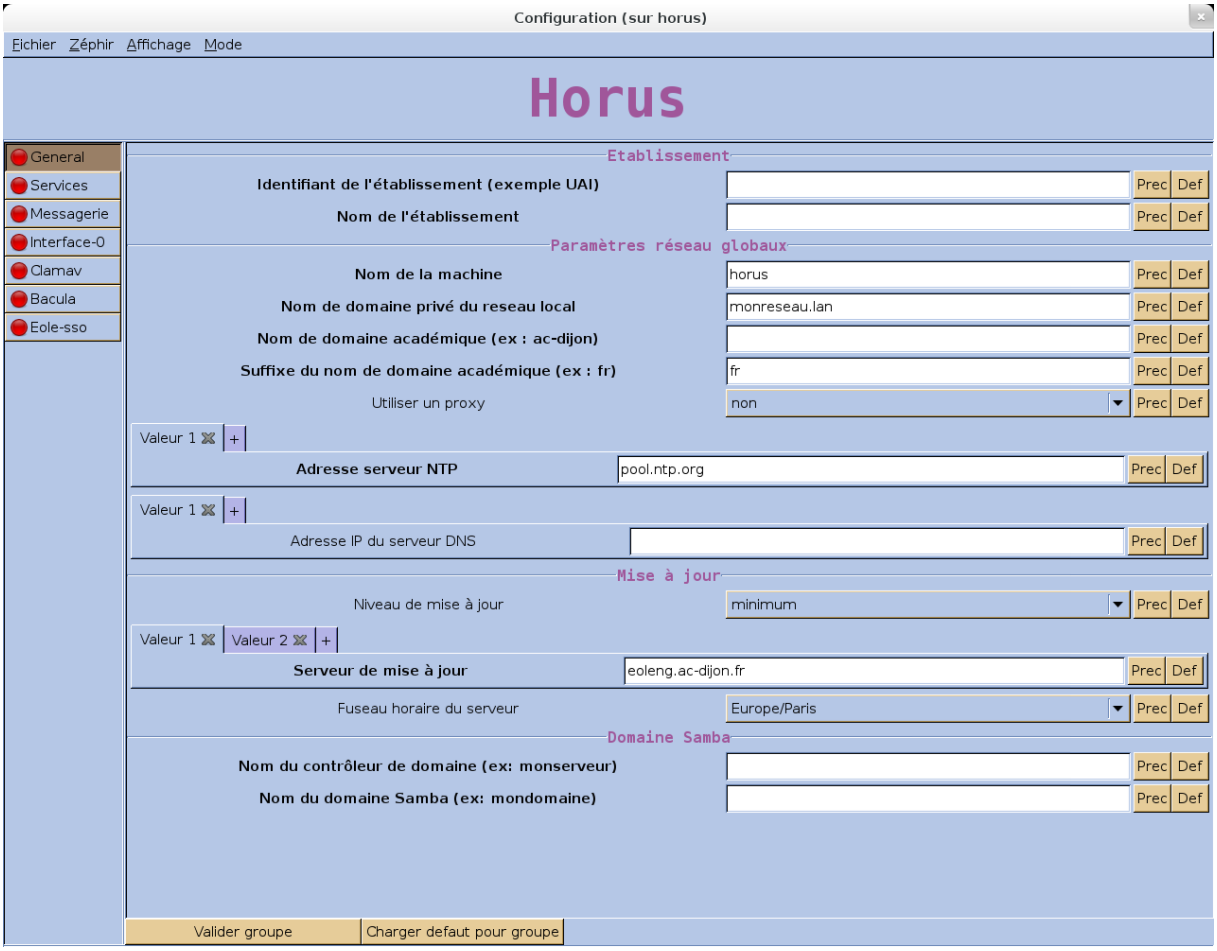
Par défaut les groupes Unix autorisés sont `root` et `adm`.

VII Configuration du module Horus

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

- *General*;
- *Services* ;
- *Messagerie* ;
- *Interface-0* (configuration de l'interface réseau) ;
- *Mots de passe* ;
- *Clamav* (configuration de l'anti-virus) ;
- *Bacula* ;
- *Esu* (*);
- *Eole-sso* ;
- *Applications web* (*).

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



1 Configuration du contrôleur de domaine

EOLE propose un contrôleur de domaine principal (PDC*) 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.).

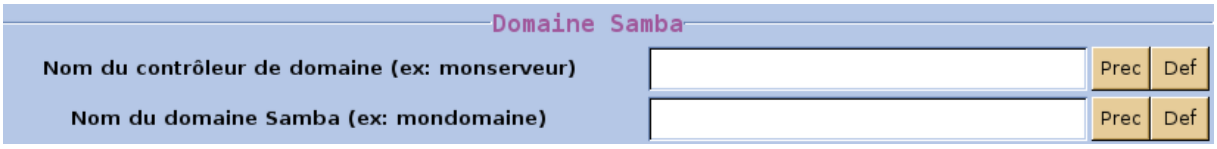
Les droits d'accès sont différents suivant les groupes auxquels l'utilisateur appartient.

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 *General* de l'interface de configuration du module.

Domaine Samba



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

Attention

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

En mode conteneur (module AmonEcole et ses variantes), il doit impérativement être différent du **Nom de la machine**.

Le champ **Nom du domaine Samba** (le nom de domaine NetBIOS), est aussi appelé groupe de travail (workgroup), il est à utiliser lors de l'intégration d'une station au domaine.

Attention

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

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

Complément

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

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

Anti-virus temps réel

Afin de limiter la propagation des virus à travers le réseau, il est possible d'activer une surveillance anti-virus temps réel sur les partages.

La surveillance s'active en passant la variable **Activer l'anti-virus temps réel sur SMB** à **oui** dans l'onglet *Clamav* de l'interface de configuration du module.

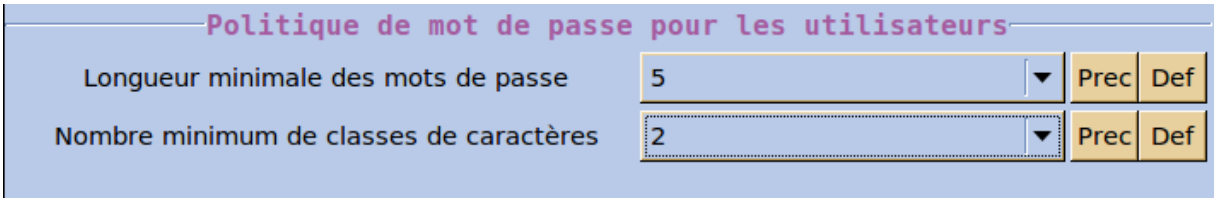
Attention cet onglet n'est plus visible si vous avez désactivé le service **Activer l'anti-virus Clamav** dans l'onglet *Services*.

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

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

Configuration de l'anti-virus

2 Politique de mot de passe pour les utilisateurs



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 mélanger les classes de caractères qui composeront les mots de passe. Il est possible de choisir de 1 à 4 classes différentes.

Attention

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

3 Configuration de l'anti-virus

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

Activation de l'anti-virus

Par défaut le service est activé sur le module et l'anti-virus est actif sur tous les services.

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

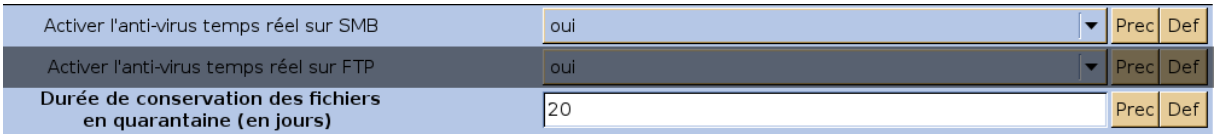
- le service SMB ;
- le service FTP.

Truc & astuce

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

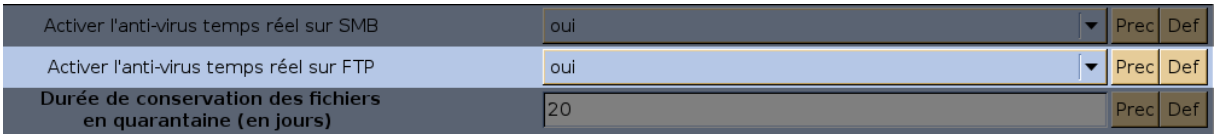
Le service est activé par défaut il est possible de le désactiver en passant la variable **Activer l'anti-virus temps réel sur SMB** à **non** dans l'onglet *Clamav*.



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.

Activation de l'anti-virus sur FTP

Pour activer 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 SMB** à **oui** dans l'onglet *Clamav*.



Contribuer

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

Il est possible de faire des signalements :

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

Pour cela il faut utiliser le formulaire suivant (en) : http://cgi.clamav.net/sendvirus.cgi

L'équipe de soutien à la base de données de virus examinera votre demande et mettre 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.

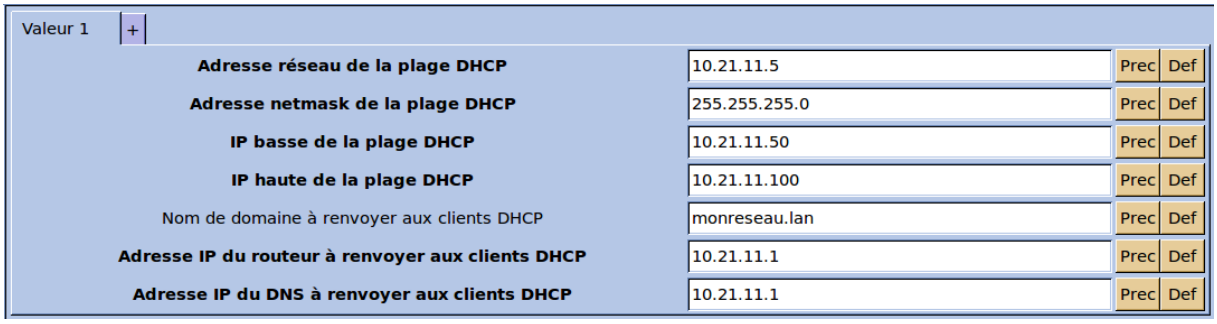
Attention

Il ne faut pas signaler des PUA* comme étant des faux positifs.

4 Configuration du serveur DHCP

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

L'onglet *Dhcp* apparaît uniquement si il est activé.



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

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

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

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.

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

- dans le mode 1 carte l'adresse sera l'adresse IP de la passerelle saisie dans l'onglet **Interface-0** ;
- dans le cas du mode 2 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 de votre FAI* pour une utilisation sans le module Amon.

Si vous disposez d'un module Amon ou d'un module AmonEcole il est préférable de l'utiliser comme relais DNS*.

Il est également possible d'utiliser des serveurs DNS disponibles sur Internet.

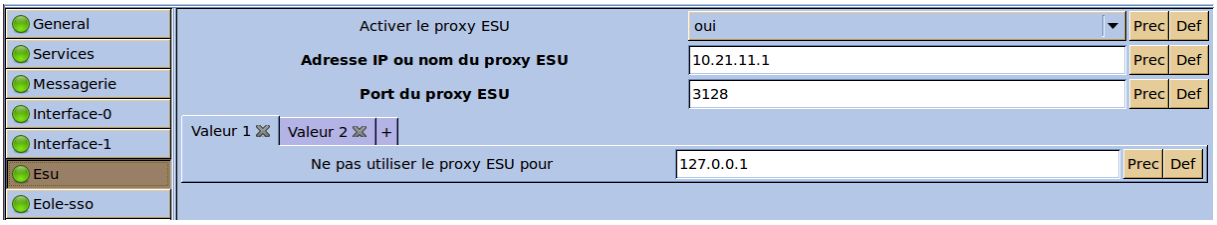
Truc & astuce

Sur le module AmonEcole, l'adresse IP du DNS à renvoyer correspond à celle renseignée dans **adresse_ip_eth1_proxy_link** (onglet *Interface-1*)

5 Configuration du proxy ESU

Sur les modules Scribe, AmonEcole et AmonEcole+, l'utilisation du couple ESU/clientScribe est obligatoire pour les stations Microsoft rattachées au domaine et l'onglet *Esu* est visible.

Sur les autres modules, l'outil ESU est activable/désactivable dans l'onglet *Services* par l'intermédiaire de l'option : **Utiliser le logiciel ESU** et l'onglet *Esu* n'apparaît que si le service est activé.



Sur les versions 2.2 et antérieures, la configuration manuelle d'un proxy dans ESU se retrouvait systématiquement écrasée par la commande [reconfigure] et la mise en place d'un patch EOLE était obligatoire pour conserver cette configuration.

Afin d'éviter cette manipulation, la configuration du proxy pour des stations clientes gérées par ESU s'effectue désormais au niveau de l'interface de configuration du module.

Pour cela il faut se rendre dans l'onglet *Esu* et passer la variable **Activer le proxy ESU** à **oui**.

Il faut ensuite saisir l'adresse IP ou le nom du proxy ESU et si besoin changer le port proposé par défaut.

En cliquant sur le bouton +, il est également possible de spécifier des adresses IP, des réseaux, des noms de domaine et des noms de machines pour lesquels le proxy ESU ne sera pas utilisé (exemple de valeur : mozilla.org, asso.fr, 192.168.1.0/24).

Truc & astuce

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

Remarque

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

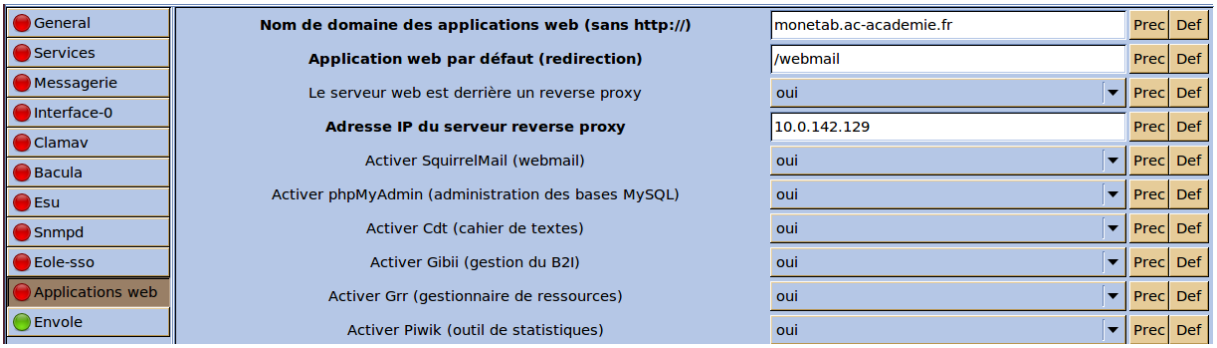
Pour récupérer une station utilisable hors du domaine, vous pouvez :

- ré-activer ESU, renseigner les options telles qu'elles sont sur un Windows par défaut (cases décochées), ouvrir une session et désactiver ESU ;
- modifier la base de registre de la station, en appliquant des fichiers .REG* tels que ceux fournis par l'archive suivante : ftp://eoleng.ac-dijon.fr/pub/Outils/Scribe/BureauMenuDem.zip

6 Configuration des applications web

Le serveur web apache est activable/désactivable dans l'onglet *Services* par l'intermédiaire de l'option : **Activer le serveur web Apache**.

L'onglet *Applications web* et l'onglet expert *Apache* sont disponibles uniquement si il est activé.



L'onglet *Applications web* permet de régler les paramètres essentiels du serveur web et d'activer/désactiver les applications web EOLE installées sur le module.

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 Scribe, il est fortement recommandé d'utiliser un nom de domaine.

Truc & astuce

Le paramétrage de l'application web par défaut dépend de l'activation du portail Envole :

- Si le portail Envole n'est pas activé ou que la variable de l'onglet *Envole* : **Utiliser Envole comme application par défaut en frontal** est à **non**, l'application web par défaut sera celle renseignée dans la variable de l'onglet *Applications web* : **Application web par défaut (redirection)**. Exemple : Si la variable **Application web par défaut** vaut **/webmail**, alors l'adresse **http://<adresse_serveur>/** pointera vers **http://<adresse_serveur>/webmail/** (SquirrelMail).
- Si le portail Envole est activé et que la variable de l'onglet *Envole* : **Utiliser Envole comme application par défaut en frontal** est à **oui**, l'adresse **http://<adresse_serveur>/** renverra vers le portail.

Toute modification nécessitera une reconfiguration du serveur avec la commande [reconfigure].

VIII Configuration avancée du module Horus

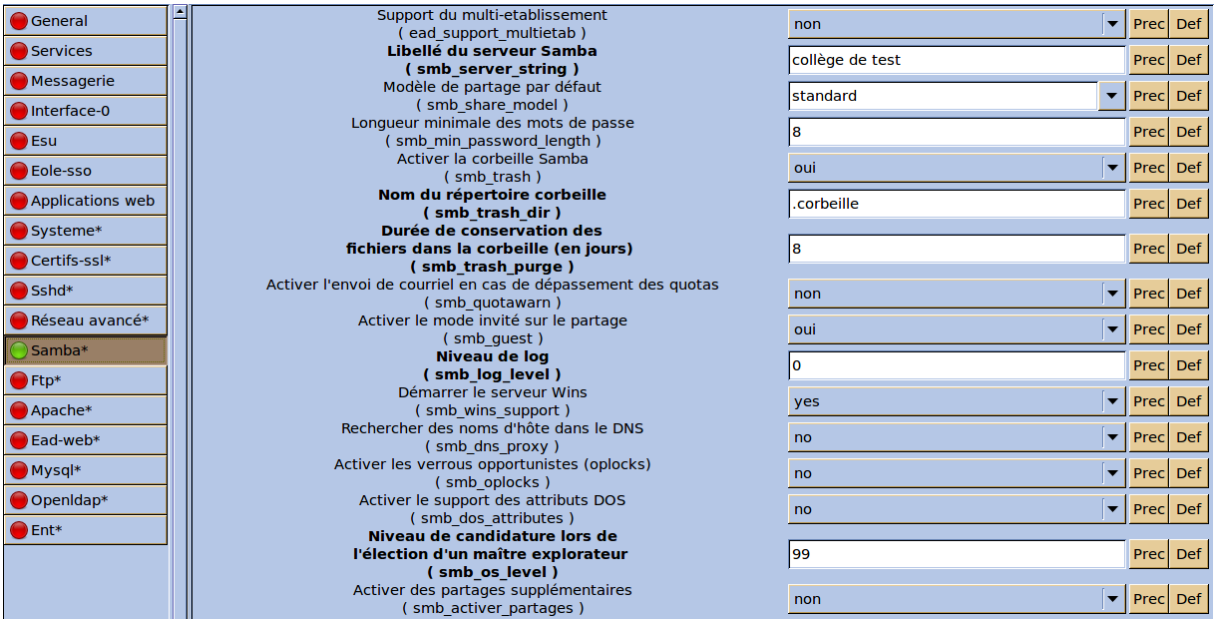
Certains onglets déjà disponibles comportent de nouvelles variables.

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

- *Samba** (configuration avancée du contrôleur de domaine) ;
- *Cups** (configuration avancée du serveur d'impressions) ;
- *Ftp** (configuration avancée du serveur FTP) ;
- *Apache** (configuration avancée du serveur web) ;
- *Mysql** (configuration avancée du serveur de bases de données) ;
- *OpenLdap** (configuration avancée du service d'annuaire) ;
- *Tftp* (onglet visible après activation du service dans l'onglet *Services* en mode expert).

1 Configuration avancée du contrôleur de domaine

La configuration avancée est accessible dans l'interface de configuration du module, en mode expert, dans l'onglet *Samba*.



Multi-Établissement

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

Passer la variable à `oui` pour activer le support du multi-Établissement.

En savoir plus sur le mode Multi-Établissement

Libellé

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

Modèle de partage par défaut

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

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

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

Il existe déjà plusieurs modèles à disposition :

- standard

  héritage des permissions, accès en écriture, accès autorisé uniquement aux membres du groupe
- commun

  héritage des permissions, accès en écriture, accessible à tous en lecture et en écriture, accès anonyme (guest)
- devoirs

héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture

- groupes

  héritage des permissions, accès en écriture, accessible à tous les utilisateurs authentifiés en lecture et en écriture

- icones$

  caché dans le voisinage réseau, accès anonyme (guest)

- minedu

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

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.

Remarque

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.

Démarrer le serveur Wins

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

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

Rechercher des noms d'hôte dans le DNS

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

Option à **non** par défaut.

Activer les verrous opportunistes (oplocks)

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

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

Activer le support des attributs DOS

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

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

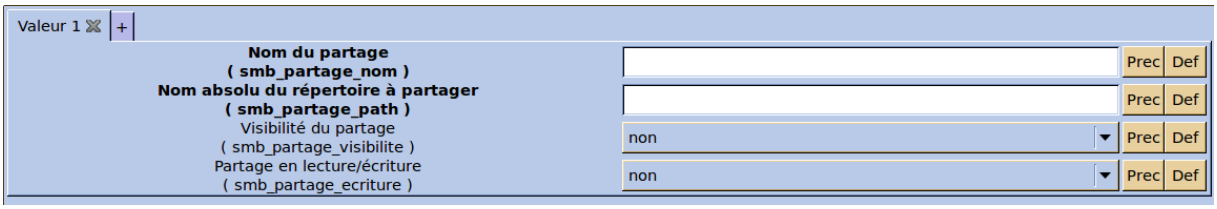
Cette valeur va influer sur les chances de Samba de remporter les élections de maître explorateur.

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

Activer des partages supplémentaires

L'option est à **non** par défaut. Passer l'option à oui permet d'activer un ou plusieurs nouveaux partages.

Pour en ajouter plusieurs il faut cliquer sur l'onglet +.



Les options à saisir 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 ;
- si le partage est en lecture/écriture = oui → lecture/écriture ; non → lecture seule.

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

Partages "manuels"

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

Ce fichier est généré à partir du template : **global_smb.tmpl** et des partages déclarés dans l'annuaire LDAP.

Le template (qui contient principalement la section [global]) peut éventuellement être patché.

La gestion des ACL 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].

Consulter la rubrique Création de patch

Consulter la Gestion fine des groupes et des utilisateurs : ACL

Complément

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

```
# man smb.conf
```

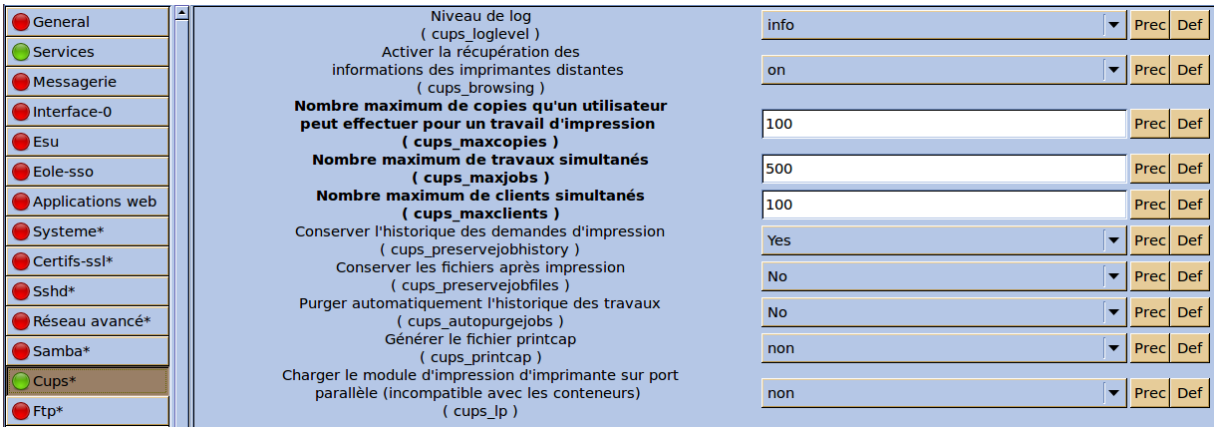
ou

http://manpages.ubuntu.com/manpages/lucid/fr/man5/smb.conf.5.html

2 Configuration du serveur d'impression

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* n'apparaît en mode expert que si le service est activé.



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

Les paramètres en question se retrouvent dans le nom des variables Creole et sont généralement préfixés par la chaîne "**cups_**".

Complément

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

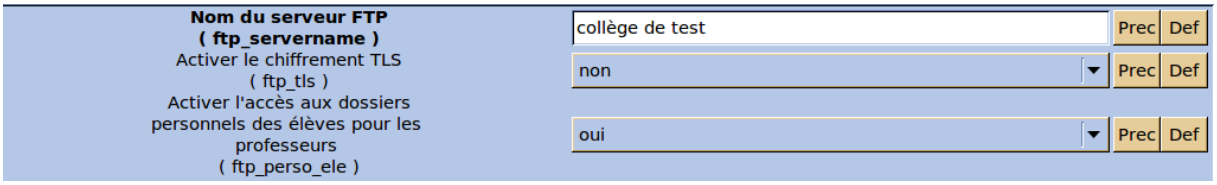
[man cupsd.conf]

ou http://manpages.ubuntu.com/manpages/lucid/fr/man5/cupsd.conf.5.html

3 Configuration du serveur FTP

Le serveur FTP est activable/désactivable dans l'onglet *Services* par l'intermédiaire de l'option : **Activer l'accès FTP**.

L'onglet *Ftp* n'apparaît en mode expert que si le service est activé.



Il est possible 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.

Il est possible de passer l'option **Activer le chiffrement TLS** à **oui** mais son utilisation est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

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.

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**.

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 (Ajaxplorer sur le module Scribe).

Pour accéder aux documents avec un navigateur web il faut préciser le protocole dans l'URL :

ftp://user@<adresse_serveur>/

ou

ftp://<adresse_serveur>/

Pour accéder aux fichiers par l'application web Ajaxplorer il faut l'activer dans l'onglet *Applications web*. 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>/ajaxplorer/** moyennant l'authentification (mire EoleSSO).

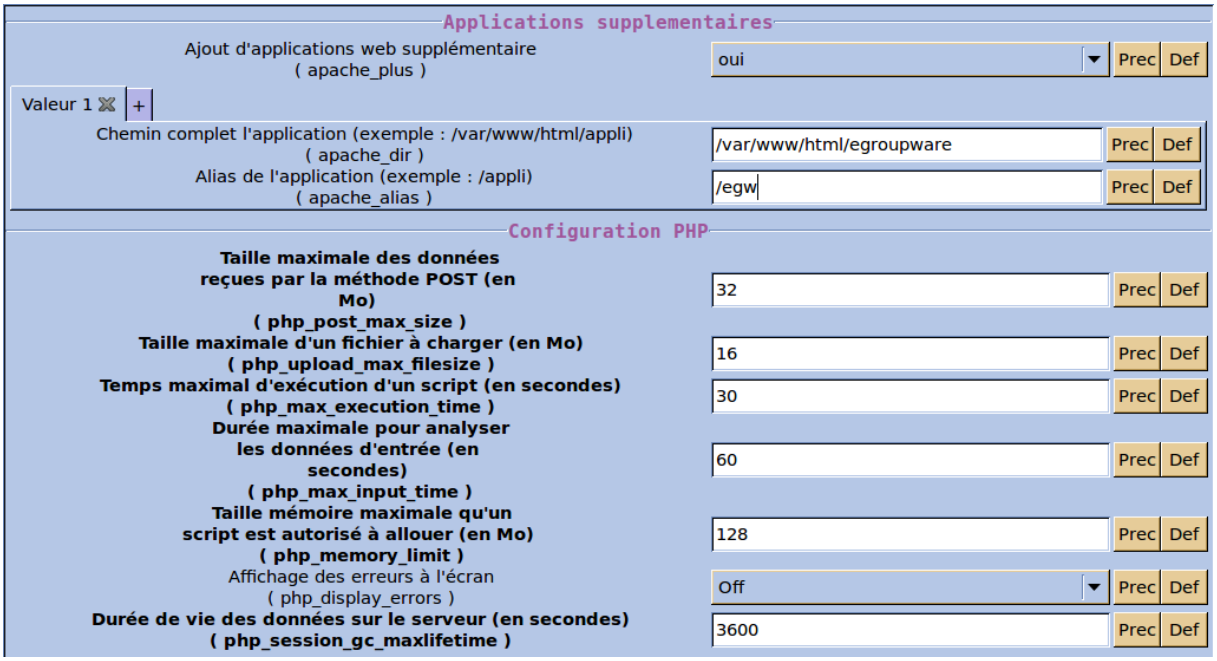
Attention

- 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.
- L'utilisation du chiffrement TLS est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

4 Configuration avancée du serveur web

Le serveur web apache est activable/désactivable dans l'onglet *Services* par l'intermédiaire de l'option : **Activer le serveur web Apache**.

L'onglet *Applications web* et l'onglet expert *Apache* sont disponibles uniquement si il est activé.



L'onglet expert *Apache* permet d'affiner la configuration du serveur web.

Applications supplémentaires

Les premières variables permettent de déclarer des applications supplémentaires sur le module.

Remarque

Une sous-section est dédiée à l'*Ajout d'applications web* dans la section concernant *Les applications web* et dans la documentation Envole.

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 paramètres en question se retrouvent dans le nom des variables Creole et sont généralement préfixés par la chaîne "**php_**".

Complément

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**

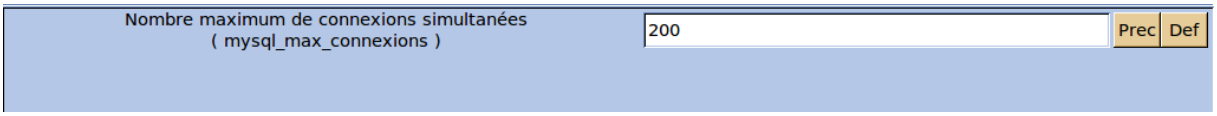
ou consulter : http://www.php.net/manual/fr/ini.list.php

5 Configuration du serveur MySQL

Sur les modules Scribe, AmonEcole et AmonEcole+, le serveur de bases 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**.

Complément

Pour plus d'informations, vous pouvez consulter les exemples de configuration fournis dans :

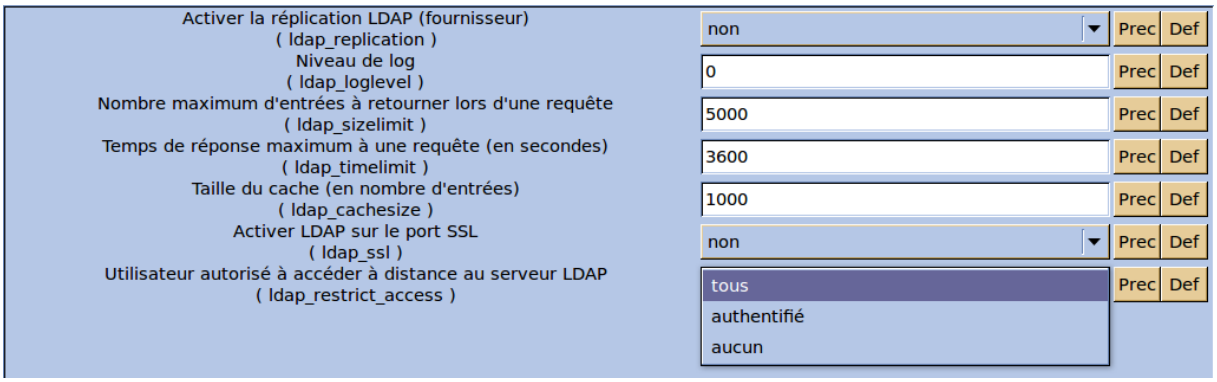
/usr/share/doc/mysql-server-5.1/examples

ou consulter : http://dev.mysql.com/doc/refman/5.1/en/server-system-variables.html

6 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.



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_`".

Réplication LDAP

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

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

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

Complément

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

[# man slapd.conf]

ou

http://manpages.ubuntu.com/manpages/lucid/fr/man5/slapd.conf.5.html

7 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 n'est disponible qu'en mode expert après activation du service dans l'onglet *Services*.

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.

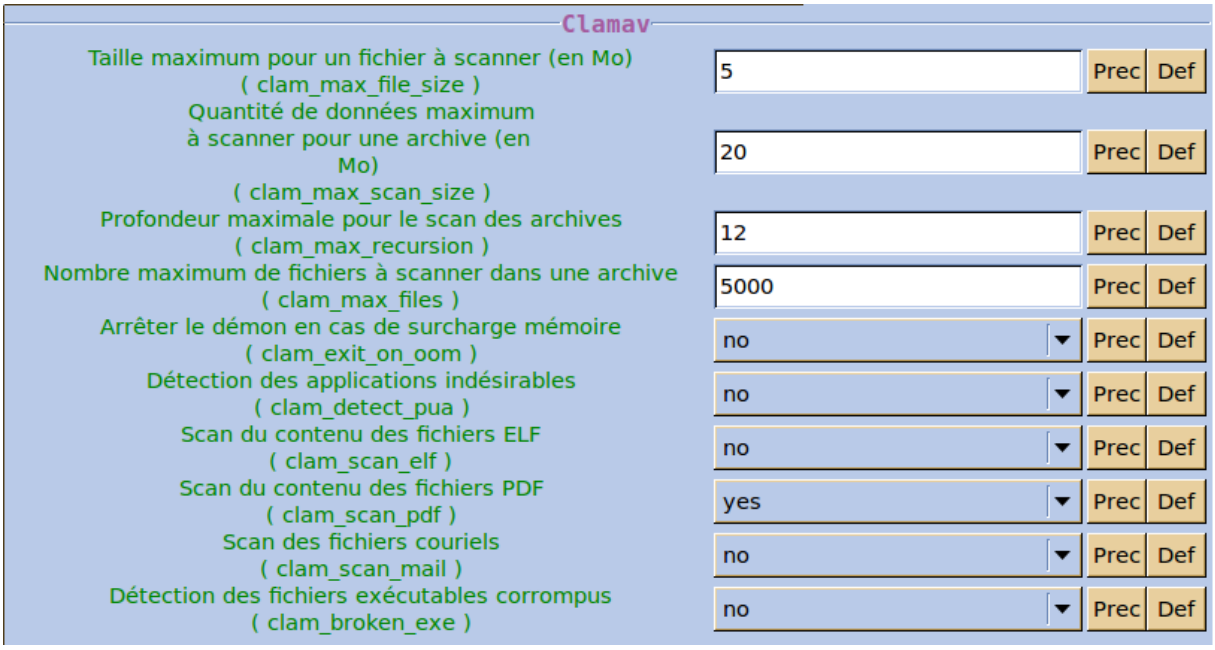
Exemple d'OSCAR*, outil de clonage édité par le CRDP de Lyon (http://oscar.crdp-lyon.fr) :

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

8 Configuration avancée de l'anti-virus

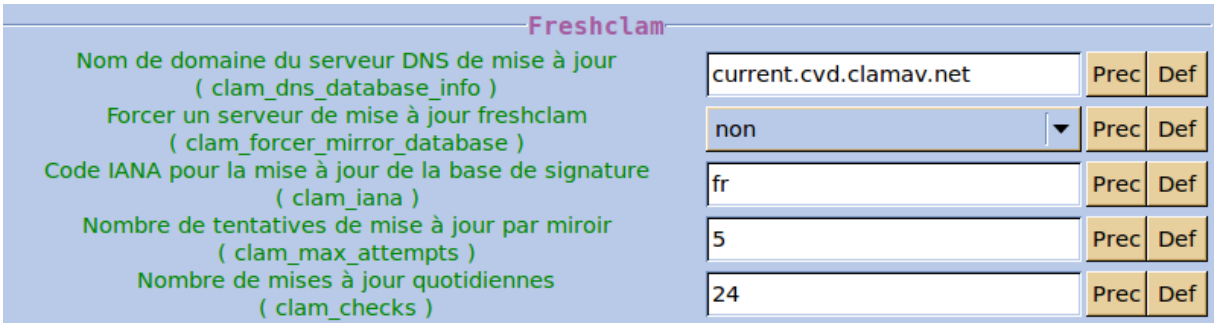
En mode expert, l'onglet *Clamav* comporte de nombreuses variables qui permettent d'affiner la configuration de ClamAV.

- **Taille maximum pour un fichier à scanner (en Mo)** ;
- **Quantité de données maximum à scanner pour une archive (en Mo)** ;
- **Profondeur maximale pour le scan des archives** ;
- **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* ;
- **Scan du contenu des fichiers PDF** ;
- **Scan des fichiers courriels** ;
- **Détection des fichiers exécutables corrompus**.

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

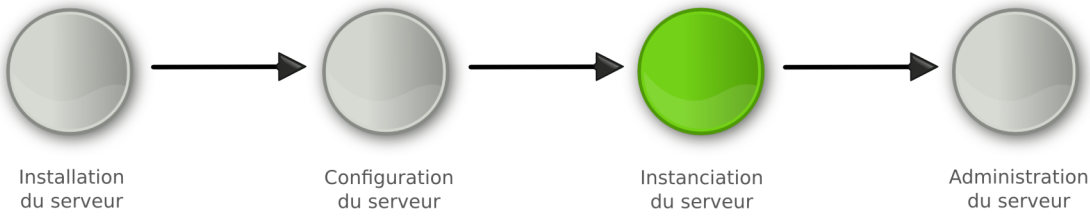


- **Nom de domaine du serveur DNS de mise à jour** permet de spécifier un miroir interne pour les signatures ;
- **Forcer un serveur de mise à jour freshclam** permet d'ajouter un ou plusieurs miroirs pour les signatures ;
- **Code IANA pour la mise à jour de la base de signature** ;
- **Nombre de tentatives de mise à jour par miroir** permet de réduire le nombre de tentatives de mise à jour, en effet des fichiers sont récupérés systématiquement à chaque tentatives ;

- **Nombre de mises à jour quotidiennes** permet de réduire le nombre de mises à jour quotidienne.

IX Instanciation

La troisième des quatre phases



1 Principes de l'instanciation

Les modules EOLE sont livrés avec un ensemble de **templates**.

Les templates sont les fichiers de configuration de chacun des logiciels utilisés. Ils sont pré-paramétrés et contiennent des variables.

Parallèlement les modules fournissent des dictionnaires décrivant l'ensemble de ces variables, comme expliqué dans la phase de configuration.

L'instanciation consiste à remplacer les variables par les valeurs renseignées dans le fichier **/root/zephir.eol** et à copier les fichiers vers leur emplacement cible.

Remarque

Si des patchs ont étés créés pour personnaliser le serveur, ils seront pris en compte durant cette phase.

Personnalisation du serveur à l'aide de Creole

2 Lancement de l'instanciation

Pour lancer l'instanciation, faire : [instance /root/zephir.eol]

Le compte rendu d'exécution est dans le fichier **/var/log/creole.log**

En complément du traitement ci-dessus, l'instanciation :

- arrête et redémarre des services ;
- lance des commandes ;
- effectue certaines tâches en fonction des réponses aux dialogues proposés.

2.1. Les mots de passe

Au premier lancement de l'instanciation, il est nécessaire de modifier les mots de passe :

- de l'utilisateur `root` ;
- du ou des utilisateurs à droits restreints (`eole`, `eole2`, ...) ;
- de l'utilisateur `admin` sur Scribe, Horus et AmonEcole ;
- de l'utilisateur `admin_zephir` sur Zéphir.

Remarque

Sur un module Amon, en cas d'utilisation d'un réseau pédagogique et d'un réseau administratif, le second administrateur (`eole2`) permet d'administrer le réseau pédagogique.

Par défaut, le système vérifie la pertinence des mots de passe. Pour cela, il utilise un système de "classe de caractères" :

- les lettres en minuscule [a-z] ;
- les lettres en majuscule [A-Z] ;
- les chiffres [0-9] ;
- les caractères spéciaux (exemple : $*ùµ%£, ; : !§/. ?) ;

Il faut utiliser différentes classes de caractères pour que le mot de passe soit considéré comme valide. Il n'est pas possible de réutiliser le mot de passe par défaut fournit à l'installation.

Par défaut, voici les restrictions :

- une seule classe de caractères : impossible ;
- deux classes de caractères : 9 caractères ;

- trois et quatre classes : 8 caractères.

Cette configuration est modifiable durant l'étape de configuration, en mode expert (onglet Systeme).

Attention

Il s'agit de comptes d'administration donc sensibles sur le plan de la sécurité. Il est important de renseigner des mots de passe forts.

Cet article du CERTA donne une explication détaillée sur la stratégie des mots de passe.

http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

2.2. L'enregistrement sur la base matériel

Une base matériel a été mise en ligne afin de permettre aux utilisateurs de vérifier, avant achat, si le matériel est utilisé par d'autres.

Dans cette action, le serveur fait une liste exhaustive du matériel détecté. Cette liste générée est ensuite envoyée au serveur matériel EOLE .

L'exécution de la sonde dépend de votre réponse à la question :

```
Pour enrichir cette base, acceptez-vous l'envoi de la description matérielle de ce serveur ? [oui/non]
```

** CONFIGURATION SERVEUR **

Description du serveur :

Ordinateur	Serveur
• Fabricant :	*Dell Computer Corporation*
• Dénomination :	*PowerEdge 830*
Caractéristiques	
• Processeur :	*Intel Corp. - Intel(R) Pentium(R) 4 CPU 2.80GHz*
• Carte Son :	*Aucune information disponible.*
• Cartes Réseaux :	*Intel Corporation - 82546EB Gigabit Ethernet Controller (Cop...* *Broadcom Corporation - NetXtreme BCM5721 Gigabit Ethernet PC...*
• Disques Durs :	*ATA - WDC WD800JD-75LS*
• Cartes Contrôleur :	*Intel Corporation - 82801G (ICH7 Family) IDE Controller* *Intel Corporation - 82801GB/GR/GH (ICH7 Family) Serial ATA S...*
• Mémoire :	512 Mo

Remarque

Les informations collectées sont anonymes.

2.3. Activation automatique des mises à jour hebdomadaire

A la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée. Cette mise à jour sera effectuée selon le niveau défini durant la phase de configuration.

La mise à jour permet de maintenir votre serveur avec le niveau de fonctionnalité le plus récent et surtout de bénéficier des dernières corrections. Certaines corrections peuvent combler des failles de sécurité importantes, il est donc important de les appliquer aussitôt qu'elles sont publiées.

Il est conseillé d'effectuer la mise à jour immédiatement, comme proposé à la fin de l'instance.

```
Une mise à jour est recommandée

Faut-il l'effectuer maintenant ? [oui/non]
```

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.

2.4. Le redémarrage

Il est possible qu'un redémarrage soit proposé à la fin de l'instance.

Si le noyau (Kernel) a été mis à jour, le serveur doit redémarrer pour pouvoir l'utiliser. Dans ce cas, la question suivante apparaîtra :

```
Un redémarrage est nécessaire
```

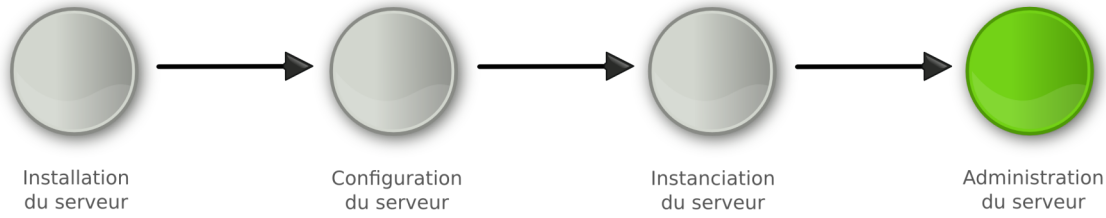
```
Faut-il l'effectuer maintenant ? [oui/non]
```

ou la remarque suivante si vous avez mis à jour :

```
Reconfiguration OK - Reboot nécessaire
```

X Administration

La dernière des quatre phases



1 Principes de l'administration

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

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

Il est également possible d'utiliser la **ligne de commande**.

Le choix de l'outil à utiliser s'effectue en fonction du type de module, de l'emplacement de ce module dans l'architecture (serveur en établissement ou serveur académique) et du profil de l'administrateur (administrateur académique, relai académique, personne ressource en établissement...).

2 Découverte de GNU/Linux

2.1. Les Bases

Descriptif sommaire

Une distribution

- un kernel = Linux *
- des outils périphériques = GNU *
- un environnement console ou graphique
- un système de fichiers éprouvé, hérité d'UNIX

2.1.1. L'arborescence GNU/Linux

L'arborescence GNU/Linux

Pour l'utilisateur, un système de fichiers est vu comme une arborescence : les fichiers sont regroupés dans des répertoires (concept utilisé par la plupart des systèmes d'exploitation). Ces répertoires contiennent soit des fichiers, soit récursivement d'autres répertoires. Il y a donc un répertoire racine et des sous-répertoires. Une telle organisation génère une hiérarchie de répertoires et de fichiers organisés en arbre.

Racine de l'arbre

/ (appelé slash ou root) : racine de l'arborescence sur laquelle sont raccrochés tous les sous-répertoires et fichiers.

Arborescence 1er niveau

- **bin/** : commandes liées au système, exécutables par tous ;

- **boot/** : noyau et initrd nécessaires au démarrage (ou boot) du système ;
- **dev/** : fichiers spéciaux effectuant le lien noyau / périphériques ;
- **etc/** : fichiers de configuration ;
- **home/** : répertoires de connexion (ou home directory) des utilisateurs ;
- **lib/** : librairies essentielles au démarrage et modules du noyau ;
- **mnt/** : contient les sous-répertoires de montage des partitions des autres périphériques ;
- **opt/** : installation des applications autres ;
- **proc/** : pseudo système de fichier représentant le noyau à un instant T ;
- **root/** : répertoire de connexion de root ;
- **sbin/** : commandes réservées à root et utilisées dans les niveaux de démarrage bas ;
- **sys/** : pseudo système de fichier représentant les processus ;
- **tmp/** : répertoire temporaire accessible à tous ;
- **usr/** : commandes utilisées par les utilisateurs (bin), l'administrateur (sbin), mais aussi ensemble du système graphique ;
- **var/** : ensemble des données variables du système (spools, logs, web, bases de données, ...).

Filesystem Hierarchy Standard (« norme de la hiérarchie des systèmes de fichiers », abrégé en **FHS**) définit l'arborescence et le contenu des principaux répertoires des systèmes de fichiers des systèmes d'exploitation GNU/Linux et de la plupart des systèmes Unix.

Fichiers et répertoires

Sous Unix, tout est fichier

Les différents types :

- **fichiers ordinaires** : fichiers éditables
- **fichiers programmes** : fichiers contenant des données compilées
- **répertoires** : fichier contenant les infos sur les fichiers et sous-répertoires contenus (index)
- **fichiers spéciaux** : fichier associé à un périphérique. Ne contient qu'une description relative au driver et type d'interface.

Adresse absolue / adresse relative

Un fichier ou un répertoire peut être défini :

- soit par un chemin relatif à l'endroit où vous vous positionnez au moment T.
- soit par un chemin absolu à partir de la racine de l'arborescence.

2.1.2. La gestion des droits

Droits de base UNIX

Les droits détaillés ci-après s'appliquent à l'ensemble des composantes de l'arborescence GNU/Linux, à savoir les fichiers et les répertoires.

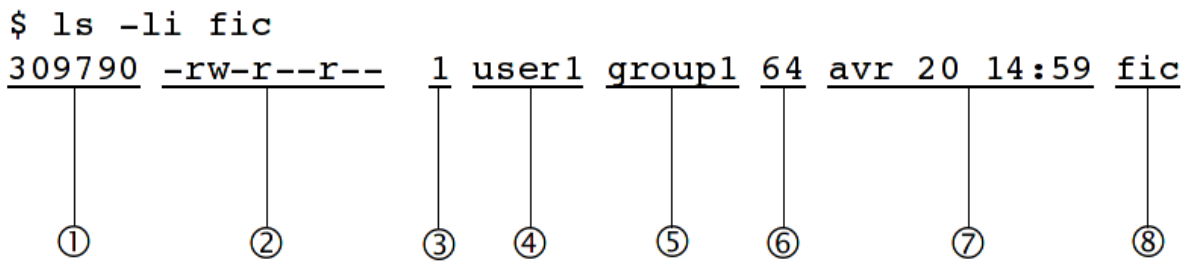
Droits essentiels :

- lecture
- écriture
- exécution

Autres droits :

- sticky bit
- setuid et setgid bits

Description d'un fichier



1. numéro d'inode
2. type & droits sur le fichier (ou répertoire)
3. compteur de liens physiques
4. propriétaire
5. groupe
6. taille
7. date de dernière modification
8. nom du fichier (répertoire)

Représentation du type et des droits des fichiers

Le schéma précédent montre, dans le second bloc, comment sont affichés les droits associés à un fichier (ou répertoire).

Ce bloc se décompose en 4 sous-parties :

- La première, codée sur un caractère, représente le type du fichier
- On trouve ensuite 3 groupes de 3 caractères indiquant les droits de lecture/écriture/exécution.

Le type du fichier peut être un des éléments suivants :

- **d** : répertoire
- **l** : lien symbolique
- **c** : périphérique de type caractère
- **b** : périphérique de type bloc
- **p** : pile fifo
- **s** : socket
- **-** : fichier classique

Exemple

- Fichiers de périphériques :
  - brw-rw---- 1 root disk 8, 0 nov 12 08:17 /dev/sda
  - brw-rw---- 1 root cdrom 3, 0 nov 12 08:17 /dev/hda
  - crw-r----- 1 root kmem 1, 1 nov 12 08:17 mem
  - crw-rw---- 1 root root 4, 0 nov 12 08:17 tty0
- Répertoires :
  - drwxr-xr-x 13 root root 4096 oct 20 10:22 /usr
  - drwxr-xr-x 17 user1 group1 4096 oct 31 09:18 /home/user1
- Fichiers standards :
  - -rw-r--r-- 1 root root 2008 oct 17 19:36 /etc/inittab
  - -rw-r--r-- 1 root root 724 déc 20 2006 /etc/crontab
  - -rwxr-x--1 root root 1024 oct 29 /home/user1/monScript
- Lien symbolique :
  - lrwxrwxrwx 1 root root 31 oct 27 15:00 /var/lib/postgresql/8.3/main/root.crt -> /etc/postgresql-common/root.crt
- Socket :
  - srw-rw-rw- 1 root root 0 nov 12 08:18 /var/run/gdm_socket

Détail des droits standards

Comme énoncé précédemment, les droits sont codés sur 3 jeux de 3 droits.

Cet ensemble de 3 droits sur 3 entités se représente généralement de la façon suivante : on écrit côte à côte les droits **r** (*R*ead/lecture), **w** (*W*rite/écriture) puis **x** (e*X*ecute/exécution) respectivement pour le propriétaire (**u**), le groupe (**g**) et les autres utilisateurs (**o**). Les codes u, g et o (u comme user, g comme group et o comme others) sont utilisés par les commandes UNIX qui permettent d'attribuer les droits et l'appartenance des fichiers.

Lorsqu'un droit est attribué à une entité, on écrit ce droit (r, w ou x), et lorsqu'il n'est pas attribué, on écrit un '-'. Par exemple : **rwxr-xr--**

Droits Spécifiques

SUID Bit

Ce droit s'applique aux fichiers exécutables, il permet d'allouer temporairement à un utilisateur les droits du propriétaire du fichier, durant son exécution.

En effet, lorsqu'un programme est exécuté par un utilisateur, les tâches qu'il accomplira seront restreintes par ses propres droits, qui s'appliquent donc au programme.

Lorsque le droit SUID est appliqué à un exécutable et qu'un utilisateur quelconque l'exécute, le programme détiendra alors les droits du propriétaire du fichier durant son exécution.

Bien sûr, un utilisateur ne peut jouir du droit SUID que s'il détient par ailleurs les droits d'exécution du programme. Ce droit est utilisé lorsqu'une tâche, bien que légitime pour un utilisateur classique, nécessite des droits supplémentaires (généralement ceux de root). Il est donc à utiliser avec précaution.

- -r-**s**--x--x 1 root root 15540 jun 20 2004 /usr/bin/passwd

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci : ---**s**------ ou ---**S**------

SGUID Bit

Ce droit fonctionne comme le droit SUID, mais appliqué aux groupes. Il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire.

De plus, ce droit a une tout autre utilisation s'il est appliqué à un répertoire. Normalement, lorsqu'un fichier est créé par un utilisateur, il en est propriétaire, et un groupe par défaut lui est appliqué (généralement users si le fichier a été créé par un utilisateur, et root s'il a été créé par root). Cependant, lorsqu'un fichier est créé dans un répertoire portant le droit SGID, alors ce fichier se verra attribuer par défaut le groupe du répertoire. De plus, si c'est un autre répertoire qui est créé dans le répertoire portant le droit SGID, ce sous-répertoire portera également ce droit.

- -rwxr-sr-x 1 root utmp 319344 avr 21 2008 /usr/bin/xterm

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci : ---**s**------ ou ---**S**------

Sticky Bit

Lorsque ce droit est positionné sur un répertoire, il interdit la suppression des fichiers qu'il contient à tout utilisateur autre que le propriétaire. Néanmoins, il est toujours possible pour un utilisateur possédant les droits d'écriture sur ce fichier de le modifier (par exemple de le transformer en un fichier vide).

Notation : il est représenté par la lettre **t** ou **T**, qui vient remplacer le droit d'exécution **x** des autres utilisateurs que le propriétaire et ceux appartenant au groupe du fichier, de la même façon que les droits SUID et SGID. La majuscule fonctionne aussi de la même façon, elle est présente si le droit d'exécution x caché n'est pas présent : ---------**t** ou ---------**T**

Exemple : le répertoire /tmp

- drwxrwxrw**t** 23 root root 4096 oct 20 14:27 /tmp/

Listes de contrôle d'accès

Une liste de contrôle d'accès ou ACL, permet de définir une liste de permission sur un fichier ou répertoire.

Aux habituels utilisateur, groupe et autre, il est possible d'étendre le nombre d'utilisateurs et de groupes ayant des droits sur un même fichier

Les ACLs s'ajoutent aux droits standards. Lorsqu'on liste les droits d'un fichier, les ACLs sont symbolisées par un "+".

```
-rwxrwx---+ 1 root professeurs 26 2009-05-27 16:37 fic
```

Les droits étendus apparaissent de la façon suivante :

```
user::rwx
user:p.nom:rwx
group::---
mask::rwx
other::---
```

Les ACLs d'un dossier père ne sont pas automatiquement repris pour le fichier fils.

Il est possible de modifier ce comportement, à associant des droits par défaut (grâce à l'attribut *default*).

Par exemple :

```
user::rwx
user:p.nom:rwx
group::rwx
mask::rwx
other::--x
default:user::rwx
default:user:p.nom:rwx
default:group::---
default:mask::rwx
default:other::---
```

2.1.3. La gestion des processus

Définition d'un processus

Un processus est un programme qui s'exécute en mémoire.

Tout processus lancé :

- se voit attribuer un numéro appelé **PID** (Process Identifier).
- est fils du processus qui l'a lancé. Le fils connaît le PID de son père, et en garde une trace sous la forme d'un numéro appelé **PPID** (Parent Process Identifier).

- appartient à un propriétaire (**UID** - celui qui a lancé le programme et qui pourra interagir avec ce processus)
- détermine son activité par un état : Actif, Exécutable, Endormi, Zombi.

Si un processus disparaît, tous les processus fils disparaissent également, sauf quand un processus est raccroché à **init**. Ainsi donc, à l'instar des fichiers, les processus sont organisés en arbre.

Enfin GNU/Linux est un système multi-tâche, c'est à dire que plusieurs processus peuvent être exécutés en même temps, en réalité, un seul utilise le processeur à la fois, ce dernier ne sachant effectuer qu'une seule instruction à la fois.

Etat d'un processus

Comme évoqué précédemment, un processus peut avoir un état : Actif, Exécutable, Endormi, Zombi.

- **Actif** : le processus utilise le processeur, et est donc en train de réaliser des actions pour lequel il a été conçu.
- **Exécutable** : le processus est en exécution mais il est en attente de libération du processus qui est utilisé par un processus actif. Pour l'utilisateur, ceci est invisible car l'opération est très rapide.
- **Endormi** : comme son nom l'indique, le processus est endormi, il ne fait rien. Par exemple, un processus peut attendre un événement pour redevenir *Actif*, comme par exemple, que l'on appuie sur une touche lors de l'affichage d'un message.
- **Zombie** : un processus zombie est un processus terminé, mais le système ou le processus parent n'en a pas été informé. L'état d'un processus peut être modifié par un autre processus, par lui même ou par l'utilisateur.

2.2. Quelques Commandes

Actions sur les fichiers et répertoires

Se déplacer dans l'arborescence :

- savoir où je me situe : **pwd** ;
- aller vers : **cd [répertoire]**.

Lister les fichiers et les droits : ls [-la] [fichier...] [répertoire...].

Lister les ACLs : getfacl [fichier...] [répertoire...].

Créer/supprimer un répertoire :

- créer un répertoire : **mkdir [-p] <répertoire...>** ;
- supprimer un répertoire (déjà vide) : **rmdir <répertoire...>**.

Copier, renommer, déplacer :

- copier : **cp [-fr] <source1>... <destination>** ;
- renommer : **mv <source> <destination>** ;
- déplacer : **mv <source1>... <destination>**.

Liens physiques, liens symboliques : ln [-s] <origine> <destination>.

Manipuler les droits & les propriétaires :

changer les droits : **chmod [-R] [MODE|MODE-OCTAL] <fichier...> <répertoire...>** ;

changer le propriétaire : **chown [-R] <user>[.<group>] <fichier...> < répertoire...>** ;

changer le groupe : **chgrp [-R] <group> <fichier...> < répertoire...>** ;

changer les ACLs : **setfacl [-R] -m <u|g|o>:<utilisateur|group>:<droit> < répertoire...>**.

Gestion des processus

Voir l'état des processus :

- à un instant T : **ps [auxef...]** ;
- visualisation dynamique : **top**.

Arrêt d'un processus : kill [-Num_Sig] <PID...>.

Autres commandes diverses

passwd : permet de changer le mot de passe d'un utilisateur système (il ne permet pas de changer les mots de passe des utilisateurs dans un annuaire LDAP)

[passwd] sans option modifie le mot de passe de l'utilisateur courant.

[passwd nom_d_utilisateur] permet de changer le mot de passe d'un autre utilisateur.

Si la commande est exécuté par un utilisateur autre que "root" le mot de passe actuel sera demandé.

sort : trier des lignes en fonction d'une ou plusieurs clés : **sort [-ndtX] [-k num_champs] fichier...**.

grep : rechercher des chaînes de caractère dans un ou plusieurs fichiers : **grep [-vni] chaîne fichier...**.

cut : extraire des colonnes d'un ou plusieurs fichiers : **cut -f <nombre> [options] fichier...**.

wc : déterminer le nombre de lignes, mots ou caractères dans un ou plusieurs fichiers : **wc [-lwc] fichier...**.

tail et head : visualiser les dernières ou les premières lignes d'un fichier :

- **tail [-n] fichier** ;
- **head [-n] fichier**.

screen : multiplexeur de terminaux en mode texte. Il permet de détacher un terminal et de le récupérer en cas de déconnexion. Ce logiciel est particulièrement adapté aux travaux à distance, en cas de coupure réseau il est possible de reprendre la main dessus le serveur. Voici le fonctionnement de base :

- lancer un nouveau terminal : **screen** ;
- détacher ce terminal : [ctrl a d] ;

- re-attacher le terminal : **screen -rd**.

2.3. Les conteneurs

Pour gérer les conteneurs, différentes commandes sont disponibles :

- installation d'un paquet dans un conteneur : [apt-eole install-conteneur (nom_du_conteneur) paquet]
- statut de tous les conteneurs : [lxc-status] ;
- arrêt de tous les conteneurs : [service lxc stop] ;
- démarrage de tous les conteneurs : [service lxc start] ;
- arrêt d'un conteneur : [lxc-halt -n (nom_du_conteneur)];
- forcer l'arrêt d'un conteneur : [lxc-stop -n (nom_du_conteneur)] ;
- démarrage d'un conteneur : [lxc-start -n (nom_du_conteneur) -d]
- entrer dans un conteneur : [ssh (nom_du_conteneur)].

Les conteneurs seront installés dans le répertoire **/opt/lxc/**, mais, normalement, il n'est pas nécessaire de modifier les fichiers directement dans ce répertoire.

2.4. La gestion des onduleurs

Quelques commandes utiles :

- test d'une installation sans démarrer le service upsd : `upsdrvctl start` ;
- test de l'arrêt du serveur sans avoir à attendre que la batterie soit vide : `upsmon -c fsd` ;
- lister la configuration : `upsc eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur) ;
- modifier la configuration : `upsrw eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur).

2.5. Les manuels

L'organisation du man

L'ensemble du man est organisé en sections numérotées de 1 à 9 pour les plus courantes :

1. commandes utilisateurs pouvant être exécutées quelque soit l'utilisateur
2. appels systèmes, c'est-à-dire les fonctions fournies par le noyau
3. fonctions des bibliothèques
4. périphériques, c'est-à-dire les fichiers spéciaux que l'on trouve dans le répertoire /dev
5. descriptions des formats de fichiers de configuration (comme par exemple /etc/passwd)
6. jeux
7. divers (macros, conventions particulières, ...)
8. outils d'administration exécutables uniquement par le super utilisateur (root)
9. autre section (spécifique à GNU/Linux) destinée à la documentation des services offerts par le noyau

Lorsque la documentation est interrogée à propos d'un terme présent dans plusieurs sections (ex : **passwd**, à la fois commande et fichier de configuration), si le numéro de section n'est pas précisé, c'est toujours la section de numérotation la moins élevée qui sera affichée.

Contenu d'une page

Chaque page de man est structurée en paragraphes contenant des éléments particuliers.

Intitulé de la commande ou du fichier et section du manuel

Vérifier qu'il s'agit de la documentation attendue.

Exemple :

- **CP(1) Manuel de l'utilisateur Linux CP(1)**

documentation pour la commande cp, section 1

- **PASSWD(5) Manuel de l'administrateur Linux PASSWD(5)**

documentation pour le fichier passwd, section 5

Nom

comme son nom l'indique, il s'agit du nom de la commande ou du fichier ainsi que d'une description synthétique.

Exemple :

- **NOM**

  cp - Copier des fichiers.

Synopsis

Dans ce paragraphe, on retrouve la syntaxe d'une commande, c'est-à-dire l'ensemble des options et arguments disponibles.

Quelques précisions pour bien lire cette syntaxe : si à première vue elle peut paraître rébarbative, elle dit tout au sujet de la manipulation d'une commande.

Exemple :

- **cp [options] fichier chemin**

  Options GNU (forme courte) : [-abdfilprsuvxPR]

la commande **cp** accepte des options (introduites par un "-") et des arguments (sans "-").

Les éléments spécifiés entre crochets sont facultatifs pour le fonctionnement de la commande.

Au contraire, les éléments indiqués sans crochets sont obligatoires et, s'ils sont omis, provoqueront une erreur.

Lorsque les options sont indiquées dans les mêmes crochets, elles peuvent être combinées. Dans le cas contraire, elles sont incompatibles et devront être utilisées séparément.

Enfin les options peuvent être abrégées (ex : -f) ou complètes (ex : --force), la signification est la même et elle est développée dans le paragraphe `description`.

Description

Cette section du man détaille la totalité des options et arguments d'une commande, ou les éléments d'un fichiers de configuration.

Fichiers

Dans ce paragraphe, vous trouverez une liste de fichiers intéressants à consulter, en complément d'information pour une commande ou un fichier de configuration.

Voir aussi

(ou "See also")

Comme son nom l'indique, il s'agit d'une liste de commandes, fichiers, appels système... auquel on renvoie le lecteur pour compléter son information

Exemple :

- **VOIR AUSSI**

  passwd(1), login(1), group(5), shadow(5).

Cette page propose ici de consulter les commandes **passwd** et **login** dans la section 1 et les fichiers **group** et **shadow** dans la section 5 de la documentation.

Environnement

ici sont spécifiées les variables d'environnement qu'il est possible de configurer pour le fonctionnement de la commande ou du fichier.

2.6. L'éditeur de texte Vim

Qu'est ce que Vim ?

Vim est un éditeur de texte libre. Il est à la fois simple est puissant.

Il est néanmoins nécessaire de passer par un temps d'apprentissage pour maîtriser l'outil.

Pourquoi Vim ?

L'éditeur est généralement installé de base sur la plupart des distributions. C'est un logiciel stable et éprouvé.

L'éditeur peut être lancé directement sans interface graphique. Il est ainsi possible d'exécuter depuis le serveur.

De plus, Vim est pré-configuré par l'équipe EOLE. Il n'y aura pas de problème de balise de fin de ligne, de nombre d'espace lors de l'indentation, ... Problème qu'il est possible de rencontrer avec d'autres éditeurs.

2.6.1. Les modes Vim

Introduction

Vim utilise un système de "modes". Ce concept de base est indispensable pour comprendre le fonctionnement du logiciel.

Vim est un éditeur entièrement accessible au clavier. Un ensemble de commande permet d'accéder à un ensemble de fonctionnalité. Pour que l'éditeur distingue la saisie de commande (le mode "normal") et la saisie de texte (le mode "insertion"), différents modes sont utilisés.

Il existe également le mode "visuel" permettant de sélectionner une zone de texte où sera appliquée un ensemble de commande.

Cette distinction n'existe pas, généralement, dans les autres éditeurs. Ils utilisent alors des entrées dans un menu graphique ou des raccourcis clavier à la place du mode "normal".

Comparé au mode graphique, le mode commande ne nécessite pas l'usage de la souris pour rechercher le bon menu. Par rapport aux raccourcis clavier, le mode commande est souvent plus facile à se rappeler (write pour écrire).

Passage d'un mode à l'autre

Pour passe au mode "normal", il suffit de taper la touche [Echap] ou [Esc].

Pour passer au mode "insertion" (depuis le mode "normal") :

- insérer avant le curseur : [i] (ou la touche [Inser] du clavier) ;
- insérer après le curseur : [a] ;
- insérer en début de ligne : [I] ;
- insérer en fin de ligne : [A] ;
- insérer une ligne après : [o] ;
- insérer une ligne avant : [O] ;
- supprime pour remplacer un (et un seul) caractère : [s] ;
- supprime pour remplacer la ligne complète : [S] ;
- remplacer un caractère : [r] ;
- remplacer plusieurs caractères : [R] ;

Pour passer au mode "visuel" (depuis le mode "normal") :

- sélection caractère par caractère : [v];
- sélection ligne par ligne : [V] ;
- sélection colonne par colonne : [ctrl v].

2.6.2. Première prise en main

Exécuter Vim

Pour exécuter Vim, il suffit de taper [vim] dans l'interpréteur de commande. Il est aussi possible d'ouvrir directement un fichier en faisant [vim fichier.txt].

Ouvrir un fichier

En mode normal, taper : [:edit fichier.txt] (ou [:e fichier.txt]).

Insérer du texte

Passer en mode insertion : [i] et taper votre texte.

Enregistrer le texte

Quitter le mode insertion : [esc].

Enregistrer le texte : [:write] (ou [:w]).

Quitter l'éditeur

Pour quitter l'éditeur : [:quit] (ou [:q]).

Remarque

Vim créé un "buffer" lorsque l'on édite un fichier. Cela signifie que l'on ne modifie pas directement le fichier. Il faut sauvegarder les changements sous peine de perdre les modifications.

Le buffer est sauvegardé de façon fréquente dans un fichier "swap" (généralement **.fichier.txt.swp**). Ce fichier est supprimé lorsqu'on enregistre ou ferme le document.

2.6.3. Les déplacements

- se déplacer d'un caractère vers la gauche : [h] ;
- se déplacer de 20 caractères vers la gauche : [20h] ;
- se déplacer d'une ligne vers le bas : [j] ;
- se déplacer de 20 lignes vers le bas : [20j] ;
- se déplacer d'une ligne vers le haut : [k] ;
- se déplacer d'un caractère vers la droite : [l] ;
- se déplacer au début du prochaine mot : [w] ;
- se déplacer au début de deux mots : [2w] ;
- revenir au début du mot précédent : [b] ;
- se déplacer à la fin du prochain mot : [e] ;
- se déplacer à la prochaine phrase : [)];
- revenir à la phrase précédente : [(];
- se déplacer au prochain paragraphe : [}] ;
- revenir au paragraphe précédent: [{] ;
- revenir au début de la ligne : [^] ;
- aller à la fin de la ligne : [$] ;
- remonter d'un écran : [pgup] ;
- descendre d'un écran : [pgdown] ;
- descendre à la fin du fichier : [G] ;
- aller à la ligne 20 : [20G] ;
- aller au début de la page courante : [H] ;
- aller au milieu de la page courante : [M] ;
- aller à la fin de la page courante : [L] ;
- revenir à l'emplacement précédent : [ctrl o] ;
- aller à l'emplacement suivant : [ctrl i] ;
- la troisième occurrence de la lettre "e" : [3fe] ;

Il est possible de "marquer" des positions dans le texte. Cela permet de revenir très facilement à cet emplacement plus tard.

Pour cela, il faut utiliser la commande [m] suivi du nom de la marque (c'est à dire une lettre). Par exemple : [ma]. Pour revenir à la marque, il suffira de taper : ['a].

2.6.4. Recherche et remplacement de texte

Rechercher

- chercher les occurrences EOLE : [/EOLE] ;
- chercher les mots EOLE : [/\<EOLE\>] ;
- chercher l'occurrence suivante : [n] ;
- chercher l'occurrence précédente : [N] ;
- chercher les autres occurrences du mot sous le curseur : [*];
- chercher en arrière les autres occurrences du mot sous le curseur : [ctrl #] ;

Remplacement

- remplacer le mot EOLE par Scribe : [:%s/EOLE/Scribe/g]
- remplacer le mot EOLE par Scribe en demande confirmation : [:%s/EOLE/Scribe/gc]
- remplacer le mot EOLE par Scribe sur les 20 première ligne d'un fichier : [:0,20s/EOLE/Scribe/g]

2.6.5. Couper, copier et coller

- couper un texte sélectionné : [d] ;
- couper le caractère sélectionné : [x] ;
- couper les deux caractères suivants : [d2l] ;
- couper un mot : [dw] ;
- couper la ligne courante : [dd] ;
- couper 2 lignes : [d2] ;
- couper le paragraphe : [d}] ;
- copier un texte sélectionné : [y] ;
- coller le texte après : [p].
- coller le texte avant : [P] ;

2.6.6. Le mode fenêtre

Ouvrir plusieurs fenêtres

Il est possible d'ouvrir plusieurs fichiers en même temps.

Pour cela, il suffit de lancer plusieurs fois la commande [:e nomdufichier].

Pour passer d'un buffer à un autre, il suffit de taper [:bn] (n étant le numéro du buffer).

Ouvrir plusieurs tabulations

Pour ouvrir le fichier dans une nouvelle tabulation : [:tabedit fichier.txt].

Pour se déplacer de tabulation en tabulation, il suffit d'utiliser [ctrl alt pgup] et [ctrl alt pgdown].

Voir plusieurs fichiers

Il est possible de voir plusieurs fichiers dans la même interface.

Pour cela, il faut créer un nouveau buffer en tapant [:new] et ensuite ouvrir le nouveau fichier : [:e fichier.txt].

Pour se déplacer dans les buffers, il faut utiliser le raccourci [ctrl w] et les touches de déplacement [hjkl].

Pour se déplacer de buffer en buffer, il est possible également de taper deux fois [ctrl w].

Il est ensuite possible de déplacer les fenêtres horizontalement et verticalement avec [ctrl w] et les touches de déplacement en majuscule [HJKL].

Pour fermer une fenêtre, il suffit de faire [:q].

Voir plusieurs fois le même fichier

Il est possible d'ouvrir plusieurs fois le même buffer en faisant [ctrl w s]. Cela permet de voir simultanément plusieurs parties du même texte.

Attention

Dans ce cas, il s'agit du même buffer. Une modification dans une vue sera automatiquement reporter dans les autres vues.

Système de fichier

Il est possible d'ouvrir une fenêtre de système de fichier en faisant : [:Sex] ou [:Vex].

2.6.7. Autres

Complétion automatique

La complétion permet de compléter un mot automatiquement à partir d'une liste de mot présent dans le texte en court d'écriture. Il est souvent utile pour ne pas faire d'erreur dans le nom des fonctions.

Pour l'utiliser, il suffit de commencer a écrire le début du mot et faire [ctrl n] ou [ctrl p].

Annuler et refaire

Pour annuler la dernière action : [u] ;

Pour revenir sur l'annulation : [ctrl r].

Passer un texte en majuscule

Pour passer un texte en majuscule, il suffit de taper [~] ou [maj u].

Voir la différence entre les fichiers

Vim permet également de voir la différence entre deux textes. Pour cela, il suffit de lancer en ligne de commande :

[vimdiff nomdufichieroriginal.txt nomdufichiermodifier.txt]

2.6.8. Liens connexes

http://www.vim.org/

http://www.swaroopch.com/notes/Vim_fr:Table_des_Mati%C3%A8res

https://svn.timetombs.org/svn/doc-keymap/doc-keymap-cheat_sheet-vim-azerty_fr.pdf

2.7. Les commandes à distance avec SSH

2.7.1. Le protocole SSH

SSH* (Secure Shell) et un protocole de communication sécurisé. Il permet différentes actions comme l'authentification à distance, l'exécution de commande à distance ou le transfert de fichier.

Le protocole est chiffré par un mécanisme d'échange de clés de chiffrement effectué au début de la connexion.

Le transfert de fichier d'une machine à une autre se fait par un protocole proche de FTP*. La différence étant que les transferts du client et du serveur se font par un tunnel chiffré.

2.7.2. SSH sous GNU/Linux

Connexion à distance

Le client SSH est installé par défaut sur la plupart des distributions. Si ce n'est pas le cas, il faut installer un paquet dont le nom est généralement "openssh-client".

Une fois installé, il est possible d'ouvrir une session à distance de la manière suivante :

```
ssh utilisateur@ip_serveur
```

Si vous ne spécifiez pas de nom d'utilisateur, c'est l'utilisateur courant de votre session GNU/Linux qui sera utilisé.

Pour lancer des applications graphiques, il faudra le préciser dans la commande ssh en rajoutant l'option -X :

```
ssh -X utilisateur@ip_serveur
```.

A la première connexion, le message suivant apparaît :

```
Warning: Permanently added 'xxxxx' (RSA) to the list of known hosts.
```

Cela signifie qu'on ne s'est jamais connecté sur cette station et qu'un identifiant est ajouté à la liste des hôtes connus.

Il peut arriver que le certificat du serveur change (par exemple en cas de réinstallation).

Le message suivant apparaîtra :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
65:6d:9d:c0:78:f7:60:bf:13:86:59:16:53:07:3b:a4.
Please contact your system administrator.
Add correct host key in /home/xxx/.ssh/known_hosts to get rid of this message.
Offending key in /home/xxx/.ssh/known_hosts:12
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle
attacks.
X11 forwarding is disabled to avoid man-in-the-middle attacks. Permission
denied (publickey,password).
```

Ce message nous apprend plusieurs choses :

- le serveur ssh a une clef différente de celle de notre dernier passage ;
- le fichier comprenant les hôtes connus est **/home/xxx/.ssh/known_hosts** ;

- l'identifiant de l'hôte est spécifié à la ligne 12 (Offending key in /home/xxx/.ssh/known_hosts:12).

Si vous êtes sûr que l'hôte est le bon, il vous suffira de supprimer la ligne 12 du fichier known_hosts et de relancer une connexion.

Il faudra spécifier le mot de passe de l'utilisateur pour se connecter.

Ssh propose également la connexion par échange de clef. Cela permet de se connecter à distance sans connaître le mot de passe de l'utilisateur.

L'échange de clef peut être réalisé par l'intermédiaire d'un serveur Zéphir. Pour plus d'informations, consulter la documentation spécifique à ce module.

Exécution de commande à distance

Une fois connecté à distance, vous pouvez lancer n'importe quelle action comme si vous étiez en local.

Transfert de fichier à distance

Pour envoyer un fichier sur un serveur, il faut faire :

```
scp nom_du_fichier utilisateur@ip_serveur:/repertoire/de/destination/
```

Pour récupérer un fichier d'un serveur :

```
scp                    utilisateur@ip_serveur:/repertoire/source/nom_du_fichier
/repertoire/de/destination/
```

Pour récupérer un répertoire d'un serveur :

```
scp -r utilisateur@ip_serveur:/repertoire/ /repertoire/de/destination/
```

Enfin, il est possible d'avoir un shell proche de la commande FTP en faisant :

```
sftp utilisateur@ip_serveur
```

Truc & astuce

Sur la plupart des gestionnaires de fichier disponibles sous GNU/Linux, il est possible de faire des transferts de fichier avec SSH graphiquement (logiciel Filezilla par exemple).

2.7.3. SSH sous Windows

Exécution de commande à distance

Putty est un logiciel libre implémentant un client Telnet* et SSH* pour Unix et Windows.

http://www.chiark.greenend.org.uk/~sgtatham/putty/

Dans l'environnement EOLE, il permet de se connecter à un serveur à distance depuis un poste Windows et, ainsi, pouvoir exécuter des commandes.

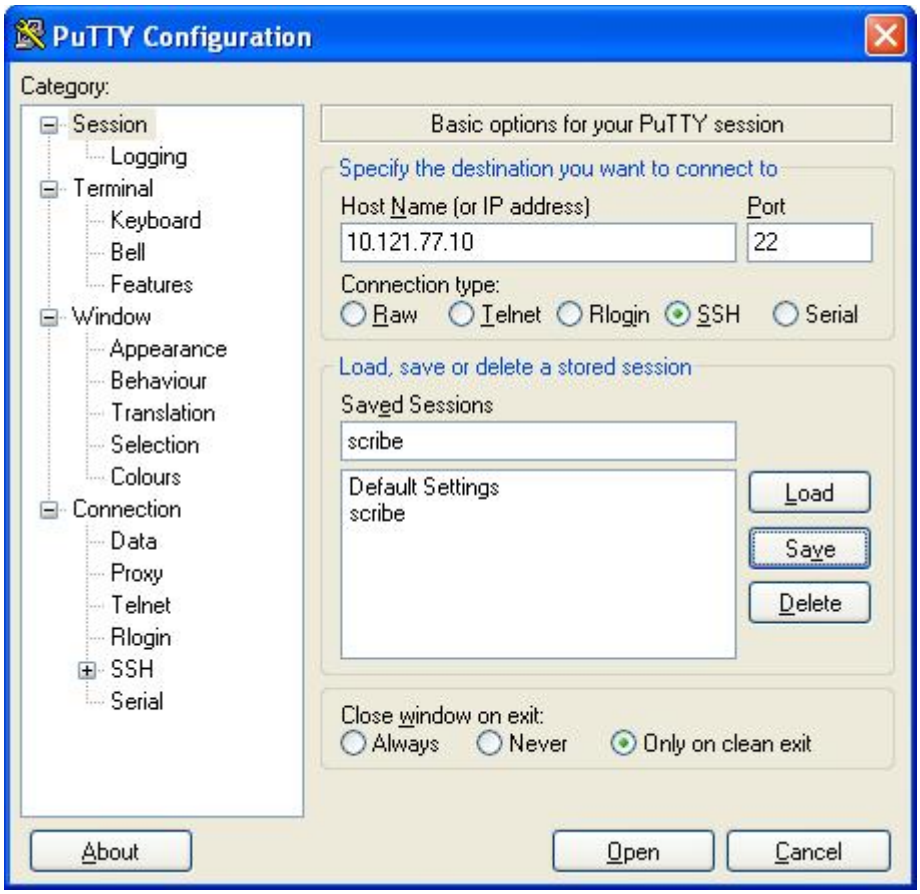
La connexion avec Putty au serveur se fait en utilisant le protocole SSH.

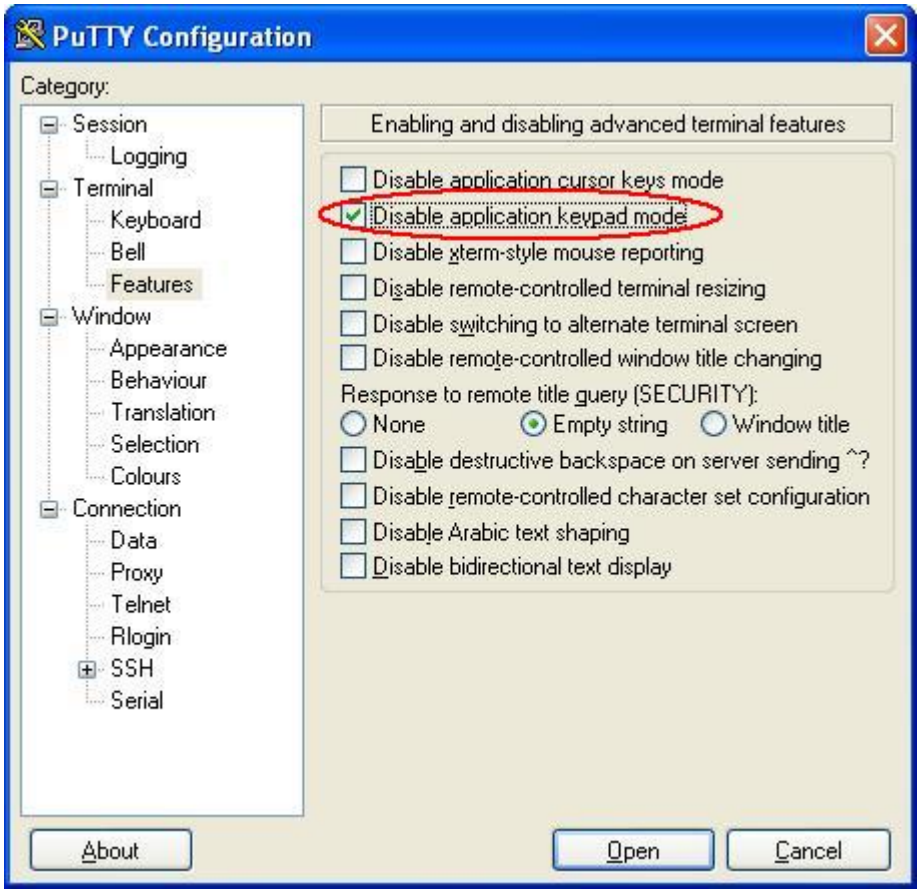
Remarque

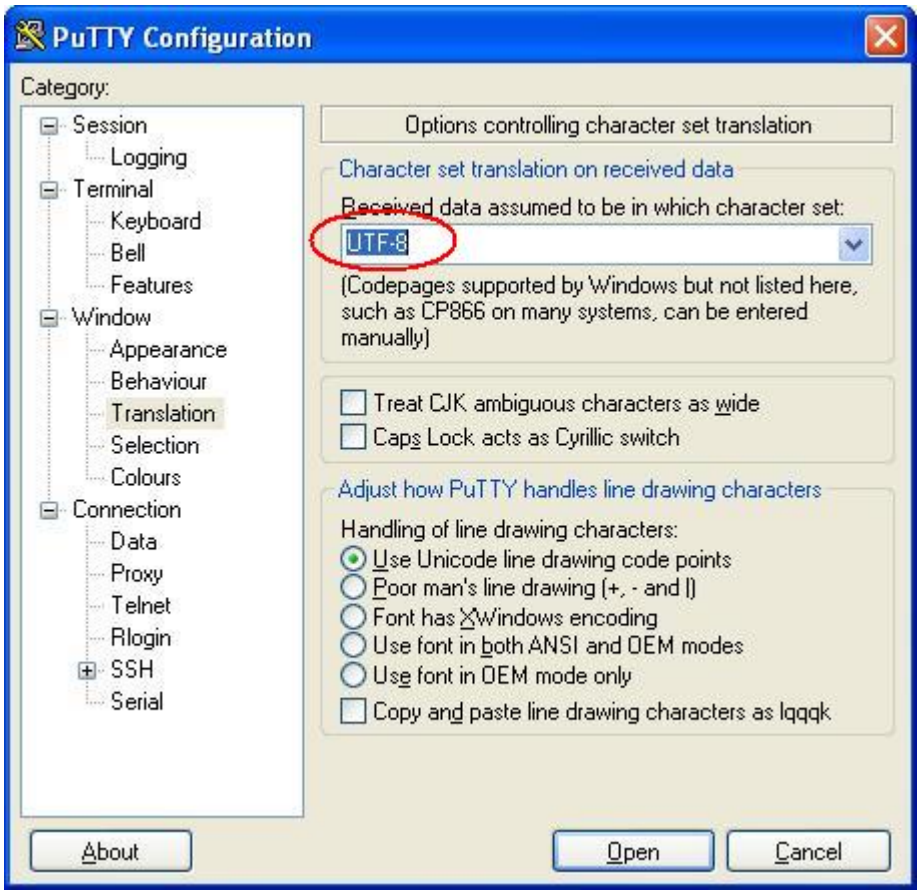
Sur le module Scribe, Putty est pré-installé dans le répertoire personnel d'*admin* (**U:\client\putty.exe**).

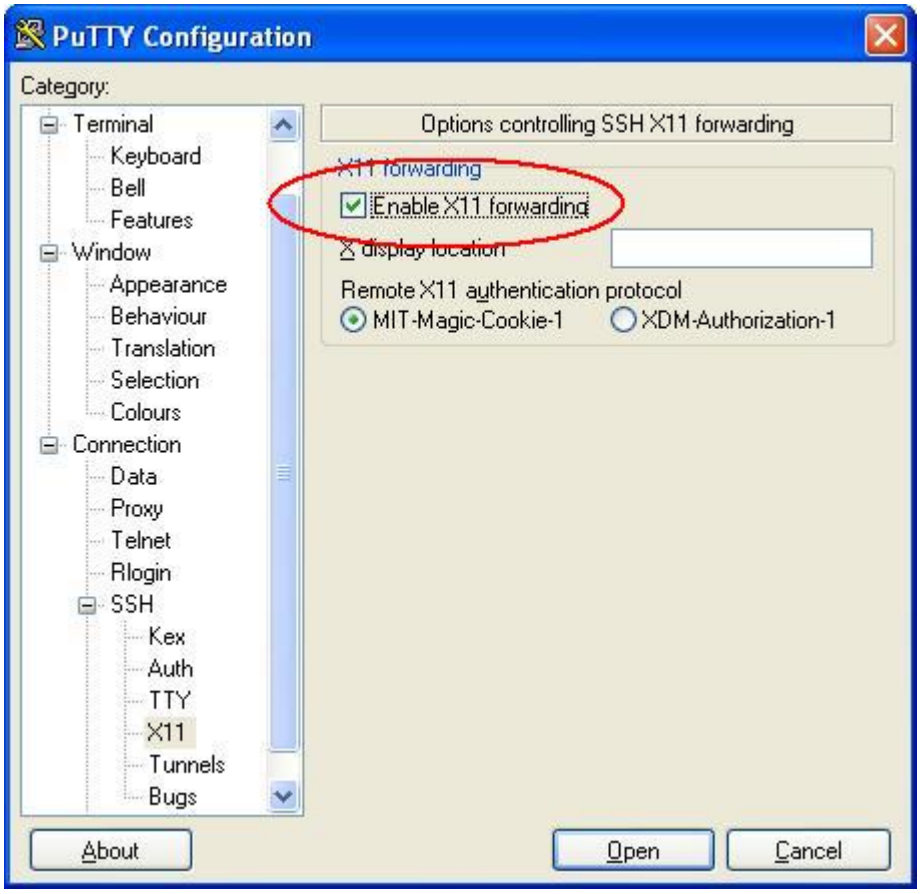
Configuration pour les serveurs EOLE

Pour obtenir un meilleur environnement de travail, la configuration par défaut de Putty doit être modifiée.





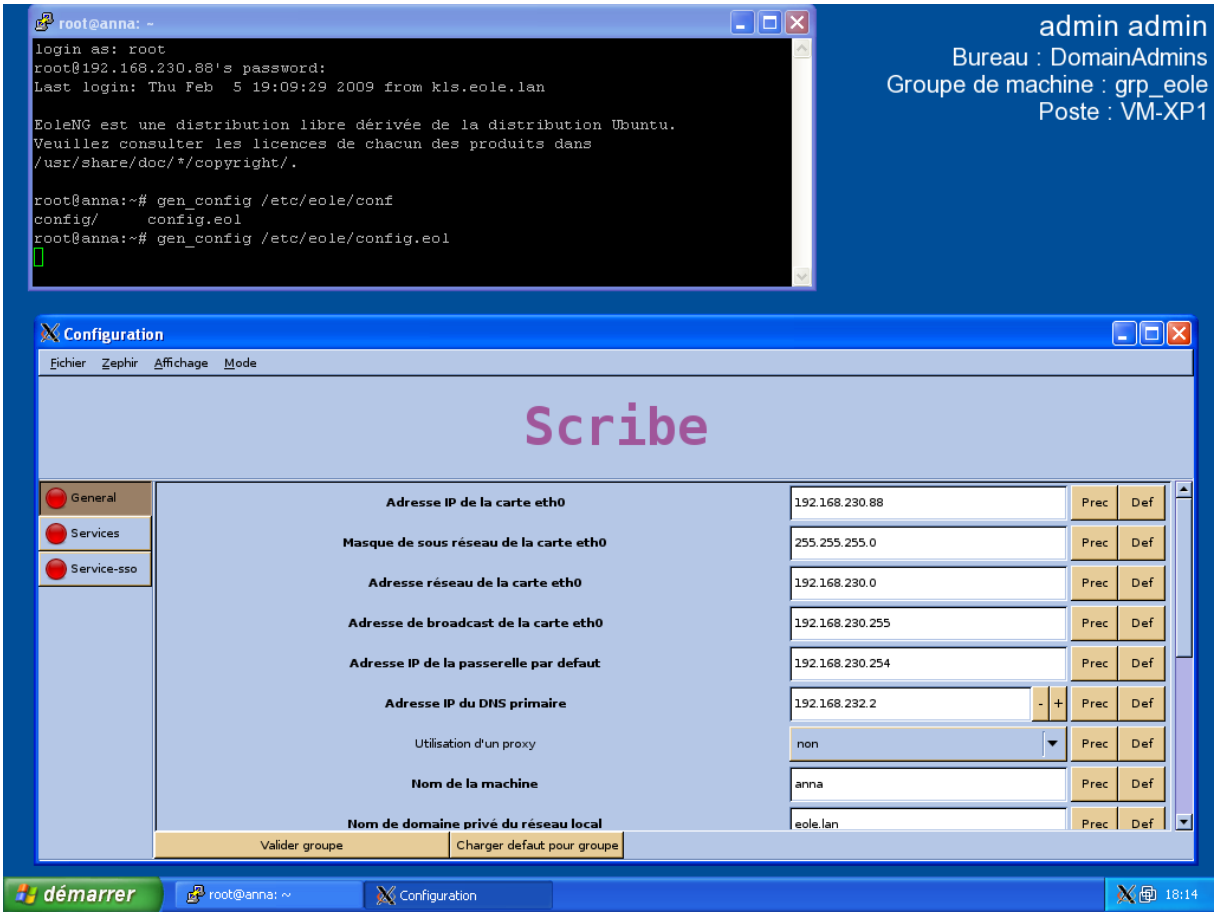




La dernière capture montre comment autoriser la redirection des applications graphiques vers votre poste.

Cependant vous devrez utiliser Xming.

C'est un logiciel libre permettant d'émuler un serveur X vers lequel sera redirigé l'application graphique lancée à travers ssh sur le serveur EOLE.



Transfert de fichier à distance

Il existe une interface graphique de transfert de fichier à distance. Il s'agit de WinSCP.

On utilise le logiciel comme un client FTP normal.

2.8. Quelques références

- Le site du Kernel Linux : http://www.kernel.org ;
- Le projet GNU : http://www.gnu.org ;
- Site réputé pour ses documentations et son forum d'entraide : http://www.lea-linux.org/ ;
- Guide de survie du débutant : http://www.delafond.org/survielinux/ ;
- Un manuel en ligne (man) : http://unixhelp.ed.ac.uk/CGI/man-cgi ;
- Définitions sur Wikipédia :
  - Noyau Linux : http://fr.wikipedia.org/wiki/Noyau_Linux,
  - Projet GNU :http://fr.wikipedia.org/wiki/GNU,

- Distribution :http://fr.wikipedia.org/wiki/Distribution_Linux,
- Les Permissions Unix : http://fr.wikipedia.org/wiki/Permissions_Unix.

3 Reconfiguration

Reconfigure

Suite à un diagnostic, à des corrections dans le paramétrage ou suite à une mise à jour, il est nécessaire de reconfigurer le serveur.

On réalise cette opération avec la commande **reconfigure**, plutôt qu'avec la commande **instance**.

reconfigure est la commande à lancer pour appliquer un changement de configuration (par exemple, le changement d'adressage IP) ou si au moins un paquet a été mis à jour (automatique si la mise à jour est lancée par l'EAD).

Avec **Maj-Auto**, un message orange indique s'il est nécessaire de lancer **reconfigure**.

Cette commande :

- ré-applique le SID trouvé dans l'annuaire sur Horus et Scribe ;
- supprime des paquets (utilisé pour les noyaux notamment) ;
- exécute les scripts pre/postreconf ;
- met à jour les valeurs par défaut des dictionnaires ;
- recréé "admin" s'il n'a pas été trouvé (Scribe et Horus) ;
- copie, patch et renseigne les templates ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD) ;
- relance les services.

Remarque

Il est à noter que la commande [instance] prend comme argument le fichier de configuration à exploiter ([instance zephir.eol]). Il génère un fichier **/etc/eole/config.eol** - s'il existe déjà, un avertissement apparait).

De son coté, [reconfigure] exploite le fichier **/etc/eole/config.eol**.

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

Pourquoi reconfigure au lieu d'instance

Instance : est la commande à lancer à l'installation d'un nouveau serveur. Cette commande :

- initialise les mots de passe *"root"*, "*<nom du module>*" et "*admin*" ;
- génère un nouveau SID ;
- génère l'annuaire et les bases MySQL si inexistants ;
- lance des commandes spécifiques à l'instanciation ;
- copie, patch et renseigne les templates ;
- (re)lance les services ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD).

Reconfigure : ré-applique la configuration (exemple, après une mise à jour) ou des modifications de configuration (exemple, changement d'adresse IP). Cette commande :

- ré-applique le SID trouvé dans l'annuaire ;
- supprime des paquets (exemple le noyau) ;
- exécute des commandes spécifiques à la reconfiguration ;
- met à jour les valeurs par défaut des dictionnaires ;
- recréé "admin" s'il n'a pas été trouvé ;
- copie, patch et renseigne les templates ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD) ;
- relance les services.

Lors d'une mise à jour via l'EAD, `reconfigure` est lancé automatiquement. Si la mise à jour a été effectuée sur la console ou via ssh avec la commande `Maj-Auto` un message orange indique s'il est nécessaire de lancer reconfigure.

Il existe plusieurs contre-indications à l'utilisation de la commande `instance` sur un serveur déjà instancié :

- attention à l'annuaire sur Scribe et Horus, instance permet de le re-générer ce qui efface tous les comptes utilisateurs et les stations intégrés au domaine. Une nouvelle extraction ne réglera pas forcément le problème ;
- risque de désynchronisation du SID ;
- les commandes exécutés peuvent être différentes ;
- valeurs par défaut non mises à jour ;
- reconfigure est automatique, il ne pose pas de question.

4 L'interface d'administration EAD

EOLE offre une interface simplifiée de gestion du serveur : l'interface d'administration EAD.

Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

4.1. Fonctionnement général

4.1.1. Principes

L'EAD (Eole ADmin) est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible avec un navigateur à l'adresse **https://<adresse_module>:4200**.

L'EAD est composé de deux parties :

- un serveur de commandes (**ead-server**), présent et actif sur tous les modules ;
- une interface (**ead-web**), activable depuis l'interface de configuration du module : *Services/Activation du frontend EAD*.

Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, Sentinelle, ...) ne disposent que de la **version de base** qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...).

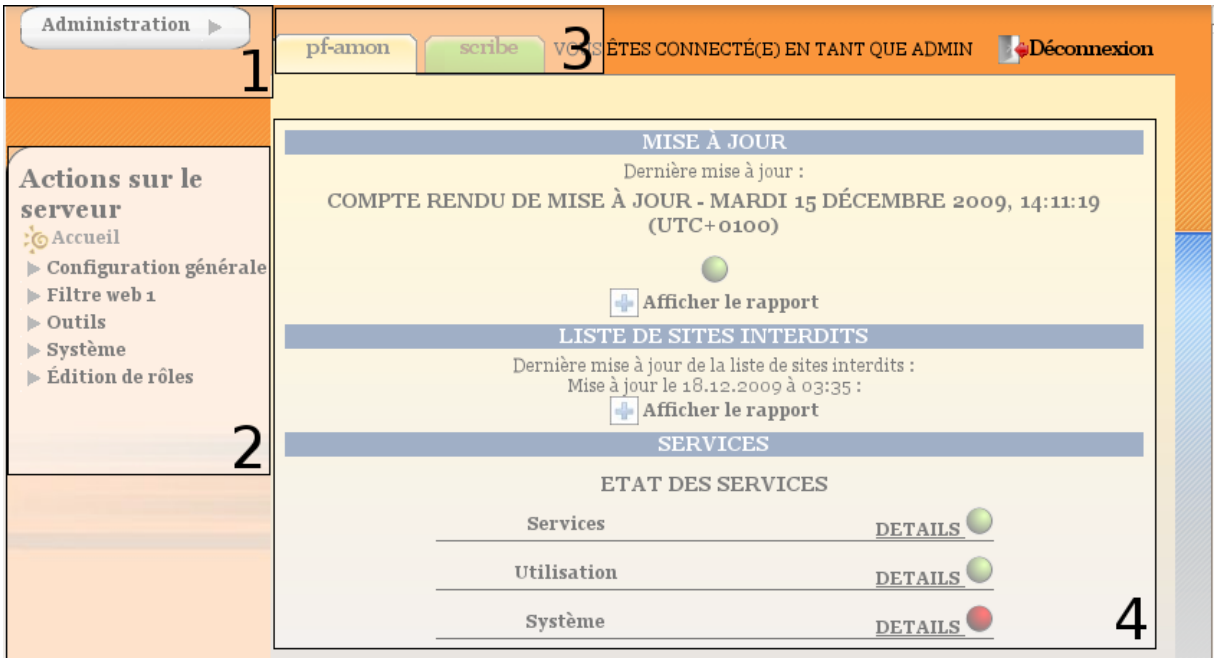
Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.

Aide

Un point d'interrogation est accessible en bas à droite de certaines pages, il permet d'afficher une aide associée.

4.1.2. Premier pas dans l'administration d'un serveur

Lorsque vous vous êtes connecté sur un serveur de commandes, vous avez quatre éléments :



1. la gondole d'administration ;
2. le menu d'action (propose les actions auxquelles vous avez accès) ;
3. les onglets (les serveurs enregistrés sur l'interface) ;
4. la partie centrale ou espace de travail (il s'agit de la partie venant du serveur de commandes).

1 - La gondole d'administration

Elle permet d'accéder aux actions de base de l'interface (ajout/suppression de serveur, déconnexion, retour vers l'accueil, choix de la feuille de style CSS, connexion locale).

2 - Le menu d'action

Il permet d'accéder aux actions disponibles sur le serveur de commandes.

3 - Les onglets (les serveurs enregistrés sur l'interface)

Ils permettent d'accéder aux divers serveurs EOLE enregistrés sur l'interface.

4 - La partie centrale ou espace de travail

Les éléments affichés dans cette partie viennent du serveur de commandes.

C'est un conteneur pour les actions (sous forme de rapport, formulaire ...).

La page d'accueil d'un serveur de commandes affiche les rapports de :

- mise à jour (sur tous les modules) ;
- mise à jour de listes de sites interdits sur le module Amon ;
- sauvegarde Bacula sur les modules Horus et Scribe ;
- importation sur le module Scribe.

Elle affiche également les diodes d'état du serveur (agents Zéphir).

Truc & astuce

Les agents Zéphir peuvent être consultés directement en utilisant l'adresse :

`http://<adresse_module>:8090`

4.2. Ajout/suppression de serveurs

Il est possible de connecter plusieurs serveurs de commandes à une même interface.

Une seule interface sert alors à administrer l'ensemble des serveurs EOLE d'un établissement.

Ajout/suppression de serveurs de commandes dans l'interface

L'interface de l'EAD est une coquille vide.

Elle permet de se connecter à des serveurs de commandes qui proposent des actions.

Lors de l'instanciation du serveur, le serveur de commandes du serveur est enregistré auprès de son interface.

La coquille n'est pas laissée vide.

Il est possible d'enregistrer plusieurs serveurs EOLE sur l'interface.

On obtient ainsi un point d'entrée unique pour administrer l'ensemble des serveurs d'un établissement.

Une seule interface web dans laquelle chaque onglet représente un des serveurs.

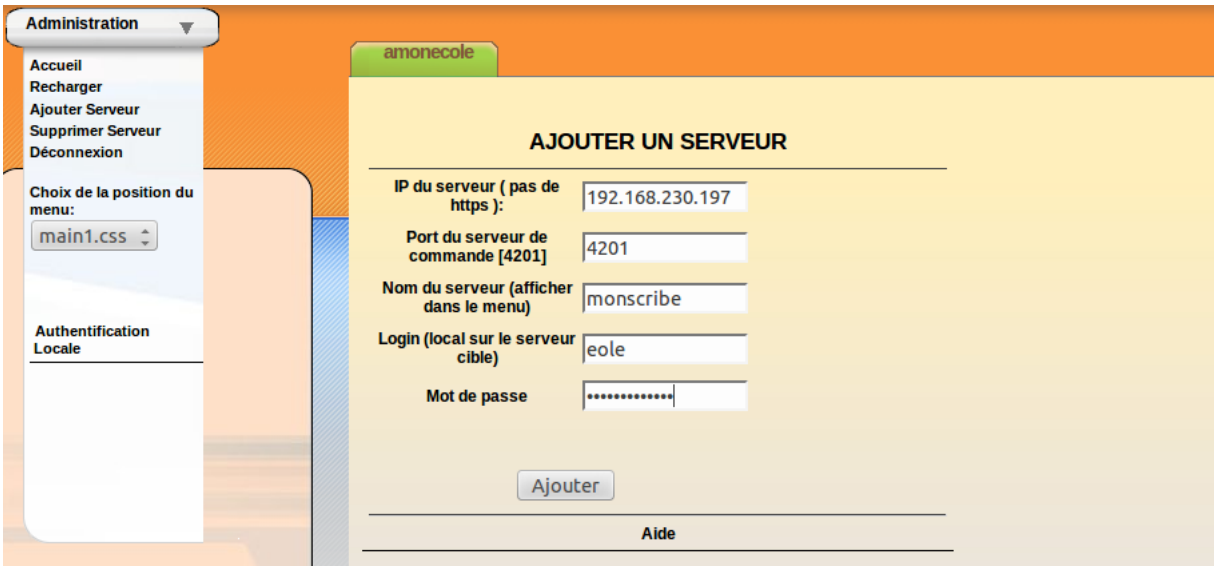
Il est ensuite possible de gérer les accès ainsi que les actions autorisées par utilisateur ou par groupe.

Ajout de serveur

Dans la gondole d'administration, cliquer sur *`Ajouter serveur`* et renseigner :

- l'IP du serveur ;

- le port du serveur de commandes (4201) ;
- le nom à afficher dans l'onglet ;
- le nom de l'utilisateur `eole` du serveur de commandes à enregistrer ;
- le mot de passe correspondant (sur le serveur à enregistrer).



Truc & astuce

Le compte `root` peut être utilisé à la place du compte `eole` pour toutes les manipulations présentées ici.

Suppression de serveur

Suppression normale

C'est le mécanisme de suppression classique. L'onglet du module est vert et on souhaite le retirer.

Dans la gondole d'administration, cliquer sur *`Supprimer Serveur`* :

- choisir le serveur à supprimer ;
- entrer le login `eole` du serveur de commandes à désinscrire ;
- entrer le mot de passe ;
- valider.

La référence sera supprimée côté interface et côté serveur de commandes.

Suppression forcée

Il ne faut utiliser la suppression forcée du serveur que si l'onglet est rouge ou que le mot de passe du serveur de commandes à supprimer est inconnu.

Attention

Il est préférable d'utiliser la suppression normale d'un serveur.

Dans la gondole d'administration, cliquez sur *`Supprimer Serveur`* :

- choisir le serveur à supprimer ;
- entrer le login (utilisez le compte `eole` du serveur de l'interface et non celui du serveur de commandes à désinscrire) ;
- entrer le mot de passe ;
- cocher la case *Forcer la désinscription* ;
- valider.

La référence ne sera supprimée que du côté de l'interface.

Désinscription forcée suite à un changement d'adresse IP

Si vous avez modifié l'adresse IP d'un serveur, il est possible que son onglet devienne rouge dans l'EAD.

Il faut alors utiliser la suppression forcée et ré-enregistrer le serveur.

4.3. Authentification locale et SSO

Dans l'EAD, il existe deux systèmes d'authentification :

- l'authentification unique (SSO*) ;
- l'authentification locale (PAM).

Dans le cas de l'authentification SSO, le serveur de commandes et l'interface se connectent à un même serveur d'authentification.

Pour se connecter en tant qu'*administrateur* :

- authentification SSO : l'utilisateur `admin` de l'annuaire associé au serveur sera utilisé ;
- authentification locale : les utilisateurs `root` et `eole` peuvent être utilisés.

4.3.1. Authentification locale

L'authentification locale est un mécanisme plus simple mais moins souple que l'authentification SSO. Il utilise les comptes système de la machine hébergeant le serveur de commandes. Le nombre d'utilisateurs et leur gestion est donc plus limitée.

L'authentification locale est systématiquement activée et peut être utilisé conjointement avec l'authentification SSO.

Pour vous authentifier localement, dans la gondole d'administration :

- cliquer sur *authentification locale* ;
- cliquer sur le nom de votre serveur.

Vous accédez alors au formulaire d'authentification locale.

Si le serveur SSO n'est pas activé, vous arriverez sur ce même formulaire en cliquant sur l'onglet.

Remarque

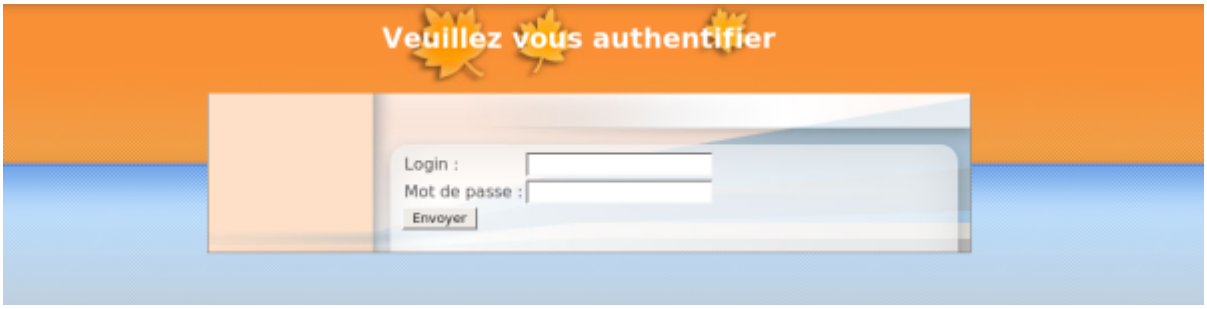
Il est possible d'utiliser la gestion des rôles pour déléguer une partie de l'administration à d'autres comptes systèmes.

4.3.2. L'authentification SSO

Connexion

Entrer l'adresse **https://<adresse_serveur>:4200** dans le navigateur et cliquer sur l'onglet du serveur à administrer.

Une re-direction vers le serveur SSO (**https://<adresse_serveur>:8443/**) est effectuée et le formulaire d'authentification apparaît :



L'utilisation d'un serveur SSO permet de centraliser l'authentification. En s'authentifiant une seule fois vous pouvez vous connecter aux différents serveurs de commandes enregistrés dans l'interface (naviguer d'un onglet à l'autre).

Les rôles permettent d'utiliser d'autres comptes pour se connecter (ex : sur Scribe, les professeurs ont un rôle prédéfini).

Remarque

Pour utiliser l'authentification SSO, il est indispensable que le serveur SSO utilisé par l'interface et par les serveurs de commandes qui y sont inscrits **soit identique**.

4.4. Redémarrer, arrêter et reconfigurer

Il est possible de redémarrer, arrêter ou reconfigurer un module EOLE directement depuis l'interface d'administration EAD.

Ces actions sont accessibles depuis *Système/Serveur*.

Remarque

Ces trois actions vous déconnectent de l'EAD.

Redémarrer un serveur

Reconfigurer un serveur

Arrêter un serveur

4.5. Mise à jour depuis l'EAD

Dans *Système* / *Mise à jour*, l'EAD propose une interface de mise à jour du serveur, il est possible de :

- de lister les paquets disponibles pour la mise à jour ;
- de programmer une mise à jour différée (dans 3 heures par exemple, ou dans 0 heure pour le faire tout de suite) ;
- d'activer / désactiver les mises à jour hebdomadaires (le jour et l'heure de la mise à jour automatique sont déterminés aléatoirement).

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.

Rapport de mise à jour

Penser à consulter le rapport de mise à jour et l'état des services sur la page d'accueil.

Reconfiguration et redémarrage automatique

Une mise à jour lancée depuis l'EAD exécute automatiquement une reconfiguration du serveur avec la commande **reconfigure**, il n'est donc pas nécessaire d'en lancer un par la suite comme c'est le cas depuis la console.

Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

4.6. Arrêt et redémarrage de services

Dans l'EAD, il existe deux manières d'arrêt ou de redémarrage des services : le mode normal et le mode expert.

4.6.1. Redémarrer ou arrêter des services (mode normal)

Création de groupes de services

Le nom des services, au sens système, n'est pas souvent parlant. Par exemple, il faut savoir qu'"apache2" est un serveur web.

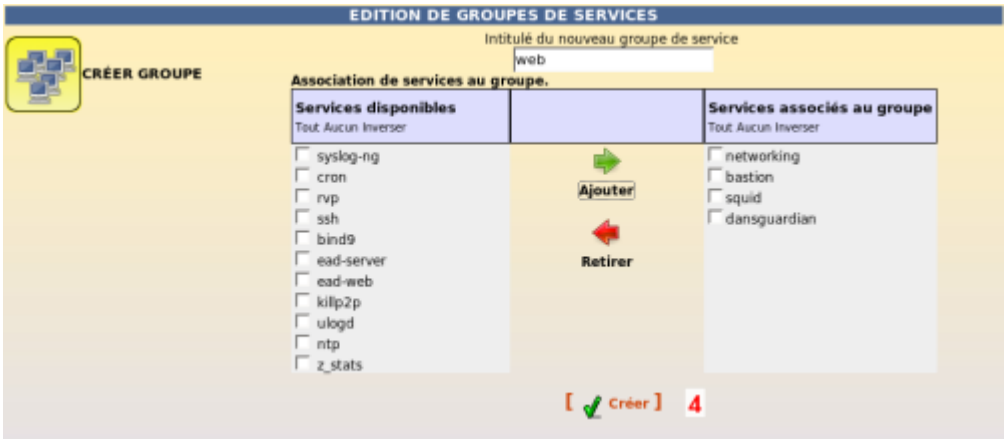
Les groupes de services permettent de regrouper un ou plusieurs services sous une dénomination claire. Cela permet de faciliter le redémarrage/arrêt de services.

Exemple

Création un groupe de services nommé "*web*" :

Pour créer un groupe, cliquer sur le bouton créer groupe dans *Système/Editeur de services* :

1. entrer le nom du groupe ;
2. choisir les services du groupe (cocher les cases) ;
3. cliquer sur la flèche verte ;
4. valider.



Remarque

Les groupes de services peuvent être modifiés ou supprimés en cliquent sur le nom du groupe listé en dessous du bouton créer groupe.

Redémarrer ou arrêter un groupe de services

Une fois créé, dans *Système/Services (mode normal)* on peut redémarrer ou arrêter le groupe de services voulu.

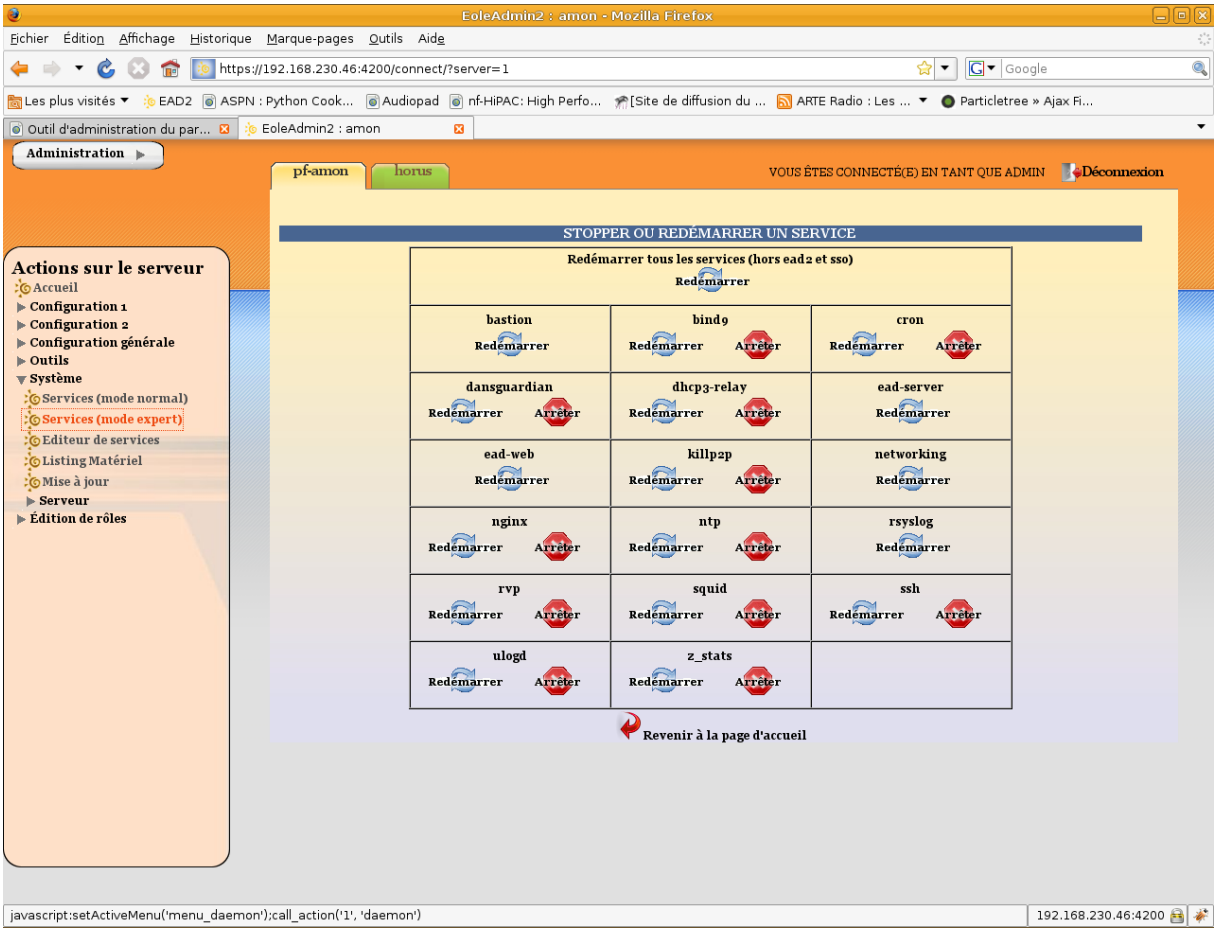
Remarque

La gestion des rôles permet de déléguer l'accès à des actions, on peut ainsi permettre à la documentaliste de redémarrer le logiciel BCDI.

Tous les groupes de services lui seront néanmoins accessibles.

4.6.2. Redémarrer ou arrêter des services (mode expert)

Dans *Système/Services (mode expert)*, cliquer sur le bouton *Arrêter* ou *Redémarrer* du service voulu.



Remarque

Les services liés au fonctionnement de l'EAD ne sont disponibles qu'en redémarrage. Sinon, vous perdrez tout accès à l'interface.

Pour relancer l'ensemble des services (sauf l'EAD et le serveur SSO) choisir le bouton : *`Redémarrer tous les services (hors EAD et SSO)`*.

4.7. Rôles et association de rôles

L'EAD est composé, comme nous l'avons vu précédemment, d'*actions*. Chaque action ayant un but bien précis.

L'EAD dispose d'un mécanisme de délégation d'*actions* à des utilisateurs bien déterminés.

Pour affecter certaines actions à un utilisateur, l'EAD utilise une mécanisme interne : les **rôles**.

Exemple

Par défaut sur un module EOLE, l'utilisateur "*admin*" est associé au rôle "*administrateur*".

Plusieurs rôles sont prédéfinis sur les modules EOLE :

- administrateur ;
- professeur (utilisé sur le module Scribe) ;
- élève (utilisé sur le module Scribe) ;
- administrateur de classe (utilisé sur le module Scribe) ;
- administratif dans Scribe (utilisé sur le module Scribe) ;
- administrateur du Scribe (utilisé sur le module AmonEcole) ;
- administrateur de l'Amon (utilisé sur le module Amon) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon).

4.7.1. Déclaration des actions

Les actions de l'EAD sont déclarées dans les fichiers : **/usr/share/ead2/backend/config/actions/actions_*.cfg**

Ces fichiers au format *texte* permettent de déclarer les fichiers python déclarant eux-mêmes des actions EAD à charger.

Ces fichiers sont situés dans **/usr/share/ead2/backend/actions** et ses sous-répertoires.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- **/usr/share/ead2/backend/config/actions.cfg** : fichiers des actions de base ;
- ainsi que tout les fichiers **actions_*.cfg** présents dans le répertoire **/usr/share/ead2/backend/config/actions**.

Syntaxe des fichiers

Les fichiers d'action sont déclarés avec leur chemin court depuis **/usr/share/ead2/backend/actions** et sans l'extension ".py".

Exemple

La déclaration des fichiers d'action suivants :

- **/usr/share/ead2/backend/actions/mes_actions.py**

- **/usr/share/ead2/backend/actions/repertoire/autres_actions.py**

prend la forme suivante dans le fichier **actions_perso.cfg** :

```
$ cat /usr/share/ead2/backend/actions/actions_perso.cfg
mes_actions
repertoire/autres_actions
```

4.7.2. Gestion des rôles

Les rôles de l'EAD sont déclarés dans les fichiers : **/usr/share/ead2/backend/config/perms/perm_*.ini**

Ces fichiers au format *ini* permettent d'associer des actions (permissions) à un ou plusieurs rôles.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- **/usr/share/ead2/backend/config/perm.ini** : rôles de base ;
- **/usr/share/ead2/backend/config/perm_local.ini** : rôles déclarés localement (édition manuelle ou via l'EAD) ;
- **/usr/share/ead2/backend/config/perm_acad.ini** : rôles déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers **perm_*.ini** présents dans le répertoire **/usr/share/ead2/backend/config/perms**.

Syntaxe des fichiers

Les permissions associent un rôle à une ou plusieurs actions.

Les fichiers **perm*.ini** doivent posséder une section `[role]` et une section `[permissions]`.

Exemple

```
[role]
nom_du_role = libelle du role
[permissions]
action1 = nom_du_role
action2 = nom_du_role
```

Création de rôle via l'EAD

L'interface EAD permet de créer des rôles personnalisés.

Ces rôles ne sont, en fait, qu'une liste d'actions regroupées sous un intitulé et un libellé unique.

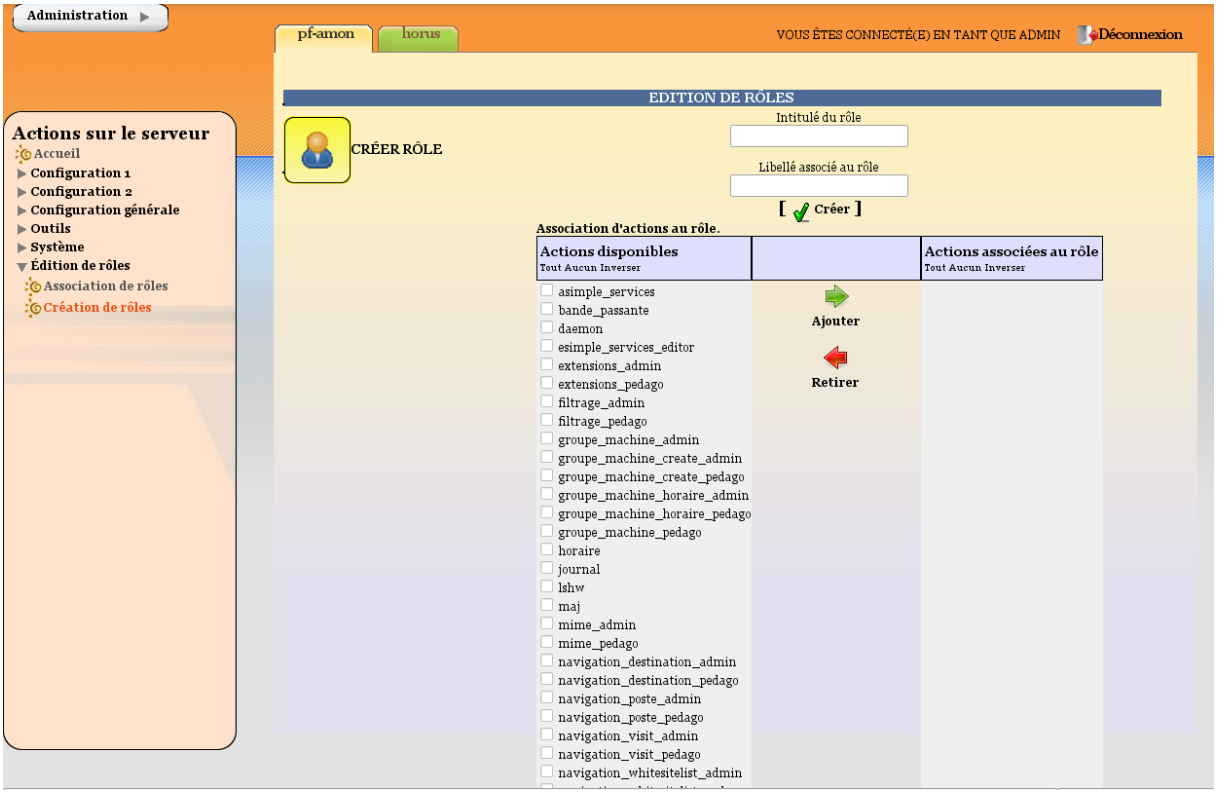
Il est possible, dans un deuxième temps d'associer ces rôles à des utilisateurs.

Pour créer un nouveau rôle cliquer sur :

- *Édition de rôles/Création de rôles*

puis

- *Créer rôle*
- entrer l'intitulé (le nom) du rôle (sans caractère spécial, sans accent et sans espace) ;
- entrer un libellé (courte description) du rôle ;
- cocher les actions à autoriser ;
- ajouter ;
- créer.



Actions obligatoires

Certaines actions doivent être obligatoirement permises pour tous les utilisateurs :

- help : utilisé notamment pour l'affichage d'aide ;
- main_status : page d'accueil appelée par défaut, elle gère un rôle prof (n'affiche pas les états de services) et un rôle admin ;
- update_ead : outil de téléchargement des javascripts, CSS, images spécifiques au module.

Actions communes aux différents modules

- lshw : listing matériel ;
- maj : action de mise à jour ;
- daemon : relancer des services (mode expert) ;
- simple_services_editor : éditer des groupes de services pour le mode simplifié ;
- simple_services : redémarrer/arrêter les services (mode simplifié) ;
- server-configure/server-reboot/server-stop : redémarrer/arrêter/reconfigurer le serveur ;
- role_editor : création de rôles ;
- role_manager : association de rôle (appelée par d'autres actions).

Actions spécifiques au module Amon

La modification du système de filtrage sur Amon apporte de profondes modifications sur ce module.

Selon les choix effectués lors de la phase de configuration (gen_config), vous pouvez choisir d'utiliser une ou deux zones de configuration pour le filtrage et les options du pare-feu.

La zone 1 correspond à 'admin' et la zone 2 correspond à 'pedago'.

Menu configuration

- postes
  - navigation_poste_admin (ou pedago) : action de gestion des postes à interdire ;
  - navigation_destination_admin (ou pedago) : interdire des destinations.
- groupe de machine
  - groupe_machine_admin (ou pedago) : action d'entrée pour la gestion des groupes de machine (gère des restrictions pour le rôle prof) ;
  - groupe_machine_create_admin (ou pedago) : action de création de groupe de machine (nécessite groupe_machine) ;
  - groupe_machine_horaire_admin (ou pedago) : action de gestion des horaires pour les groupes de machine.
- utilisateurs
  - navigation_banned_user_admin (ou pedago) : action de gestion des utilisateurs à interdire ;
  - navigation_moderateur_admin (ou pedago) : action de gestion des modérateurs ;
  - navigation_whitelist_admin (ou pedago) : action de gestion des utilisateurs en liste blanche ;
  - navigation_whitesitelist_admin (ou pedago) : action de gestion des sites en liste blanche.
- sites
  - opt_filters_admin (ou pedago) : gestion des filtres optionnels pour la zone de configuration 1 (ou 2) ;
  - filtrage_admin (ou pedago) : gestion du mode de filtrage syntaxique pour la zone de configuration 1 (ou 2) ;
  - sites_interdits_admin (ou pedago) : gestion des sites interdits pour la zone de configuration 1 (ou 2) ;
  - sites_autorises_admin (ou pedago) : gestion des sites autorisés pour la zone de configuration 1 (ou 2) ;
  - extensions_admin (ou pedago) : gestion des extensions interdites pour la zone de configuration 1 (ou 2) ;
  - mime_admin (ou pedago) : gestion des types mime interdits pour la zone de configuration 1 (ou 2).
- règles du pare-feu
  - regles : mode de fonctionnement du pare-feu ;

- peertopeer : autorisation/interdiction du peer to peer ;
- horaire : horaire de fonctionnement du pare-feu.

Menu outils

- navigation_visit : action de consultation des logs ;
- filtrage_bayes : action d'évaluation d'URL à l'aide du filtrage bayésien ;
- bande_passante : outil de test de bande passante.

Actions spécifiques au module Scribe

- Gestion des utilisateurs
  - scribe_user_create : action de création ;
  - scribe_user_list : renvoie le formulaire de recherche par critères qui appelle scribe_user_table pour la validation ;
  - scribe_user_table : action de listing d'utilisateur (gère les rôles prof_admin et admin) appelle scribe_user_modify, scribe_user_delete, scribe_user_password ;
  - scribe_user_modify : action de modification d'utilisateur (utilisée par scribe_user_table gère les rôles prof_admin et admin) ;
  - scribe_user_delete : action de suppression d'utilisateur. (gère les rôles prof_admin et admin) ;
  - scribe_user_password : action de modification de mot de passe. (gère les rôles prof, prof_admin et admin).
- Actions restreintes (créées pour les professeurs et les professeurs admins, gère le rôle de prof et prof_admin)
  - scribe_prof_preference : préférences du professeur connecté (mot de passe, inscription aux groupes, mail) ;
  - scribe_prof_mod_mail : modifie le mail d'un professeur (nécessite scribe_prof_preference) ;
  - scribe_prof_mod_groupe : Inscription du prof connecté aux groupes ;
  - scribe_prof_user : action d'entrée pour la gestion des utilisateurs par les profs lien vers scribe_prof_user_create et scribe_prof_user_modify ;
  - scribe_prof_user_create : action de création d'utilisateur (nécessite scribe_prof_user) ;
  - scribe_prof_user_modify : action d'entrée pour la modification des utilisateurs (nécessite scribe_prof_user) ;
  - scribe_grouped_edition : action d'entrée pour l'édition groupée d'utilisateur (appelle scribe_user_table).
- Gestion des groupes
  - scribe_group_create : création de groupes, niveau, classe..., appelle scribe_group_list ;
  - scribe_group_list : liste les groupes, appelle scribe_group_delete, appelle scribe_group_create ;
  - scribe_group_modify : modification de groupe ;

    - scribe_group_delete : suppression de groupe ;
    - scribe_prof_group : entrée pour la gestion des groupes par un prof_admin ou un prof, appelle scribe_prof_user_modify et scribe_prof_group_create ;
    - scribe_prof_group_create : action de création de groupe par un prof_admin.
- Gestion des partages
    - scribe_share : attribution de lettre de lecteur à un partage.
- Gestion des stations et connexions
    - scribe_station : action de suppression forcée de station du domaine ;
    - scribe_extraction : action d'extraction sconet ;
    - scribe_connexion_index : page d'accueil des observations des connexions ;
    - scribe_connexion_machine : page d'affichage des machines connectées ;
    - scribe_connexion_quota : observation des quotas ;
    - scribe_connexion_virus : affiche la liste les virus repérés ;
    - scribe_connexion_history : affiche l'historique des connexions.
- Autres actions
    - scribe_devoir_distribuer / scribe_devoir_ramasser / scribe_devoir_rendre / scribe_devoir_supprimer : gestion des devoirs ;
    - bacula : action de programmation de sauvegarde ;
    - bacula_config : action de configuration de sauvegarde ;
    - scribe_sympa : action renvoyant des liens pour l'interface de gestion de listes de diffusion ;
    - printers : action de gestion simplifiée des imprimantes.

Actions spécifiques au module Horus

- Gestion des connexions
    - isis : action d'entrée pour l'interface d'observation des connexions, appelle les actions isis ;
    - isis_stop : action d'arrêt de toutes les connexions ;
    - isis_disconnect : action de déconnexion d'utilisateur connectés au domaine ;
    - isis_sendmsg : action d'envoi de message à des utilisateurs connectés ;
    - isis_machine : action de listing des machines connectées au domaine (client, maitres explorateurs...) ;
    - isis_login : action d'autorisation des utilisateurs par login ;
    - isis_quota : action d'affichage des quotas ;
    - gestion_index : action d'entrée vers les gestions d'utilisateur, groupe, partage, appelle les actions gestion.
- Gestion des utilisateurs

- gestion_user_modify: action de modification d'utilisateur ;
- gestion_user_create: action de création d'utilisateur ;
- gestion_user_suppr: action de suppression d'utilisateur.

- Gestion des partages
  - gestion_share_create: action de création de partage ;
  - gestion_share_modify: action de modification de partage ;
  - gestion_share_suppr: action de suppression de partage.
- Gestion des groupes
  - gestion_group_create: action de création de groupe ;
  - gestion_group_modify: action de modification de groupe ;
  - gestion_group_suppr: action de suppression de groupe.
- Autres actions
  - gestion_account_suppr: action de suppression forcée de compte ;
  - extraction_aaf: action pour l'extraction AAF ;
  - bacula: action programmation de sauvegarde ;
  - bacula_config: action de configuration de Bacula pour la sauvegarde ;
  - scripts_admin: action pour l'exécution de scripts d'administration ;
  - printers: action de gestion des imprimantes.

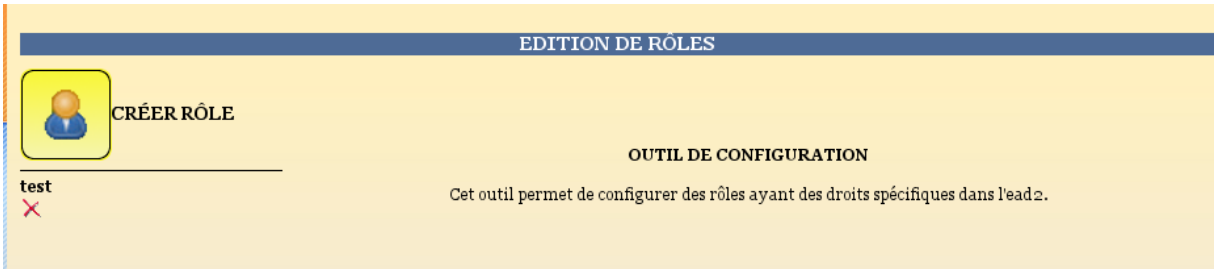
Actions spécifiques au module Seshat

Menu Messagerie

- routes : gestion du routage des messages vers les établissements de l'Académie.

Modification et suppression de rôle via l'EAD

- Pour modifier un rôle, il suffit de cliquer sur le nom voulu ;
- pour le supprimer, cliquer sur la croix rouge associée.



4.7.3. Association des rôles

Les associations de rôle de l'EAD sont déclarées dans les fichiers : **/usr/share/ead2/backend/config/roles/roles_*.ini**

Ces fichiers au format *ini* permettent d'associer des rôles à un ou plusieurs utilisateurs.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- **/usr/share/ead2/backend/config/roles.ini** : associations de base (admin, eleve, prof, ...) ;
- **/usr/share/ead2/backend/config/roles_local.ini** : associations déclarés localement (édition manuelle ou via l'EAD) ;
- **/usr/share/ead2/backend/config/roles_acad.ini** : associations déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers **roles_*.ini** présents dans le répertoire **/usr/share/ead2/backend/config/roles**.

Syntaxe des fichiers

L'association d'un rôle se fait à partir du login d'un utilisateur système (section `[pam]`) ou de la valeur associée à un attribut ldap (section `[nom_attribut]`) de l'annuaire utilisé pour l'authentification SSO sur l'EAD du module.

Exemple

```
[pam]
scribe2=admin
[uid]
jean.dupont=prof_admin
[user_groups]
minedu=admin_horus
```

Remarque

La clé spéciale `[user_groups]` permet d'attribuer un rôle à tous les membres d'un groupe déclaré dans l'annuaire LDAP.

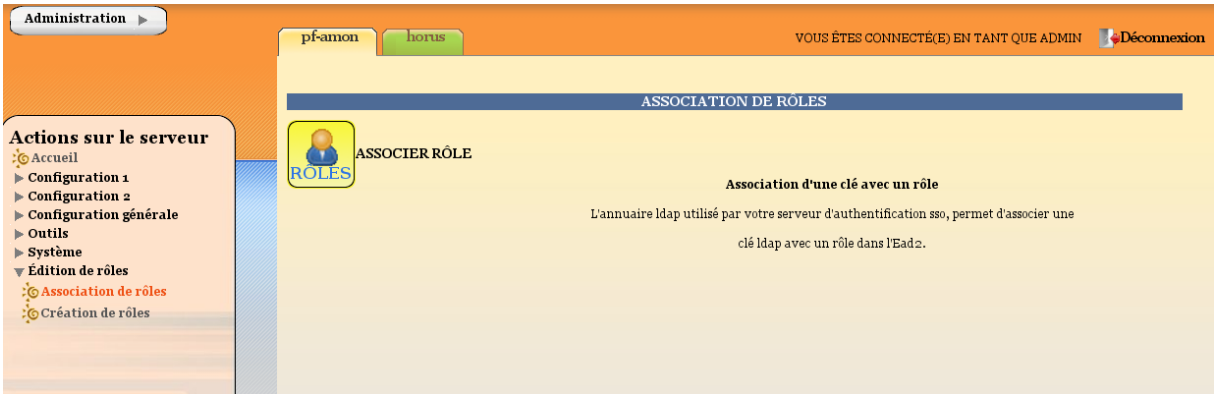
Création d'association via l'EAD

Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

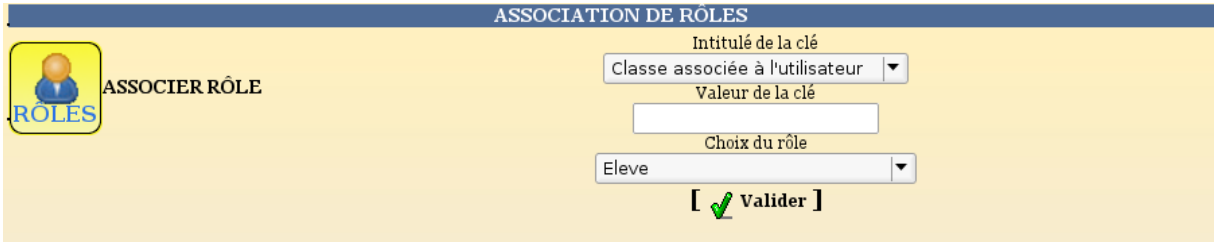
Certaines de ces informations sont utilisées pour lui attribuer des rôles et ainsi lui donner accès à certaines actions.

Pour associer un rôle à des utilisateurs:

- dans *Édition des rôles/Association de rôle* ;
- cliquer sur *Associer Rôle*.



- choisir la clef (attribut de l'utilisateur) ;
- renseigner la valeur recherchée pour cet attribut (dans le cas d'une authentification locale on mettra le login de l'utilisateur) ;
- choisir le rôle à associer ;
- valider.



L'intitulé de la clef dépend du système d'authentification utilisé pour se connecter :

Authentification locale :

- le login de l'utilisateur.

Authentification SSO :

- l'élève fait partie de la classe ;
- la valeur de la clé typeadmin (elle indique si un professeur est professeur principal dans une classe) ;
- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.

Il existe quelques limitations dans l'affectation des rôles :

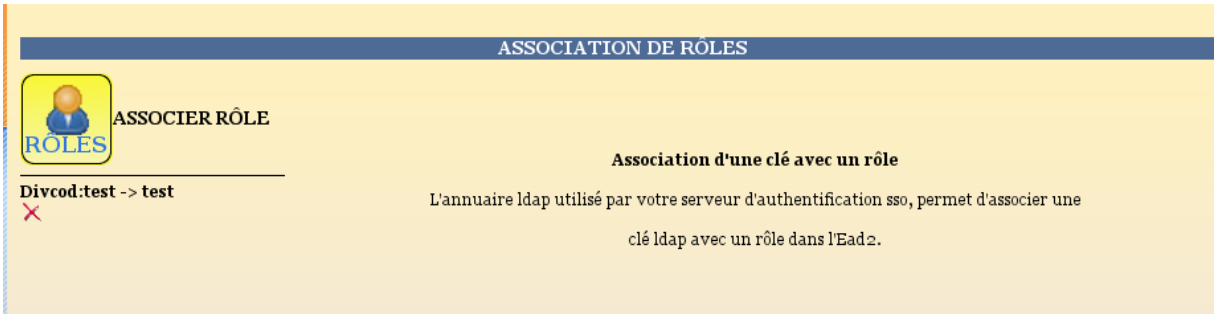
- un utilisateur nommé "*admin*" sera administrateur ;
- un utilisateur ayant une clé "*typeadmin*" de valeur **0** aura le rôle "*professeur*".

Remarque

Il est indispensable de redémarrer le service ead-server dans `Système->Services (mode expert)` pour que les modifications soient prises en compte.

Suppression d'une association via l'EAD

Une association de rôle peut par la suite être supprimée en cliquant sur la croix rouge.



4.7.4. Les rôles sur le module Scribe

L'EAD est accessible aux utilisateurs *root* et *eole* (authentification locale), *admin* et à tous les *professeurs* (authentification SSO).

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Il existe, par défaut, 3 rôles dans l'EAD :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS ;
- responsable de classe : en plus des actions "professeur", peut ré-initialiser le mot de passe des élèves des classes dont il est responsable.

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

L'EAD, dans son mode le plus complet, présente les fonctions suivantes :

- distribution de devoirs ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/Sconet/AAF/BE1D ;
- gestion des quotas ;
- observation des virus ;
- gestion des listes de diffusion ;
- modification du mode de contrôle des élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur.

Accès "professeur"

Un professeur dispose d'actions permettant de configurer ses propres paramètres.

Les fonctions disponibles :

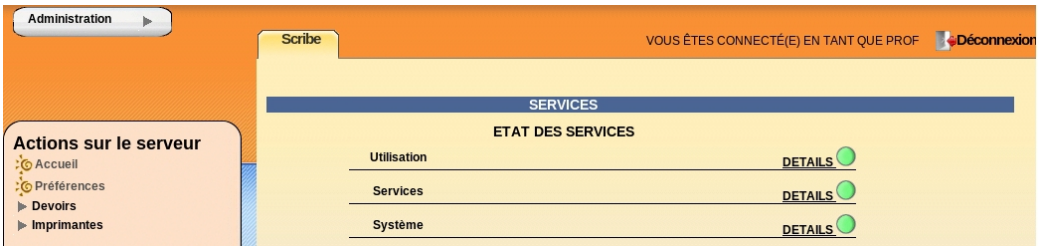
- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS).

L'item *Préférences* permet à un professeur de :

- modifier son mot de passe ;
- s'inscrire/se désinscrire d'un groupe ;
- renseigner/modifier son adresse mail.

Le mot de passe peut également être modifié depuis une station cliente Windows en faisant *Ctrl+Alt+Suppr => Modifier le mot de passe*.

L'adresse mail est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.



Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.

Remarque

Un professeur peut être responsable de plusieurs classes.

Une classe peut se voir affecter plusieurs responsables.

4.7.5. Les rôles sur le module Amon

L'EAD est accessible aux utilisateurs *root* et *eole* (authentification locale), *admin* et à tous les *professeurs* (authentification SSO).

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Il existe, par défaut, 3 rôles dans l'EAD :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- administrateur de l'Amon (utilisé sur le module Amon) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon).

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

L'EAD, dans son mode le plus complet, présente les fonctions suivantes :

- distribution de devoirs ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/Sconet/AAF/BE1D ;
- gestion des quotas ;
- observation des virus ;
- gestion des listes de diffusion ;
- modification du mode de contrôle des élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;

- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur.

Accès "administrateur de l'Amon"

Cette partie n'est pas encore documentée #fixme

Accès "administrateur du réseau pédagogique"

Cette partie n'est pas encore documentée #fixme

4.7.6. Les rôles sur le module AmonEcole

L'EAD est accessible aux utilisateurs *root* et *eole* (authentification locale), *admin* et à tous les *professeurs* (authentification SSO).

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Il existe, par défaut, 7 rôles dans l'EAD :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS ;
- responsable de classe : en plus des actions "professeur", peut ré-initialiser le mot de passe des élèves des classes dont il est responsable ;
- administratif dans Scribe ;
- administrateur du Scribe ;
- administrateur de l'Amon ;
- administrateur du réseau pédagogique.

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

L'EAD, dans son mode le plus complet, présente les fonctions suivantes :

- distribution de devoirs ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/Sconet/AAF/BE1D ;
- gestion des quotas ;
- observation des virus ;
- gestion des listes de diffusion ;
- modification du mode de contrôle des élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur.

Accès "professeur"

Un professeur dispose d'actions permettant de configurer ses propres paramètres.

Les fonctions disponibles :

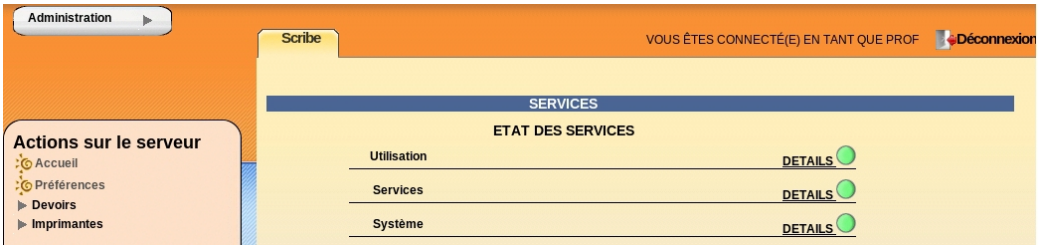
- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS).

L'item *Préférences* permet à un professeur de :

- modifier son mot de passe ;
- s'inscrire/se désinscrire d'un groupe ;
- renseigner/modifier son adresse mail.

Le mot de passe peut également être modifié depuis une station cliente Windows en faisant *Ctrl+Alt+Suppr => Modifier le mot de passe*.

L'adresse mail est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.



Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.

Remarque

Un professeur peut être responsable de plusieurs classes.

Une classe peut se voir affecter plusieurs responsables.

Accès "administrateur de Scribe"

Cette partie n'est pas encore documentée #fixme

Accès "administrateur de l'Amon"

Cette partie n'est pas encore documentée #fixme

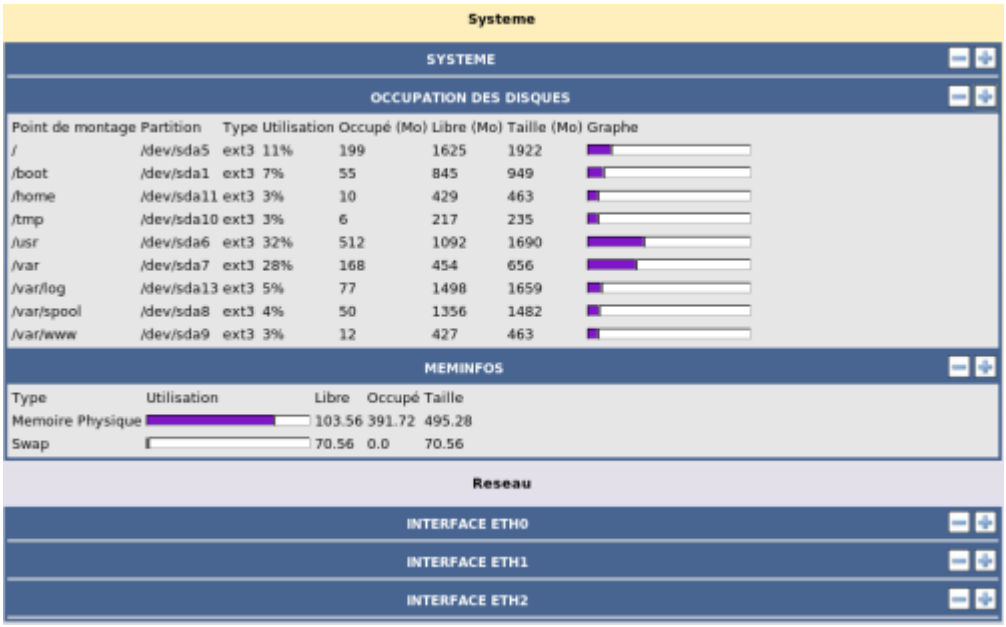
Accès "administrateur du réseau pédagogique"

Cette partie n'est pas encore documentée #fixme

4.8. Listing matériel

Le listing matériel permet de visualiser les éléments matériels du serveur.

Il indique notamment l'occupation des disques, de la mémoire vive et de la partition swap.



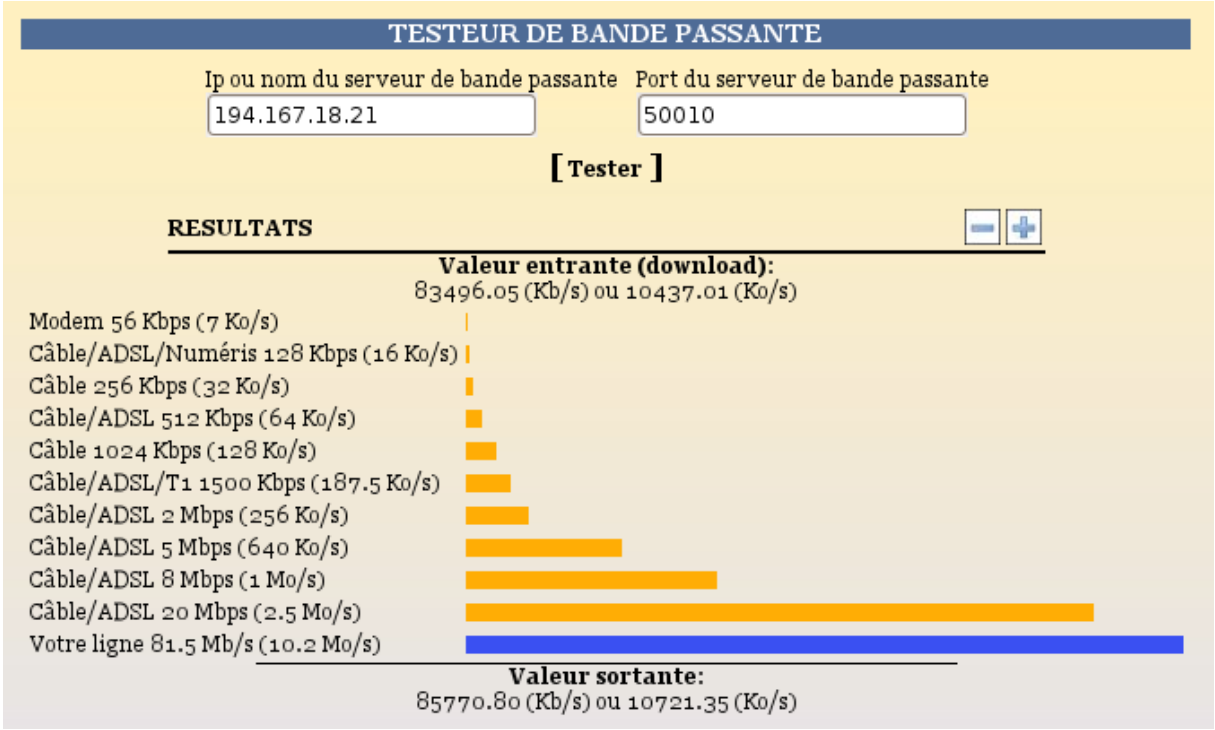
La mémoire physique (RAM)

Le noyau Linux* utilise un système de cache mémoire pour limiter les accès disque. Le chiffre "mémoire physique" comprend ce cache. Cela signifie qu'il n'est pas inquiétant de voir une valeur proche de 100%.

Le critère important étant l'occupation le swap (mémoire virtuelle). Une utilisation du swap indique que le serveur manque de RAM. Il faut alors envisager d'en augmenter la quantité ou chercher à alléger la charge de la machine.

4.9. Bande passante

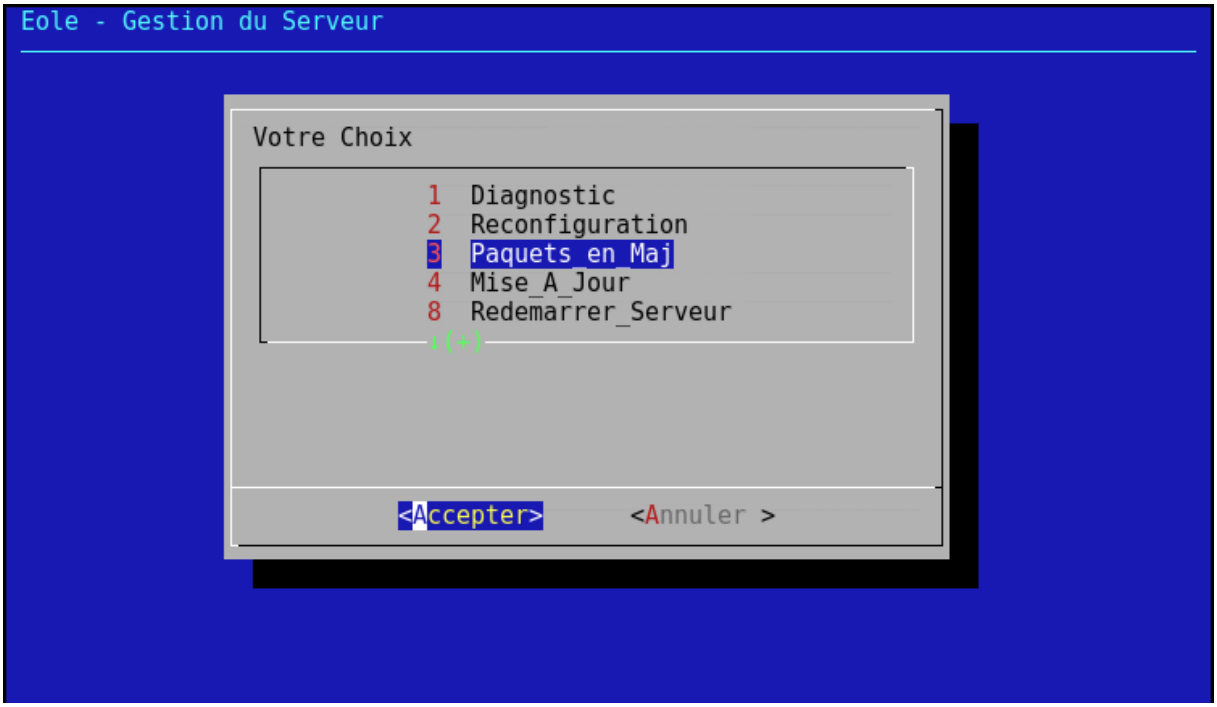
Le menu *Outils/Bande passante* permet de tester la bande passante dont dispose le serveur.



5 L'interface d'administration semi-graphique

En plus de l'EAD, une interface semi-graphique est disponible.

Cette interface (`manage-eole`) permet d'exécuter quelques tâches simples d'administration du serveur : diagnostique, mise à jour, liste des paquets en mise à jour, etc.



Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ...

6 Les mises à jour

6.1. Les différentes mises à jour

Sur les modules EOLE, il faut différencier :

- les paquets provenant d'Ubuntu :
  - stables (lucid) ;
  - mises à jour de sécurités (lucid-security) ;
  - mises à jour de fonctionnalités (lucid-updates).
- les paquets provenant d'EOLE :
  - stables (eole-2.3) ;
  - mises à jour de sécurités (eole-2.3-security) ;
  - mises à jour de fonctionnalités (eole-2.3-updates) ;
  - paquets candidats à la mise à jour (eole-2.3-proposed) ;
  - paquets de développements (eole-2.3-dev).

Les mises à jour stables

En ce qui concerne les mises à jour EOLE on peut distinguer deux modes qui n'ont pas de conséquence sur les mises à jour Ubuntu :

- le mode **mise à jour minimum** contient :
  - les mises à jour de sécurités EOLE dès leur publication ;
  - les mises à jour fonctionnelles à chaque publication d'une nouvelle image ISO :
    - beaucoup d'améliorations et de nouveautés ;
    - beaucoup de corrections de dysfonctionnements mineurs ;
    - beaucoup de paquets mis à jour.
- le mode **mise à jour complète** contient :
  - les mises à jour de sécurité EOLE dès leur publication ;
  - les mises à jour fonctionnelles dès leur publication :
    - améliorations et nouveautés ;
    - corrections de dysfonctionnements mineurs ;
    - peu de paquets mis à jour.

À chaque génération d'une nouvelle image ISO, tous les paquets du mode mise à jour complète sont reversés et proposés dans le mode mise à jour minimale.

Par défaut, sur EOLE 2.3, le mécanisme de mise à jour va chercher les paquets sur les dépôts suivants :

- lucid, lucid-security, lucid-updates
- eole-2.3, eole-2.3-security, eole-2.3-updates

Attention

Le passage de mise à jour minimum à mise à jour complète ne pose pas de problème.

Par contre, il est fortement déconseillé de passer de mise à jour complète à mise à jour minimum.

Les mises à jour candidates

Les mises à jour candidates sont les futures mises à jour stables. En attendant leur publication elles sont proposées à l'évaluation par tout un chacun. Les paquets proposés ont été testés et qualifiés par l'équipe. Cependant il peut rester des cas d'utilisation non testés ou des dysfonctionnements qui auraient échappés à la vigilance de l'équipe.

Il est très important que des utilisateurs testent les mises à jour candidates et fassent un retour à l'équipe sur les listes de diffusions. Si un éventuel dysfonctionnement est signalé sur les listes ou sur la forge, il sera pris en charge et traité spécifiquement avant la publication définitive en stable.

Sur EOLE 2.3, le mécanisme de mise à jour va chercher les paquets sur les dépôts par défaut et la demande de mise à jour en candidate ajoute le dépôt eole-2.3-proposed.

Attention

Les mises à jour candidates sont susceptibles d'apporter quelques dysfonctionnements.

Il n'est pas conseillé de les utiliser sur un serveur en production.

Les mises à jour de développement

Les mises à jour en développement sont destinées aux développeurs EOLE.

Certains des paquets peuvent ne pas être utilisables du tout.

Sur EOLE 2.3, le mécanisme de mise à jour va chercher les paquets sur les dépôts par défaut et la demande de mise à jour en développement ajoute le dépôt eole-2.3-dev.

Attention

Les mises à jour de développement sont susceptibles de rendre le serveur instable.

Il est fortement déconseillé de les utiliser sur un serveur en production.

> "cf Les dépôts EOLE", page 264.

6.2. Les procédures de mise à jour

À la fin de l'instanciation d'un module, une mise à jour hebdomadaire est configurée automatiquement. Mais il est possible de passer des mises à jour manuellement.

Les procédures de mise à jour des modules EOLE sont accessible de quatre manières :

- au travers de l'EAD ;
- avec interface semi-graphique ;
- depuis le serveur Zéphir ;
- en ligne de commande.

Intégrité de la mise à jour

Une mise à jour EOLE représente un ensemble de paquets : les dépendances. L'installation manuelle et forcée de seulement l'un d'entre eux peut rendre votre système instable.

L'utilisation des méthodes listées ci-dessus permet de garantir l'intégrité du serveur.

Mise à jour depuis l'EAD, avec l'interface semi-graphique et mise à jour automatique

> "cf Mise à jour depuis l'EAD", page 170.

> "cf L'interface d'administration semi-graphique", page 192.

> "cf Activation automatique des mises à jour hebdomadaire", page 132.

6.3. Les mises à jour en ligne de commande

Il est important de tenir son système à jour. Pour cela, il est possible de lancer manuellement une mise à jour.

Query-Auto et Maj-Auto

Query-Auto : affiche la liste des paquets à mettre à jour depuis le réseau ;

Maj-Auto : télécharge et/ou installe les paquets à mettre à jour depuis le réseau.

Ces deux scripts permettent également de tester les paquets candidats avec -C ou de développements avec -D.

Il est également possible de simuler l'installation (-s) ou seulement télécharger en cache les paquets (-d).

Truc & astuce

Si vous n'avez pas encore configuré votre module et que vous voulez d'abord mettre à jour, il faut utiliser les options suivantes :

`Maj-Auto -i -S eoleng.ac-dijon.fr`.

Reconfiguration

À la fin de l'exécution de la commande [Maj-Auto], si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur. La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état instable.

Reconfigurer le serveur remet en place la configuration correcte, telle que définie lors de la configuration du serveur.

Pour ce faire, exécuter la commande [reconfigure].

Query-Cd et Maj-Cd

[Maj-Cd] est le script à utiliser pour mettre un module à jour depuis un CD-Rom d'installation ou de mise à jour plus récent que celui utilisé pour l'installation mais d'une même version majeure (exemple : mettre à jour un serveur installé avec un CD X.X avec le CD X.X.1).

Query-Cd : affiche la liste des paquets à mettre à jour depuis un CD-ROM ;

Maj-Cd : installe les paquets à mettre à jour depuis un CD-ROM (sauf option -s).

Reconfiguration

À la fin de l'exécution de la commande [Maj-Cd], si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur. La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état instable.

Reconfigurer le serveur remet en place la configuration correcte, telle que définie lors de la configuration du serveur.

Pour ce faire, exécuter la commande [reconfigure].

Options de mise à jour

Options communes aux scripts de mise à jour

- -a : n'efface pas l'écran (clear) ;
- -f : force le blocage Zéphir ;
- -h : affiche l'aide ;
- -i : ignore le fichier de configuration **/etc/eole/config.eol** ;
- -V mode verbose (pour débogage) ;
- -W : génère une sortie HTML.

Options spécifiques aux scripts Maj-Auto et Query-Auto

- -C : force la mise à jour en candidate ;
- -D : force la mise à jour en développement ;

- -E : force la mise à jour complète ;
- -S : force le site de mise à jour (ex : -S monsite.fr).

Options spécifiques aux scripts Maj-Auto et Maj-Cd

- -d : télécharge uniquement les paquets ;
- -s : simulation (rien ne sera installé) ;
- -F : installation forcée (--force-yes) ;
- -r : lance la commande reconfigure si nécessaire ;
- -R : lance la commande reconfigure et redémarre le serveur si nécessaire.

Option spécifique aux scripts Query-Auto et Query-Cd

- -v : n'affiche pas la liste des paquets à mettre à jour.

Remarque

L'utilisation des options [-C] ou [-D] entraîne l'apparition d'une demande de confirmation.

6.4. Ajout de dépôts supplémentaires

Les outils `Query-Auto`, `Query-CD, Maj-Auto` et `Maj-Cd` réinitialisent systématiquement la liste des dépôts à utiliser pour les mises à jour (i.e. : le fichier **/etc/apt/sources.list**).

Il est possible d'ajouter des fichiers dans **/etc/apt/sources.list.d/**, cependant, ceux-ci ne seront pas pris en compte à l'intérieur des conteneurs.

A la place, il est recommandé de créer et d'utiliser le fichier spécial :

/etc/apt/sources.list.local.

Gestion des mises à jour avec Creole et eole-schedule

> "cf Gestion des tâches planifiées eole-schedule", page 250.

7 Installation manuelle de paquets

Maj-Auto installe l'ensemble des paquets disponibles pour la version de mise à jour désirée (Stable, Candidate, Développement).

Il est possible d'installer manuellement des paquets, pour n'en tester que certains par exemple.

Ceci se fait avec la commande :

`apt-eole`

Avant de procéder à l'installation d'un paquet, assurez-vous que les sources APT sont configurées sur la bonne version de mise à jour avec la commande `Query-Auto`.

- Mises à jour Stables : `Query-Auto`
- Mises à jour Candidates : `Query-Auto -C`
- Mises à jour de Développement : `Query-Auto -D`

Ensuite, pour installer le paquet "eole-bacula" (exemple), exécutez la commande :

```
apt-eole install eole-bacula
```

Intérêt de la commande "apt-eole"

La commande `apt-eole` a été ajoutée afin d'appeler la commande `apt-get` avec les bonnes options lors des appels **install** et **remove**.

Pour installer un paquet dans un conteneur, il faut utiliser l'option install-conteneur :

[apt-eole install-conteneur (nom_du_conteneur) paquet]

Le mode conteneur

XI Personnalisation

Les modules EOLE peuvent être personnalisés et adaptés afin de prendre en compte les spécificités rencontrées en production.

1 Panorama des services disponibles

Les services disponibles sur les modules EOLE 2.3 ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE 2.3 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 un module EoleBase.

1.1. Services liés aux bases de données

1.1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un serveur OpenLDAP.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

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 et Seshat, 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)**.

1.1.2. 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.

Historique

Utilisé à la base sur les modules Horus, Scribe et Sentinelle, le paquet **eole-mysql** est désormais 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)**.

1.1.3. eole-postgresql

Attention

La création d'un paquet spécifique **eole-postgresql** permettant la mise en place d'un serveur de bases de données PostgreSQL est prévue mais n'a pas encore été réalisée.

De ce fait les configurations EOLE pour ce service sont toujours imbriquées dans le paquet **conf-zephir**.

Logiciels et services

Le paquet devrait s'appuyer sur le service postgresql-8.4.

Historique

Ce service est uniquement utilisé sur Zéphir.

Conteneurs

L'identifiant de conteneur `"id=11"` a été réservé pour ce service mais pour l'instant, celui-ci n'est pas fonctionnel s'il est installé dans un conteneur.

1.1.4. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de bases de données Interbase.

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)`

1.2. Services liés aux serveurs de fichiers

1.2.1. eole-fichier

Le paquet `eole-fichier` permet la mise en place d'un serveur de fichiers complet.

Attention

Il est probable que ce paquet soit, un jour, découpé en plusieurs sous-paquets (un par logiciel) afin d'améliorer la modularité et la maintenance des outils qu'ils contient.

Logiciels et services

Le paquet `eole-fichier` permet de gérer les services suivants :

- smbd, nmbd et scannedonly (serveur de fichiers) ;
- nscd (cache) ;
- cups (serveur d'impressions) ;
- proftpd (serveur FTP) ;

Historique

Les services fournis sont spécifiques aux modules Horus et Scribe.

Grâce au paquet `eole-fichier`, 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)`.

Attention

En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.2. 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.

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.

1.2.3. eole-nfs

Le paquet `eole-nfs` permet la mise en place d'un serveur NFS (partage de fichiers en réseau).

Logiciels et services

Le paquet `eole-nfs` s'appuie sur le service nfs-kernel-server.

Historique

L'installation et l'activation de ce service sur Scribe 2.3 est obligatoire si l'on souhaite accéder aux partages par le biais d'un serveur Eclair 2.3 : http://dev-eole.ac-dijon.fr/projects/eole/wiki/Eclair23

Conteneurs

Le service s'installe sur système hôte (maître) et non dans un conteneur.

Remarques

Le protocole NFS étant peu sécurisé, il est recommandé de ne pas ouvrir ce service sur l'intégralité du réseau.

1.3. Services web

1.3.1. eole-web

Le paquet `eole-web` permet la mise en place d'un serveur web.

Attention

L'installation d'`eole-web` entraîne celle d'`eole-mysql`.

Logiciels et services

Le paquet eole-web s'appuie principalement sur le service apache2.

Il permet également d'activer l'application phpMyAdmin.

Historique

A 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.

1.3.2. eole-tomcat

Le paquet `eole-tomcat` permet la mise en place d'un serveur web Tomcat.

Attention

Le module Sentinelle n'ayant pas été porté en version 2.3, ce paquet doit être considéré comme **expérimental**.

Logiciels et services

Le paquet `eole-tomcat` s'appuie principalement sur le service tomcat6.

Historique

Historiquement ce service est uniquement utilisé sur le module Sentinelle.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `tomcat (id=19)`.

1.3.3. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, Nginx*, peut aussi faire office de serveur web.

http://nginx.org/

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.4. Services liés à la messagerie

1.4.1. 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.

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.2. eole-spamassassin

Le paquet `eole-spamassassin` permet la mise en place d'un serveur anti-spam.

Logiciels et services

Le paquet `eole-spamassassin` s'appuie principalement sur le service spamassassin.

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-spamassassin` est désormais installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.3. eole-courier

Le paquet `eole-courier` permet la mise en place d'un serveur POP/IMAP.

Logiciels et services

Le paquet `eole-courier` s'appuie principalement sur les services courier-imap et courier-pop.

Historique

Historiquement ces services sont uniquement utilisés sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Le greffon **authProg** fourni par le paquet `courier-eolecas` permet au serveur IMAP d'être compatible avec une authentification CAS.

1.4.4. eole-sympa

Le paquet `eole-sympa` permet la mise en place d'un serveur de listes de diffusion.

Logiciels et services

Le paquet `eole-sympa` s'appuie principalement sur le service sympa.

Son interface d'administration nécessite un serveur web apache2.

Attention

L'installation d'`eole-sympa` entraîne celle d'`eole-exim`.

Historique

Historiquement ce service est uniquement utilisé sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

1.5. Proxy et authentification

1.5.1. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- Dansguardian : filtrage web ;
- Lightsquid : analyseur de logs ;

- smbd, nmbd, winbind, krb5 : authentification NTLM/KERBEROS.

Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

Attention

En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_proxy_link`).

Remarques

Afin d'assurer l'authentification en mode NTLM/KERBEROS, ce paquet fournit des configurations Samba incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

1.5.2. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur Radius*.

Logiciels et services

Le paquet `eole-radius` s'appuie sur le projet FreeRADIUS.

http://freeradius.org/

Historique

Ce paquet est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le serveur maître.

1.5.3. eole-nuauth

Le paquet `eole-nuauth` permet la mise en place d'un serveur d'authentification réseau NuFW.

Logiciels et services

Le paquet `eole-nuauth` s'appuie sur les services nufw et nuauth.

Historique

Historiquement pré-installé sur le module Amon, ce paquet est désormais optionnel.

Conteneurs

Ces services s'installent sur le maître.

Remarques

Les projets NuFW et NuFirewall ont récemment été relancés par la FSF sous le nom UFWI : http://fsffrance.org/news/article2011-11-30.fr.html

1.6. Autres services réseau

1.6.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.

Attention

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://eoleng.ac-dijon.fr/documentations/eole-antivir.

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon et clamav-freshclam.

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirales (freshclam) s'installe sur le maître.

Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.

Sur 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)`.

Attention

C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.6.2. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9 (http://www.bind9.net/).

Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dns (id=18)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.6.3. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP.

Logiciels et services

Le paquet `eole-dhcrelay` s'appuie sur le service dhcp3-relay.

Historique

Ce service est pré-installé sur Amon.

Conteneurs

Le service s'installe sur le maître.

1.6.4. eole-pacemaker

Le paquet `eole-pacemaker` permet la mise en place d'un service de haute disponibilité*.

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync*.

Historique

A la base, le service de haute disponibilité était uniquement disponible sur le module Sphynx via le service Heartbeat. Celui-ci se fait maintenant via les logiciels Corosync* et Pacemaker. Le service a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service s'installe sur le serveur maître.

1.6.5. eole-snmpd

Le paquet **eole-snmpd** permet d'installer et de configurer un serveur SNMP.

Logiciels et services

Le paquet **eole-snmpd** s'appuie sur le service snmpd.

Historique

Ce service n'est pré-installé sur aucun module.

Il a été créé et mis à disposition pour répondre à un besoin exprimé par plusieurs académies.

Conteneurs

Le service s'installe sur le maître.

1.6.6. eole-vpn

Le paquet **eole-vpn** permet la mise en place d'un VPN*.

Logiciels et services

Le paquet **eole-vpn** s'appuie principalement sur le logiciel strongSwan*.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés ainsi que sur le module Sphynx.

Conteneurs

Le service s'installe sur le serveur maître.

2 Personnalisation du serveur à l'aide de Creole

Creole* est un ensemble d'outils permettant de mettre en œuvre un serveur suivant une configuration définie.

Il offre des possibilités de personnalisation, permettant à l'utilisateur d'ajouter des fonctionnalités sur le serveur sans risquer de créer une incohérence avec la configuration par défaut et les futures mises à jour.

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

- le **patch** : permettant de modifier un template* fournit par EOLE ;
- le **dictionnaire*** **local** permet d'ajouter des options à l'interface de configuration, d'installer de nouveaux paquets ou de gérer de nouveaux services ;
- le **template** *: reprend le fichier de configuration d'une application avec, éventuellement, une personnalisation suivant des choix de configuration.

2.1. Répertoires utilisés

Répertoires liés au logiciel Créole

Dictionnaires

- **/usr/share/eole/creole/dicos** : contient les dictionnaires fournis par la distribution ;
- **/usr/share/eole/creole/dicos/local** : contient les dictionnaires créés localement pour le serveur ;
- **/usr/share/eole/creole/dicos/variante** : contient les dictionnaires fournis par une variante Zéphir.

Templates

- **/usr/share/eole/creole/distrib** : contient tous les templates (distribution, locaux et issus de variantes) ;
- **/usr/share/eole/creole/modif** : répertoire à utiliser pour créer des patch avec l'outil `gen_patch` ;
- **/usr/share/eole/creole/patch** : contient les patch réalisés localement (avec ou sans l'outil `gen_patch`) ;
- **/usr/share/eole/creole/patch/variante** : contient les patch fournis par une variante Zéphir ;
- **/var/lib/eole** : répertoire recommandé pour le stockage des fichiers templatisés nécessitant un traitement ultérieur ;
- **/var/lib/creole** : contient la copie des templates après la phase de patch (traitement interne à Créole).

Autres répertoires spécifiques

- **/etc/eole** : contient les fichiers de configuration majeurs du module ;
- **/var/lib/eole/config** : contient les fichiers de configuration de certains outils internes ;
- **/var/lib/eole/reports** : contient des fichiers de rapport (pour affichage dans l'EAD, par exemple).

2.2. Création de patch

Si le fait de renseigner correctement les options de configuration n'offre pas une souplesse suffisante, il faut envisager des adaptations complémentaires.

Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à chaque `instance`/`reconfigure`.

Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch.

L'outils `gen_patch` vous permet de générer facilement un nouveau patch. Pour ce faire il suffit de copier le fichier de configuration depuis **/usr/share/eole/creole/distrib** vers **/usr/share/eole/creole/modif**, de le modifier et de lancer la commande `gen_patch`.

Une fois le patch créé, il faut lancer [reconfigure] pour que les nouvelles options soient prises en compte.

Remarque

Sont concernés par la procédure de patch uniquement les fichiers déjà présents dans le répertoire des templates et référencés dans les dictionnaires fournis par l'équipe EOLE.

Pour les autres fichiers, l'utilisation de dictionnaires locaux et de templates personnalisés est recommandée.

Le répertoire **/usr/share/eole/creole/** contient les répertoires suivants :

- **distrib** : templates originaux fournis principalement par le paquet conf d'un module ;
- **modif** : endroit où doivent être copiés et modifiés les templates souhaités ;
- **patch** : fichiers patch générés à partir des différences entre les deux répertoires précédents.

Le répertoire **/var/lib/creole** comprend les templates finaux, c'est à dire les templates initiaux avec éventuellement des patchs.

Truc & astuce

Pour désactiver un patch, il suffit de supprimer ou déplacer le fichier patch.

2.3. Les dictionnaires Creole

En cas d'ajout de templates* et de variables supplémentaires, il est nécessaire de créer un dictionnaire local.

Ce dictionnaire peut également comprendre des noms de paquet supplémentaire à installer ainsi que des services à gérer.

Un dictionnaire local est un dictionnaire personnalisé permettant d'ajouter des options à Creole.

Un dictionnaire Creole contient un en-tête XML suivi d'une balise racine **<creole></creole>**.

Structure générale d'un dictionnaire XML Creole

```
<?xml version='1.0' encoding='utf-8'?>
<creole>
    <files>
    </files>
    <containers>
    </containers>
    <variables>
    </variables>
    <constraints>
    </constraints>
    <help>
    </help>
</creole>
```

Truc & astuce

Il est toujours intéressant de regarder dans les dictionnaires présents sur le module pour comprendre les subtilités des dictionnaires Creole.

2.3.1. En-tête XML

L'en-tête est standard pour tous les fichiers XML :

```
<?xml version="1.0" encoding="utf-8"?>
```

Cet en-tête est nécessaire pour que le fichier soit reconnu comme étant au format XML.

Afin d'éviter les problème d'encodage, il est conseillé de créer le fichier sur un module EOLE (avec l'éditeur de texte vim).

> "cf L'éditeur de texte Vim", page 147.

2.3.2. Fichiers templates, paquets et services

Local ou conteneur

Creole propose un système de conteneurs permettant d'isoler certains services du reste du système.

C'est dans le dictionnaire que les conteneurs sont définis et associés à des services.

Si le conteneur n'est pas spécifié, les services seront installés sur le serveur hôte. Nous parlerons ainsi de services locaux.

Pour distinguer les fichiers templates, les paquets et les services locaux de ceux mis dans le conteneur, il faut utiliser deux balises différentes.

Dans le cas local, les fichiers templates, les paquets et le services sont dans une balise **<files>**.

Dans le cas des conteneurs, il faut spécifier un ensemble de balises **<container>** à l'intérieur d'une balise **<containers>**.

La balise **<container>** doit obligatoirement contenir l'attribut **name** pour renseigner le nom du conteneur.

Lors de la première déclaration d'un conteneur l'attribution d'un **id** est obligatoire.

La valeur de cet id permettra de calculer son adresse IP.

Le mode conteneur

Remarque

La liste des identifiants des conteneurs et des groupes de conteneurs déjà affectés est actuellement maintenue sur le wiki EOLE :

http://dev-eole.ac-dijon.fr/projects/creole/wiki/ContainersID

Paquets

Creole permet de spécifier les paquets à installer pour profiter d'un nouveau service.

A l'instanciation de la machine, les paquets spécifiés seront installés.

Pour cela, il faut utiliser la balise **<package>** avec comme contenu le nom du paquet.

Attention

Pour spécifier plusieurs paquets, il faut obligatoirement écrire une balise **<package>** par paquet.

Fichiers templates

Les fichiers templates sont définis dans la balise **<file>**.

Les attributs de la balise <file>

- l'attribut **name** (obligatoire) indique l'emplacement où sera copié le fichier ;
- l'attribut **source** permet d'indiquer un nom de fichier source différent de celui de destination ;
- l'attribut **mode** permet de spécifier des droits à appliquer au fichier de destination ;
- l'attribut **owner** permet de forcer le propriétaire du fichier ;
- l'attribut **group** permet de forcer le groupe propriétaire du fichier ;
- l'attribut **filelist** permet de conditionner la génération du fichier suivant des contraintes ;
- si l'attribut **rm** vaut *True*, le fichier de destination sera supprimé si il est désactivé via une *filelist* ;
- si l'attribut **mkdir** vaut *True*, le répertoire destination sera créé si il n'existe pas ;
- l'attribut **container_only** permet de ne généré le fichier qu'en mode conteneur (ne fonctionne pas dans la balise <files>, uniquement dans une balise <container>) ;
- l'attribut **del_comment** engendre la suppression des lignes vides et des commentaires dans le fichier cible afin d'optimiser sa templatisation (exemple : `del_comment='#'`).

La balise **name** comprend bien le nom du fichier de destination (par exemple **/etc/hosts**). Le fichier template devra s'appeler de la même façon que le fichier de destination (**hosts**). Si deux templates ont le même nom, il faudra spécifier le nom du template renommé avec l'attribut **source**.

Services

Les dictionnaires Creole intègrent un système de gestion de services GNU/Linux (scripts d'init) qu'il est possible d'utiliser pour activer/désactiver des services non gérés par le module EOLE installé.

Services non gérés : services non référencés dans le système de gestion des services de Creole. Ils ne sont jamais modifiés. Ils restent dans l'état dans lequel Ubuntu les a installés ou dans celui que leur a donné l'utilisateur. Les services non gérés sont généralement les services de base Ubuntu (rc.local, gpm, ...) et tous ceux pour lesquels le module ne fournit pas de configuration spécifique (mdadm, ...).

Services désactivés : services systématiquement arrêtés et désactivés lors des phases d'instance et de reconfigure. Les services concernés sont généralement liés à une réponse à "non" dans l'interface de configuration du module.

Services activés : services systématiquement activés et (re)démarrés lors des phases d'instance et de reconfigure. Les services concernés sont ceux nécessaires au fonctionnement du module.

Les services à activer/désactiver se définissent dans le dictionnaire grâce à la balise **<service>.**

Les attributs de la balise <service>

- l'attribut **startlevel** (entier) permet de spécifier le niveau de démarrage ;
- l'attribut **stoplevel** (entier) permet de spécifier le niveau d'arrêt ;
- l'attribut **servicelist** (chaîne de caractères alphanumériques) permet de conditionner le démarrage ou l'arrêt d'un service suivant des contraintes ;
- l'attribut **method** permet de définir la façon de gérer le service : initd, upstart ou service (par défaut) ;
- l'attribut **hidden** (booléen) indique si le service doit être activé ou non, cet attribut est particulièrement utile lors de la redéfinition d'un service, en particulier pour forcer sa désactivation ;
- si l'attribut **pty** vaut *False*, le pseudo-terminal ne sera pas utilisé (nécessaire pour certains services) ;
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir un service déjà défini dans un autre dictionnaire ;

La balise service peut également être utilisée pour activer/désactiver des configurations de site web apache2 (commandes : [a2ensite]/[a2dissite]).

Comme pour les services système, l'activation d'un site peut être conditionnée par une `servicelist`.

On peut ainsi gérer le lien symbolique suivant : **/etc/apache2/sites-enabled/monsite** avec :

```
<service method='apache' servicelist='siteperso'>monsite</service>
```

Le fichier de configuration **monsite** étant stocké dans **/etc/apache2/sites-available/**.

Attention

Pour spécifier plusieurs services, il faut obligatoirement écrire une balise **<service>** par service.

Exemple

Fichiers templates, paquets et services locaux ou dans un conteneur

```
<containers>
  <container name="mon_reverseproxy" id='101'>
    <package>nginx</package>
    <service servicelist="myrevprox" startlevel='91'>nginx</service>
     <file  filelist='myrevprox'  name='/etc/nginx/sites-enabled/default'
source='nginx.default'/>
     <file  filelist='myrevprox'  name='/var/www/nginx-default/nginx.html'
rm='True'/>
  </container>
</containers>
<files>
  <service>ntp</service>
  <file name='/etc/ntp.conf/>
  <file name='/etc/default/ntpdate' owner='ntp' group='ntp' mode='600'/>
  <file name='/etc/strange/host' source='strangehost.conf' mkdir='True'/>
</files>
```

2.3.3. Familles, variables et séparateurs

Variables : <variables>

L'ensemble des familles et, ainsi, des variables sont définies dans un nœud **<variables></variables>**.

Familles : <family>

Un conteneur famille permet d'avoir des catégories de variables. Celle-ci correspond à un onglet dans l'interface. Les familles sont incluses obligatoirement dans une balise *<variables>*.

Exemple

Une famile *Squid* pour gérer toutes les variables relatives a *Squid*.

Les attributs de family :

- l'attribut **name** (obligatoire) est à la fois le nom et l'identifiant de la famille ;
- l'attribut **mode** permet de définir une le mode de la famille (mode normal ou expert) ;

- l'attribut **hidden** indique si la famille doit être affichée ou non, sa valeur pouvant être modifiée via une condition (voir plus bas).

Variable : <variable>

Une variable contient une description et, optionnellement, une valeur EOLE par défaut.

Les variables peuvent être à valeur unique ou multi-valuées.

Les balises **<variables>** sont incluses obligatoirement dans une balise **<family>**.

Les attributs de la balise <variable>

- l'attribut **name** (obligatoire) est le nom de la variable ;
- l'attribut **type** (obligatoire) permet de construire un type EOLE avec des vérifications automatiques (fonctions de vérifications associées a chaque type de variable) ;
- l'attribut **description** permet de définir le libellé à afficher dans les interfaces de saisie ;
- l'attribut **multi** permet de spécifier qu'une variable pourra avoir plusieurs valeurs (par exemple pour un DNS, on aura plusieurs adresses IP de serveurs DNS) ;
- l'attribut **hidden** indique si la variable doit être affichée ou non (on peut par exemple souhaiter masquer des variables dont la valeur est calculée automatiquement) ;
- l'attribut **mode** permet de définir le mode de la variable (*normal* ou *expert*) ;
- si l'attribut **mandatory** vaut *True*, la variable sera considérée comme obligatoire, cet attribut remplace l'ajout d'un *check obligatoire* au niveau des conditions :
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir une variable déjà définie dans un autre dictionnaire ;
- si l'attribut **remove_check** vaut *True* pour une variable redéfinie, alors toutes les conditions associées à cette variable sont réinitialisées ;
- si l'attribut **exists** vaut *False*, cela permet de définir une variable si et seulement si elle n'a pas déjà été définie dans un autre dictionnaire.

Comportement avec redefine='True' et remove_check='False'

- si la nouvelle variable fournit une valeur par défaut, elle remplace l'ancienne ;
- si la nouvelle variable fournit une description, elle remplace l'ancienne ;
- l'attribut *hidden* est systématiquement écrasé ;
- l'attribut *multi* n'est pas modifiable ;
- si un nouveau *valid_enum* est défini dans les fonctions *checks*, il remplace l'ancien ;
- si de nouveaux *hidden_if(_not)_in* sont définis, ils remplacent les anciens ;
- les autres conditions et contraintes sont ajoutées à celles qui étaient déjà définies.

Valeur : <value>

A l'intérieur d'une balise **<variable>**, il est possible de définir une balise **<value>** permettant de spécifier la valeur par défaut de la variable.

Séparateurs : <separators> et <separator>

Les séparateurs permettent de définir des barres de séparation au sein d'une famille de variable dans l'interface de configuration.

Les séparateurs définis dans un dictionnaire sont placés dans la balise **<separators></separators>** dans la balise **<variables>**.

A l'intérieur de la balise **<separators>** il faut spécifier autant de balises **<separator>** que de séparateurs souhaités.

Attributs de la balise <separator>

- l'attribut **name** (obligatoire) correspond au nom de la variable suivant le séparateur ;
- si l'attribut **never_hidden** vaut *True*, le séparateur sera affiché même si la variable associée est cachée.

Exemple

Variables, familles et séparateurs

```
<variables>
  <family name='general'>
    <variable name='numero_etab' type='string' description="Identifiant de l'établissement (exemple UAI)" />
    <variable name='libelle_etab' type='string' description="Nom de l'établissement" />
    <variable name='activer_log_distant' type='oui/non' description="Gestion des logs centralisés" >
      <value>non</value>
    </variable>
    <variable name='adresse_ip_dns' type='ip' description='Adresse IP du serveur DNS' multi='True' />
  </family>
  <separators>
    <separator name='numero_etab' never_hidden='True'>Etablissement</separator>
  </separators>
</variables>
```

2.3.4. Contraintes

Des fonctions (contraintes) peuvent être utilisée pour grouper/tester/remplir/conditionner des variables.

L'ensemble des contraintes d'un dictionnaire se place à l'intérieur d'un nœud XML **<constraints></constraints>**.

Lien entre variables : <group>

Il est possible de lier des variables sous la forme d'une relation maître-esclave(s).

La variable maître doit obligatoirement être multi-valuée (`multi='True'`).

Elle se définit dans l'attribut **master**.

Les variables esclaves sont définies entre les balises **<slave>**.

Les variables esclaves deviennent automatiquement multi-valuées.

Exemple

```
<group master='adresse_ip_eth0'>
  <slave>adresse_netmask_eth0</slave>
  <slave>adresse_network_eth0</slave>
</group>
```

Calcul automatique <fill>

Renseigne automatiquement (par le calcul) une valeur par défaut à une variable.

Remarque

Les fonctions utilisées doivent être définies dans le fichier eosfunc.py ou ajoutées dans les fonctions personnalisées (voir ci-dessous).

Exemple

Ici on calcule **network_eth0** à partir de **ip_eth0** et de **netmask_eth0** en utilisant la fonction **calc_network**.

```
<fill name='calc_network' target='network_eth0'>
  <param type='eole' name='ip'>ip_eth0</param>
  <param type='eole' name='mask'>netmask_eth0</param>
</fill>
```

Attention

Contrairement aux variables "auto", le calcul des valeurs n'est réalisé que la première fois.

Une fois les valeurs enregistrées, elles ne sont plus modifiées.

Dans certains cas (exemple : changement de d'adresse IP), il est nécessaire d'aller modifier plusieurs valeurs "à la main".

Calcul automatique non modifiable : <auto>

Renseigne automatiquement (par le calcul) la valeur d'une variable.

Cette valeur ne peut pas être modifiée par l'utilisateur à la différence des fonctions de calcul automatique (peut être utile pour calculer l'IP d'un serveur en DHCP).

Remarque

Les fonctions utilisées doivent être définies dans le fichier eosfunc.py ou ajoutées dans les fonctions personnalisées (voir ci-dessous).

Exemple

```
<auto name='auto_eth' target='adresse_ip_eth0'>
  <param>eth0</param>
  <param name='condition'>dhcp</param>
  <param type='eole' name='parametre'>eth0_method</param>
</auto>
```

Validation et/ou liste de choix : <check>

La valeur renseignée pour une variable est validée par une fonction.

Les principales fonctions utilisées sont :

- `valid_enum` : la valeur doit être choisie dans la liste proposée ;
- `valid_entier` : la valeur est un nombre entier ;
- `valid_regexp` : la valeur doit être conforme à une expression régulière ;
- `valid_differ` : la valeur doit être différente d'une valeur donnée ;
- `obligatoire` : la valeur ne peut pas être vide *(ce test progressivement abandonné au profit de l'attribut de variable : mandatory)* ;

Validation d'un nombre entier

```
<check name='valid_entier' target='nombre'>
  <param name='min'>0</param>
  <param name='max'>50</param>
</check>
```

La valeur doit être un entier compris entre 0 et 50.

Liste de choix ouverte

```
<check name="valid_enum" target="lettre">
    <param>['a','b','c']</param>
    <param name="checkval">False</param>
</check>
```

Les choix proposés à l'utilisateur sont `a`, `b` ou `c` mais la ligne `<param name="checkval">False</param>` va l'autoriser à renseigner la valeur de son choix (ex : si il renseigne la valeur `d`, cela ne provoquera pas d'erreur).

Contrainte entre variables : <condition>

Les conditions permettent cacher, activer un template et/ou activer un service suite à un ensemble de conditions définies dans une fonction.

Exemple

```
<condition name='hidden_if_not_in' source='port_rpc'>
  <param>0</param>
  <param>7080</param>
  <target>ip_eth0</target>
  <target type='family'>net</target>
  <target type='file'>squid.conf</target>
  <target type='filelist'>ldap</target>
  <target type='servicelist'>ldap</target>
</condition>
```

Truc & astuce

Il n'est pas possible de tester plusieurs variables dans une condition.

Ceci peut être contourné en ajoutant une variable automatique intermédiaire sur laquelle on applique la fonction *calc_multi_condition*.

Description des fonctions

Les contraintes fill, auto, check et condition permettent d'appeler une ou des fonction(s) de la librairie eosfunc.py.

Elles sont construites de la manière suivante :

- l'attribut **name** de la contraintes correspond au nom de la fonction (dans eosfunc.py) ;
- l'attribut **target** correspond à la variable concernée par la contrainte ;
- l'attribut **param** correspond aux paramètres passés à la fonction.

Attributs de la balise <param>

Si elle n'a pas d'attribut **name**, il s'agit d'un paramètre positionnel ;

Si elle possède un attribut **name**, il s'agit d'un paramètre nommé.

Si il y a un attribut **type** :

- **eole** : le paramètre est la valeur d'une variable du dictionnaire.

  Si il y a un attribut **optional**='True' : ce paramètre est ignoré si la variable n'existe pas ;
- **container** : le paramètre est le dictionnaire décrivant le conteneur indiqué ;
- **python** : le paramètre est le retour du code python indiqué ;
- l'attribut **optional**='True' : indique que le paramètre sera ignoré si une exception se produit à l'évaluation ;
- l'attribut **hidden**='False' : indique que le paramètre sera ignoré si la variable cible est cachée.

Remarque

L'usage de l'attribut **optional** est réservé aux fonctions de type **condition**

Si une variable référencée par un paramètre n'existe pas et que **optional**='True' n'est pas positionné, Creole renvoie une erreur au chargement du dictionnaire.

Dans le cas d'un paramètre de type **python**, il est possible d'accéder aux fonctions du module eosfunc de Creole (`eosfunc`.<nom_fontion>).

Il faut également penser que lors de la saisie de configuration sur Zéphir, ce code sera exécuté sur le serveur Zéphir.

Ajout de fonctions personnalisées

Il est possible d'ajouter des librairies de fonctions personnalisées dans le répertoire **/usr/share/creole/funcs**.

Les librairies doivent posséder l'extension `.py` et contenir des fonctions python.

Exemple

```
def to_iso(data):
""" encode une chaine en ISO"""
try:
    return unicode(data, "UTF-8").encode("ISO-8859-1")
except:
    return data
```

Attention

Si vous devez importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.

```
def wpkg_user_pass (user):
try:
    from creole import parsedico
    dico = parsedico.parse_dico()
except:
    print "Erreur lors du chargement du dictionnaire"
    sys.exit()
return user+dico['numero_etab']
```

2.3.5. Aide

Il est possible d'afficher de l'aide dans l'interface (affichée au survol du libellé de la variable).

L'ensemble des aides d'un dictionnaire est dans la balise **<help>**.

Exemple

```
<help>
  <variable name='adresse_ip_eth0'>Adresse IP de la premiere carte réseau
(ex: 10.21.5.1)</variable>
</help>
```

2.4. Le langage de template Creole

Les variables du dictionnaire Creole sont accessibles en les préfixant par la chaîne de caractères : `%%`.

Si dans le dictionnaire Creole :

`adresse_ip_eth0` vaut `192.168.170.1`

Et qu'on a dans un template source le contenu suivant :

```
bla bla bla %%adresse_ip_eth0 bla bla bla
```

Après instanciation, le fichier cible contiendra :

```
bla bla bla 192.168.170.1 bla bla bla
```

Truc & astuce

Dans les cas où une variable est susceptible d'être confondue avec le texte qui l'entoure, il est possible d'encadrer son nom par des accolades :

`%%{adresse_ip_eth0}` est identique à `%%adresse_ip_eth0`.

2.4.1. Déclarations du langage Creole

Creole fournit un langage de template complet.

Il est possible de créer des boucles, des tests, de gérer les lignes optionnelles, de réaliser des inclusions répétées, ...

La déclaration de test : if

Syntaxe :

```
%if EXPRESSION |code_if %else |code_else %end if
```

Dans les tests il est possible d'utiliser les opérateurs du langage python : `==`, `!=`, `>`, `<`, `>=`, `<=`, `not`, `and`, `or`, ...

Exemple

```
%if %%size > 500
c'est grand
%elif %%size >= 250
c'est moyen
%else
c'est petit
%end if
```

Exemple

```
%if %%toto == 'yes' and ( %%titi != "" or %%tata not in ['a','b','c'] ) :
la condition a été validée
%end if
```

La déclaration d'itération : for

Syntaxe :

```
%for %%iterateur in EXPRESSION
CODE avec %%iterateur
%end for
```

La boucle `%%for` est particulièrement intéressante lorsque l'on souhaite effectuer des traitements sur une **variable multi-valuée**.

Exemple

```
%for %%i in range(4)
itération %%i
%end for
%for %%valeur in %%variable_multivaluee
%%valeur
%end for
```

Truc & astuce

Pour des traitements simples, la fonction prédéfinie `%%custom_join` (voir section suivante) peut avantageusement éviter la mise en place d'une boucle `%for`.

La notation pointée

Si une variable Creole est **multivaluée** et **maître** *(master d'un groupe de variable)* alors, il est possible de faire appel à ses variables **esclaves** à l'intérieur de la boucle `%for`.

Si `network` et `netmask` sont esclaves de `ip_adresse` alors, il est possible d'appeler ces variables en notation pointée.

Par exemple : dans le dictionnaire Creole figurent les variables suivantes.

`ip_adresse` est lla variable maître (les deux autres en dépendent), et :

- `ip_adresse = ['0.0.0.0', '1.1.1.1', '2.2.2.2']`
- `network = ['0.0.0.0'0, '1.1.1.1', '2.2.2.2']`
- `netmask = ['0.0.0.0', '1.1.1.1', '2.2.2.2']`

Le template suivant :

```
%for %%ip in %%ip_adresse_eth0
%%ip, %%ip.network, %%ip.netmask
%end for
```

donnera comme résultat :

```
0.0.0.0, 0.0.0, 0.0
1.1.1.1, 1.1.1, 1.1
2.2.2.2, 2.2.2, 2.2
```

Il est également possible aussi d'accéder à l'index (la position dans la liste) de la variable en cours de boucle :

```
%for %%ip in %%ip_adresse_eth0
l'index de : %%ip est : %%ip.index
%end for
```

Le template généré sera le suivant :

```
l'index de : 0.0.0. est : 0
l'index de : 1.1.1.1 est : 1
l'index de : 2.2.2.2 est : 2
```

Il est également possible (mais déconseillé) d'utiliser une "notation par item" (notation entre crochets).

Par exemple pour accéder à l'item numéro 5 d'une variable, il faut écrire :

```
variable[5]
```

La variable doit être évidemment être **multivaluée** et comporter au minimum *(item+1)* valeurs.

```
ip_adresse_eth0 = ['1.1.1.1', '2.2.2.2', '3.3.3.3']
```

et si un template a la forme suivante :

```
bla bla
%%ip_adresse_eth0[2]
bla bla
```

alors l'instanciation du template donnera comme résultat :

```
bla bla
3.3.3.3
bla bla
```

L'attribut implicite value

La notation pointée empêche l'accès direct aux méthodes et aux attributs des variables.

Par exemple, pour avoir accès à la méthode `startswith()` de la valeur d'une variable, il faut passer pour son attribut `value` :

```
%%variable_essai.value.startswith('/')
```

Les déclarations spéciales echo et set

L'instruction `%echo` permet de déclarer une chaîne de caractères afin que celle-ci apparaisse telle quelle dans le fichier cible.

Cela est utile lorsqu'il y a des caractères spéciaux dans le template source et, en particulier, les caractères `%` et `\` qui sont susceptibles d'être interprétés par le système de template.

Exemple

```
%echo "- deux barres obliques : \\\\\n- un pourcentage : %"
```

L'utilisation de l'instruction `%echo` ne rend pas les templates très lisibles d'autant plus que, généralement, on souhaite intercaler des variables au milieu des caractères spéciaux.

En pratique, il est donc préférable de passer par des variables locales que l'on peut déclarer avec `%set`.

Exemple

```
%set %%slash='\\'
%set %%double_slash='\\\\'
%%double_slash%%machine%%{slash}partage
```

Autres déclarations

La déclaration while

Syntaxe : `%while EXPR contenu`

`%end while`

Exemple :

```
%while %someCondition('arg1', %%arg2)
The condition is true.
%end while
```

La déclaration repeat

Syntaxe : `%repeat EXPR`

`%end repeat`

La déclaration unless

`%unless EXPR`

`%end unless`

peut être utile si une variable est dans le dictionnaire Creole pour "'ne pas'" executer une action :

```
%unless %%alive
do this
%end unless
```

La syntaxe d'inclusion

il est possible d'inclure des fichiers à l'aide de la déclaration suivante :

```
%include "includeFileName.txt"
```

ou bien à partir du nom long du fichier à inclure (le nom de fichier étant ici renseigné dans une variable Creole :

```
%include source=%%myParseText
```

Effacement des retours chariots : slurp

Exemple d'utilisation :

```
%for %%i in range(15)
%%i - %slurp
%end for
```

donnera :

```
1-2-3-4-5-6...
```

sur une seule ligne (gobe les retours chariots)

remarquons que dans ce cas là, `slurp` n'est pas nécessaire et il est possible d'écrire le end sans sauter de ligne :

```
%for %%i in range(15)
%%i -%end for
```

exemple 2 :

```
%if %%dns_nameservers != <nowiki>['']</nowiki>
dns_nameservers %slurp
%for %%name_server in %%dns_nameservers %%name_server %slurp
%end for
%end if
#
```

générera :

```
dns_nameserver toto titi #
```

2.4.2. Fonctions prédéfinies

Il est possible d'accéder à des fonctions prédéfinies, provenant du module : **eosfunc.py**.

Ces fonctions peuvent être utilisées dans un template de la manière suivante (exemple) :

[...] `%%fonction_predefinie(%%variable)` [...]

Variable "optionnelle" : is_defined

Il peut arriver qu'on ne soit pas sûr que la variable que l'on souhaite tester soit définie dans les dictionnaires présents sur le module.

C'est le cas lorsque l'on veut traiter un cas particulier dans un template qui est commun à plusieurs modules.

Hors, si une variable est utilisée dans le template cible sans avoir été définie, le processus d'instanciation sera stoppé.

Pour tester si une variable est définie, il faut utiliser la fonction `%%is_defined`.

Exemple

```
%if %%is_defined('ma_variable')
%%ma_variable
%else
la variable n'est pas définie
%end if
```

Attention

Contrairement à toutes les autres fonctions, `is_defined` nécessite comme argument le nom de la variable fourni sous forme d'une **chaîne de caractères**.

Remarque

Si une variable non définie est placée dans un bloc qui n'est pas traité (conditionné par une fonction ou d'autres variables), ça n'est pas bloquant.

Variable "vide" : is_empty

Il n'est pas toujours évident, en particulier lorsque l'on manipule des variables multi-valuées, de trouver le test adéquat afin de déterminer si une variable est vide.

En effet, selon la manière dont la variable a été éditée, elle est susceptible d'apparaître soit comme une liste vide (`[]`), soit comme une liste contenant une chaîne vide (`['']`).

Pour tester si une variable est vide, il est désormais recommandé d'utiliser la fonction `%%is_empty`.

Exemple

```
%if not %%is_empty(%%ma_variable)
%%ma_variable[0]
%else
la variable est vide
%end if
```

Concaténation des éléments d'une liste : custom_join

La fonction `%%custom_join` permet de concaténer facilement les éléments d'une variable multi-valuée.

Cela permet d'éviter le recours à une boucle `%for` et l'utilisation du l'instruction `%slurp` qui est souvent source d'erreurs.

Il est possible de spécifier le séparateur à utiliser en le passant comme paramètre à la fonction.

En l'absence de ce paramètre, le séparateur utilisé est l'espace.

Exemple

```
%%custom_join(%%ma_variable, ':')
```

Si ma_variable vaut ['a', 'b', 'c'], cela donnera :

```
a:b:c
```

Variable "dynamique" : getVar

Une variable dynamique prend comme nom (ou partie du nom) la valeur d'une autre variable.

Exemple

```
%for %%interface in range(0, %%int(%%nombre_interfaces))
L'interface eth%%interface a pour adresse %%getVar('adresse_ip_eth'+str(%
%interface))
%end for
```

Variable esclave "dynamique" : getattr

Lorsque le nom de la variable esclave doit être calculé, on peut utiliser `%%getattr` à la place de la notation pointée.

Exemple

```
%set %%num='0'
%for %%ip_ssh in %%getVar('ip_ssh_eth'+%%num)
SSH est autorisé pour %%ip_ssh/%%getattr(%%ip_ssh, 'netmask_ssh_eth'+%
%num)
%end for
```

Autres fonctions

Fonctions de traitement des chaînes de caractères

- transformation d'une chaîne en majuscules : `%%upper(%%ma_chaine)` ;
- transformation d'une chaîne en minuscules : `%%lower(%%ma_chaine)` ;
- encodage d'une chaîne en ISO-8859-1 (au lieu d'UTF-8) : `%%to_iso(%%ma_chaine)` ;
- transformation d'un masque réseau (ex : *255.255.255.0*) en classe d'adresse (ex : *24*) : `%%calc_classe(%%mask)` ;

Fonctions de tests

- vérification que la variable est une adresse IP (et pas un nom DNS) : `%%is_ip(%%variable)` ;
- vérification de l'existence d'un fichier : `%%is_file(%%fichier)`.

Déclaration de fonctions locales

Pour un traitement local et répétitif, il peut être pratique de déclarer une fonction directement dans un template avec `%def` et `%end def`.

Cependant, la syntaxe à utiliser dans ces fonctions est assez complexe (on ne sait jamais quand mettre le caractère `%` !) et ce genre de déclaration ne facilite pas la lisibilité du template.

Les fonctions déclarées localement s'utilisent de la même façon que les fonctions déjà prédéfinies.

Exemple

```
%def nombre_points(chaine)
%return chaine.count('.')
%end def
Il y a %%nombre_points(%%ma_variable) points dans ma variable.
```

Ajout de fonctions personnalisées

Il est possible d'ajouter des librairies de fonctions personnalisées dans le répertoire **/usr/share/creole/funcs**.

Les librairies doivent posséder l'extension `.py` et contenir des fonctions python.

Exemple

```
def to_iso(data):
""" encode une chaine en ISO"""
try:
    return unicode(data, "UTF-8").encode("ISO-8859-1")
except:
    return data
```

Attention

Si vous devez importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.

```
def wpkg_user_pass (user):
try:
    from creole import parsedico
    dico = parsedico.parse_dico()
except:
    print "Erreur lors du chargement du dictionnaire"
    sys.exit()
return user+dico['numero_etab']
```

2.4.3. Utilisation avancée

Modification des méta-caractères utilisés

Dans le cas où il y a trop de % dans le template, il est possible de changer carrément de méta-caractères, en ajoutant une section `compiler-settings` en en-tête du template.

Cette méthode est, par exemple, utilisée pour la génération du fichier de configuration du logiciel `eJabberd` qui est en déclaré en Erlang*.

Utilisation de @ et @@ à la place de % et %%

```
%compiler-settings
directiveStartToken = @
cheetahVarStartToken = @@
%end compiler-settings
```

Jouer avec le contexte

Il est possible de lister et donc d'utiliser la liste des variables du dictionnaire.

Pour lister toutes les variables et leurs valeurs :

```
%for %%var in %%self.context
%if %%self.context[%%var] != ""
%%var est égal à %%self.context[%%var]
%end if
%end for
```

Ce qui renvoie:

```
ldap_loglevel is 0
xinet_interbase is oui
active_bacula_sd is oui
adresse_netware is 22
numero_etab is 0140096D
sso is non
sso_session_timeout is 7200
cups_loglevel is info
activer_log_distant is non
[...]
```

Si vous souhaitez ne travailler que sur certaines variables, vous pouvez définir une variable multiple dans votre dictionnaire (ex: liste_variables_eole) et l'utiliser par exemple comme suit:

```
%for %%var in %%liste_variables_eole
%if type(%%self.context[%%var.value]) != list and type(%%self.context[%
%var.value]) != dict
Scalaire %%var.value est égal à %%self.context[%%var.value]
%elif type(%%self.context[%%var.value]) == list and len(%%self.context[%
%var.value]) >= 1
Liste %%var.value est égal à %slurp
%for %%i in range(len(%%self.context[%%var.value])-1)
%%self.context[%%var.value][%%i],%slurp
%end for
%%self.context[%%var.value][len(%%self.context[%%var.value])-1]
%end if
%end for
```

Ce qui renvoie, par exemple, avec `liste_variables_eole = ['ldap_loglevel', 'adresse_ip_dns']`:

```
Scalaire ldap_loglevel est égal à 0
Liste adresse_ip_dns est étal à 192.168.55.119,192.168.55.200
```

2.4.4. Exemple

Nous voulons templatiser le fichier toto.conf à l'aide des mécanismes Creole afin de rajouter l'adresse_ip_eth0 (variable existante) ainsi que l'adresse de l'établissement (nouvelle variable).

Ajouter un dictionnaire local

Dans **/usr/share/eole/creole/dicos/local/**

ajouter un fichier .xml

```
<?xml version='1.0' encoding='utf-8'?>
<creole>
<files>
<file name='/etc/toto.conf' />
</files>
<variables>
<family name="Perso">
<variable name='nom_proviseur' type='string' description="Nom du proviseur" />
</family>
</variables>
<constraints>
<check name='obligatoire' target='nom_proviseur' />
```

```
</constraints>

<help>

<variable name="nom_proviseur">Nom du proviseur dans la page d'accueil du portail</variable>

</help>

</creole>
```

Ajouter votre fichier template

Notre fichier toto.conf sera placé dans **/usr/share/eole/creole/distrib/**

Il faut ajouter les variables à l'aide de la syntaxe Creole.

exemple : l'adresse est %%adresse_ip_eth0 et l'adresse est %%adresse_etablissement

adresse_ip = %%adresse_ip_eth0

Le nom du proviseur = %%nom_proviseur

Entrer l'adresse de l'établissement

- Taper [gen_config /etc/eole/config.eol]
- Dans l'onglet *Perso* ajouter l'adresse de l'établissement
- Enregistrer

Reconfigurer

Le mécanisme de configuration a écrit votre fichier **/etc/toto.conf** avec les variables.

Les variantes Zéphir

Cette procédure décrit comment ajouter des spécifications locales.

Dans le cadre d'un développement massif, le module Zéphir propose un mécanisme de variantes semblable.

Instancier un template avec CreoleCat

> "cf Instancier un template avec CreoleCat", page 245.

2.5. CreoleLint et CreoleCat

`CreoleLint` et `CreoleCat` sont des utilitaires permettant de faciliter les tests sur les dictionnaires et les templates.

2.5.1. Vérifier les dictionnaires et templates avec CreoleLint

`CreoleLint` est une application très pratique pour valider la syntaxe du dictionnaire et des templates.

L'outil effectue une série de tests dans le but de détecter les erreurs les plus fréquentes.

Utilisation de CreoleLint

Sur un module installé, il est possible de lancer l'application sans option particulière :

```
CreoleLint
```

Il est possible de ne faire apparaître que les messages à partir d'un niveau déterminé avec l'option "-l".

Les trois niveaux sont :

- info ;
- warning ;
- error.

Pour tester les dictionnaires et templates sur une copie du dépôt, il faut renseigner les options suivantes :

- -d : répertoire des dictionnaires ;
- -t : répertoire des templates ;
- -x : répertoire contenant la DTD (**creole.dtd**).

Le fichier creolelint.conf

Pour éviter d'afficher des avertissements pour des faux positifs, il est possible de créer un fichier "creolelint.conf".

Ce fichier peut être spécifié dans la ligne de commande :

```
CreoleLint -c creolelint.conf
```

Sinon l'application vérifiera si un fichier creolelint.conf existe dans le répertoire parent des templates et dictionnaires.

Attention

Ce fichier est un fichier de configuration reprenant la syntaxe python. Si le fichier de configuration est invalide, l'application ne pourra pas se lancer correctement.

Ce fichier contient obligatoirement le nom du paquet :

```
name='conf-amon'
```

Puis contient les éventuelles dépendances du paquet sous forme de liste :

```
dependencies=['eole-common']
```

Enfin, le fichier contient un liste de liste permettant de ne pas faire afficher certains avertissements. Pour cela, il faut renseigner la variable "skip".

La syntaxe est la suivante :

```
['nom_du_test', 'nom_de_la_variable', 'nom_du_template', ligne_du_template]
```

Pour les variables de dictionnaire, la synxtaxe est la suivante :

```
['nom_du_test', 'nom_de_la_variable', '', '']
```

Exemple

```
skip = [
['orphans_in_tmpl', 'interface_dhcp', 'dhcp3-relay', 7],
['orphans_in_dicos', 'nom_machine_eth1', '', '']
]
```

Attention

Cette variable skip ne fonctionne que pour les tests suivants :

- orphans_in_dicos ;
- orphans_in_tmpl ;
- syntax_var (seulement pour les variables définies dans un template).

Sauver les variables d'un dictionnaire

Pour utiliser le mécanisme de dépendances de creolelint.conf, il faut enregistrer les variables du dictionnaire dans un fichier spécial. Pour cela, il faut utiliser l'option '-s' de creolelint :

```
CreoleLint -d ../eole-sso/dicos/ -t ../eole-sso/tmpl/ -s
```

2.5.2. Instancier un template avec CreoleCat

`CreoleCat` permet d'instancier un seul template indépendamment des commandes `instance` et `reconfigure`.

Le script nécessite au minimum un template source et un fichier de destination (option `-o`) :

```
CreoleCat source.conf -o resultat.conf
```

En plus, il est possible de spécifier :

- un fichier de valeur (`.eol`) alternatif avec l'option `-i`
- un répertoire de dictionnaire ou un dictionnaire particulier (`.xml`) avec l'option `-x`

2.6. Ajout de scripts à l'instance ou au reconfigure

Il est parfois nécessaire d'ajouter un script à l'instanciation du module ou au reconfigure.

EOLE met en place des mécanismes permettant d'exécuter des scripts avant ou après l'instanciation ou la reconfiguration.

Ces scripts doivent être dans l'un des répertoires suivants :

/usr/share/eole/pretemplate : exécution avant la templatisation des fichiers

/usr/share/eole/postemplate : exécution entre la templatisation des fichiers et le redémarrage des services

/usr/share/eole/postservice : exécution après le redémarrage des services

Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.

Le type d'appel (instance ou reconfigure) est envoyé au script sous la forme d'un argument :

```
#!/bin/bash
if [ "$1" == "instance" ]; then
    echo "ce code n'est exécuté qu'à l'instance"
elif [ "$1" = "reconfigure" ] ;then
    echo "ce code n'est exécuté qu'au reconfigure"
fi
```

Attention

Si le script quitte avec un autre code de retour que "0", l'instance ou le reconfigure s'arrêtera immédiatement.

Il est donc préférable que le script soit de la forme :

```
#!/bin/bash
# <<< SCRIPT >>>
exit 0
```

> "cf Indications pour la programmation", page 247.

2.7. Ajouter un test diagnose

Les scripts diagnose personnalisé peuvent être placé dans le répertoire **/usr/share/eole/diagnose/module**.

Ces fichiers sont généralement écrits en bash et permettent de se connecter au service voulu pour tester l'état de celui-ci.

Un certain nombre de fonctions sont proposées de base par EOLE, mais vous pouvez créer vos propres fonctions pour vos besoins spécifiques.

Généralement, le test met "Ok" si le service est fonctionnel et "Erreur" en cas de problème.

Voici quelques fonctions proposées par EOLE :

- TestIP et TestIP2 : test si une IP répond au ping ;
- TestARP : test si un adresse MAC répond ;
- TestService : test TCP sur un numéro de port ;
- TestPid : test si l'application à un PID ;
- TestDns : test une requête DNS ;
- TestNTP : test le serveur NTP ;

- TestHTTPPage : test le téléchargement d'une page http ;
- TestCerts : test des valeurs du certificat TLS/SSL.

Exemple

```
#!/bin/bash
# utilisation de fonction EOLE
. /usr/share/eole/FonctionsEoleNg
# utilisation de variables du dictionnaire
. /usr/bin/ParseDico
# test si le serveur web est fonctionnel en testant la variable Creole
"activer_web"
# et en utilisant la fonction eole TestHTTPPage
[ "$activer_web" = "oui" ] && TestHTTPPage "Web" "http://localhost/"
```

> "cf Indications pour la programmation", page 247.

2.8. Indications pour la programmation

Certaines fonctions ont été intégrées sur les modules afin que les scripts puissent être écrits en tenant compte des spécificités des modules EOLE, que sont les variables et le mode conteneur.

Programmation bash

- exporter variables EOLE dans l'environnement :

  ```
  . /usr/bin/ParseDico
  ```

- exporter les informations concernant les conteneurs dans l'environnement :

  ```
  . /etc/eole/containers.conf
  ```

- exécution d'une commande dans un conteneur :

  ```
  . /usr/share/eole/FonctionsEoleNg
  RunCmd "<commande>" <conteneur>
  ```

- redémarrage d'un service dans un conteneur :

  ```
  . /usr/share/eole/FonctionsEoleNg
  Service <nom_du_service> restart <conteneur>
  ```

Exemple

```
#!/bin/bash
. /usr/bin/ParseDico
echo "mon adresse IP est $adresse_ip_eth0"
. /etc/eole/containers.conf
echo "La base Ldap est stockée dans $container_path_annuaire/var/lib/ldap"
echo "Le conteneur annuaire a l'adresse : $container_ip_annuaire"
. /usr/share/eole/FonctionsEoleNg
RunCmd "ls /var/lib/ldap" annuaire
Service slapd restart annuaire
```

CreoleService

Le nouvel outil `CreoleService` vient remplacer avantageusement la fonction *Service()* de `FonctionsEoleNg`.

Exemple : `CreoleService -c fichier smbd restart`

Programmation Python

- utiliser les variables EOLE :

```
from creole import parsedico
parsedico.parse_dico()
```

- utiliser les informations concernant les conteneurs :

```
from creole.eosfunc import load_container_var
load_container_var()
```

- exécution d'une commande dans un conteneur (affichage à l'écran) :

```
from pyeole.process import system_code
system_code([<commande_sous_forme de liste>], container='<conteneur>')
```

- exécution d'une commande dans un conteneur (sorties dans un tuple) :

```
from pyeole.process import system_out
system_out([<commande_sous_forme de liste>], container='<conteneur>')
```

- redémarrage d'un service dans un conteneur (affichage à l'écran) :

```
from pyeole.service import service_code
```

```
service_code('<service>', 'restart', container='<conteneur>')
```

- redémarrage d'un service dans un conteneur (sorties dans un tuple) :

```
from pyeole.service import service_out
service_out('<service>', 'restart', container='<conteneur>')
```

Exemple

```
#!/usr/bin/env python
# -*- coding: UTF-8 -*-
from creole import parsedico
variables = parsedico.parse_dico()
print "mon adresse IP est %s" % variables['adresse_ip_eth0']
from creole.eosfunc import load_container_var
conteneurs = load_container_var()
print "La base Ldap est stockée dans %s/var/lib/ldap" %
conteneurs['container_path_annuaire']
print "Le conteneur annuaire a l'adresse : %s" %
conteneurs['container_ip_annuaire']
from pyeole.process import system_code
system_code(['ls', '/var/lib/ldap'], container='annuaire')
from pyeole.service import service_code
service_code('slapd', 'restart', container='annuaire')
```

2.9. Gestion des noyaux Linux

Noyaux EOLE

Les modules EOLE utilisent normalement des noyaux Ubuntu recompilés par l'équipe EOLE afin d'y ajouter certains patchs tels que ceux pour le support de *ipp2p* ou d'*ipset*.

Le fichier **/usr/share/eole/noyau/current** indique la version du noyau que le serveur devrait utiliser. Si le noyau utilisé est différent du noyau conseillé, la commande **reconfigure** vous proposera de redémarrer le serveur.

Les anciens noyaux, qui ne sont plus utilisés, sont purgés au début du **reconfigure**.

Personnalisation du noyau

Dans certains cas (problèmes matériels, tests,...), il peut être souhaitable d'utiliser un autre noyau que celui recommandé par EOLE.

Le fichier **/usr/share/eole/noyau/local** permet d'indiquer au système le noyau à utiliser.

Attention

Cette facilité est à utiliser à titre exceptionnel.

Aucun signalement lié à l'utilisation d'un noyau différent de celui préconisé par EOLE ne sera pris en compte.

2.10. Gestion des tâches planifiées eole-schedule

Présentation

Sur les modules EOLE 2.2 et antérieur, il était possible de configurer une sauvegarde en même temps que la mise à jour hebdomadaire.

Avec le système des fichiers lock, il n'était pas rare que l'une des deux opérations ne soit pas effectuée.

Désormais, `cron` n'est plus directement utilisé pour lancer les tâches planifiées.

C'est `eole-schedule` qui le remplace.

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est `cron` qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bacula* qui lance `eole-schedule`.

Il existe 4 types de "schedule" :

- les tâches journalières (daily) ;
- les tâches hebdomadaires (weekly) ;
- les tâches mensuelles (monthly) ;
- les tâches uniques (once).

Ces tâches sont découpées en "pre" sauvegarde et "post" sauvegarde.

Si aucune sauvegarde n'est prévue : le `cron` lance "pre" puis "post" à l'heure qui a été tiré au hasard.

Si une sauvegarde est prévue : Bacula lance "pre" avant la sauvegarde et "post" à l'heure qui a été tiré au hasard (sauf si celui-ci est prévu avant la sauvegarde ou si la sauvegarde n'est pas terminée, dans ce cas ils seront exécutés après la sauvegarde).

Remarque

Les sauvegardes "post" sont obligatoirement marquées en `Full` même si cela ne correspond à rien (pas de sauvegarde, exécution des scripts uniquement). Elles sont réalisées à l'heure qui a été tiré au hasard.

Par contre, les sauvegardes "pre" sont bien lancées à l'heure définie par l'administrateur.

Gestion des tâches planifiées

Lister ce qui est programmé

- [/usr/share/eole/schedule/manage_schedule pre]
- [/usr/share/eole/schedule/manage_schedule post]

Activer/désactiver un script

Exécution d'un script "pre" tous les jours :

[/usr/share/eole/schedule/manage_schedule pre <script> daily add]

Désactivation d'un script "post" programmé tous les mois :

[/usr/share/eole/schedule/manage_schedule post <script> monthy del]

Gestion des mises à jour avec Creole et eole-schedule

La mise à jour hebdomadaire consiste en un script `eole-schedule` nommé `majauto`. Il est configuré pour être lancé une fois par semaine (`weekly`) après la sauvegarde (`post`).

Sa gestion dans les scripts python est facilitée par la librairie `creole.maj`.

Savoir quand est prévue la mise à jour

[python -c "from creole import maj; print maj.get_maj_day()"]

Activer/désactiver la mise à jour hebdomadaire

Activation de la mise à jour hebdomadaire :

[/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()"]

Activer/désactiver la mise à jour hebdomadaire via l'EAD

Mise à jour

2.11. Gestion du pare-feu eole-firewall

Introduction

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur ;
- d'un conteneur vers le maître ;
- d'un conteneur vers un autre conteneur ;
- d'un conteneur vers l'extérieur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper* et l'activation de modules noyau.

Remarque

`eole-firewall` ne gère que des "autorisations".

Par défaut tous les flux sont bloqués sauf pour le maître qui peut accéder sans restriction à l'extérieur et aux conteneurs.

Si un conteneur possède une seconde interface (variable du type : *adresse_ip_link*), il n'y aura aucune règle sur cette interface.

eole-firewall et Era

Pour les modules sur lesquels Era est installé (Amon et AmonEcole), `eole-firewall` s'exécute en complément.

Dans ce cas, il gère uniquement les connexions entre les conteneurs, des conteneurs vers le maître et des conteneurs vers l'extérieur.

Tous les flux entre zones (notamment ceux de l'extérieur vers les conteneurs) sont alors gérés par Era.

Déclaration des règles

La description des autorisations se fait dans un ensemble de fichiers contenus dans le répertoire **/usr/share/eole/firewall**.

Ces fichiers possèdent l'extension `.fw`.

Le nom du fichier est important. Il déterminera l'une des extrémités de la règle.

Il faut qu'il soit obligatoirement de la forme :

00_nomduconteneur_commentaire.fw

Par contre, le commentaire n'est pas obligatoire.

Deux types d'autorisation sont possibles :

- `allow_src` : permet d'autoriser des adresses à accéder à un service du conteneur indiqué par le nom du fichier ;
- `allow_dest` : permet d'autoriser le conteneur indiqué par le nom du fichier à accéder à un service.

Le conteneur "root" indique en réalité le serveur maître.

Il est obligatoire de définir, au minimum, l'interface d'entrée des flux, l'adresse IP extérieure ou le nom du conteneur et le port.

Certains services nécessitent également la configuration de TCP Wrapper*.

Il faut alors ajouter le nom du démon à l'attribut `tcpwrapper` (facultatif pour les règles inter-conteneurs).

`eole-firewall` permet également d'activer des modules noyau.

Pour cela, il faut utiliser l'attribut `load_modules` auquel doit être affecté une liste au format *python*.

Par défaut, les règles sont en TCP.

Il est nécessaire d'ajouter l'attribut `protocol` dans les autres cas (UDP, ICMP).

Exemple

```
# Autoriser le ping du serveur (maître) : fichier 10_root.fw
allow_src(interface='eth0', ip="0/0", protocol='icmp', typ='echo-request')
# Autoriser l'accès en SSH au serveur (maître) pour l'adresse 1.1.1.50 : fichier 10_root.fw
allow_src(interface='eth0', ip='1.1.1.50', port='22', tcpwrapper="sshd")
# Autoriser l'adresse 1.1.1.51 à accéder au serveur SMTP du conteneur "mail" : fichier 10_mail.fw
allow_src(interface='eth0', ip='1.1.1.51', port='25')
# Autoriser le conteneur "web" à accéder au serveur EoleSSO du maître : fichier 10_web.fw
allow_dest(ip='<adresse_ip_eth0>', port='8443')
# Autoriser le conteneur "dns" à accéder au serveur DNS distant 1.1.1.53 : fichier 10_dns.fw
allow_dest(interface='eth0', ip='1.1.1.53', protocol='udp', port='53')
# Autoriser le conteneur "fichier" à accéder au serveur LDAP du conteneur "annuaire" 10_fichier.fw :
allow_dest(interface='eth0', container='annuaire', port='389', tcpwrapper='slapd')
```

Truc & astuce

Parfois, il n'est pas facile de savoir sur quelle interface une règle sera appliquée.

Dans ce cas, il est possible d'utiliser le paramètre suivant :

```
interface='auto'
```

L'interface à utiliser sera calculée automatiquement à partir des résultats de la commande : *ip route get*

XII Résolution de problèmes

Sur les modules EOLE quelques outils sont disponibles pour aider à la résolution de problèmes. L'outil de diagnostic `diagnose` et la lecture des logs permettent l'identification de la plupart des problèmes. L'outil de génération de rapport aidera à rassembler des informations en vue d'une analyse.

1 Diagnostic d'un module

La commande diagnose

Lors de la mise en œuvre d'un module, un outil de diagnostic permet de valider que la configuration est correcte et fonctionnelle.

la commande **diagnose** valide donc les points clés de la configuration des services.

L'état des services est indiqué clairement par un code couleur vert/rouge.

```
*** DEBUT DU DIAGNOSTIC ***

*** Test du module horus-2.2 (horus 0210056x) ***

RESEAU
Settings for eth0:
        Link detected: yes
Settings for eth1:
        Link detected: yes

*** Controle des interfaces
horus:        10.21.11.10 =>  Ok

*** Controle des services
# Services Locaux
.                   SSH =>  Ok
.             Annuaire =>  Ok
.              Partage =>  Ok
.            Impression =>  Ok
.                   SSO =>  Ok

# Outils d'administration
.                  EAD2 =>  Ok
.              EAD2 Web =>  Ok
.        Frontend Horus =>  Ok

# Services Distants
.        DNS 10.21.11.1 =>  Ok
.         Acces distant =>  Ok


L'annuaire ldap est initialisé

*** FIN DU DIAGNOSTIC ***
root@horus:~#
```

Les points importants de l'état du serveur sont vérifiés :

- la version du module installé ;
- la connectique réseau et sa configuration ;
- l'état des principaux services.

S'il apparait que certaines sections seraient en erreur, il faudrait revoir le fichier de configuration **/etc/eole/config.eol**, et reconfigurer le serveur.

Le diagnose, mode étendu

Si le diagnostic précédent n'est pas suffisant pour comprendre l'éventuelle erreur détectée, un mode étendu permet d'obtenir plus d'informations.

Pour cela, taper :

```
diagnose -L
```

```
*** DEBUT DU DIAGNOSTIC ***

Configuration du serveur

Type  : I-Select
Invalid entry length (0). DMI table is broken! Stop. - NEC
Invalid entry length (0). DMI table is broken! Stop.
Processeur :
  AMD Athlon(tm) 64 Processor 3200+
  CPU
Carte réseau :
    SK-9E21D 10/100/1000Base-T Adapter, Copper RJ-45
Disques  :
       CD-ROM LTN-489S
       73GB ATLAS10K5_73WLS

Sys. de fich.            Tail. Occ. Disp. %Occ. Monté sur
/dev/sda5              1,9G  162M  1,6G  10% /
varrun                 252M  884K  251M   1% /var/run
varlock                252M     0  252M   0% /var/lock
udev                   252M   64K  252M   1% /dev
devshm                 252M     0  252M   0% /dev/shm
/dev/sda1              373M   30M  324M   9% /boot
/dev/sda11              52G  221M   49G   1% /data
/dev/sda9              2,6G   69M  2,4G   3% /tmp
/dev/sda6              1,4G  685M  650M  52% /usr
/dev/sda7              3,9G  583M  3,1G  16% /var
/dev/sda8              3,9G   87M  3,6G   3% /var/log

 Appuyez sur Entrée pour continuer ...
```

Le premier écran détaille l'aspect matériel du serveur.

Le détail des disques reconnus, leur partitionnement, et le taux d'occupation des partitions est affiché.

```
 Appuyez sur Entrée pour continuer ...

Version de votre serveur : horus-2.2 - Linux 2.6.24-21-eole - conf-horus 2.2-eole15

Vérification des paquets installés    OK
 Appuyez sur Entrée pour continuer ...
```

Le nom du module, ainsi que les versions de la solution sont affichés à titre indicatif.

```
*** Mise à jour du module horus-2.2 (horus 0210056x) ***

Test du serveur de mise à jour

. test-eoleng.ac-dijon.fr =>  Ok
.         Mise à jour =>  Complète
.   Création du Cache =>  Ok
.   Nb de mise à jour =>  16

Liste des paquets à mettre à jour

base-files (4.0.1ubuntu5.8.04.3)        module-init-tools (3.3-pre11-4ubuntu5.8
conf-horus (2.2-eole16)                 mysql-client-5.0 (5.0.51a-3ubuntu5.3)
creole (2.2-eole25)                     mysql-common (5.0.51a-3ubuntu5.3)
eolebase (2.2-eole40)                   mysql-server-5.0 (5.0.51a-3ubuntu5.3)
libdbus-1-3 (1.1.20-1ubuntu3.2)         python-apt (0.7.4ubuntu7.3)
libmysqlclient15off (5.0.51a-3ubuntu5.3 rsyslog (3.21.7-1eole1)
linux-ubuntu-modules-2.6.24-21-eole (2. ssmtp (2.61-13ubuntu1.1)
logrotate (3.7.1-3ubuntu0.8.04)         zephir-client (2.2-eole21)
 Appuyez sur Entrée pour continuer ...
```

L'état des mises à jour est ensuite déterminé. Si comme ici, il en existe, il est conseillé de les installer pour vérifier si le problème rencontré n'est pas corrigé par l'une de celles-ci.

```
 Appuyez sur Entrée pour continuer ...


Etat des dernières actions Creole

Nov  5 14:04:25 horus zephir: MAJ => INIT : Debut
Nov  5 14:04:33 horus zephir: MAJ => FIN : Mise à jour OK
Nov  5 14:04:56 horus zephir: QUERY-MAJ => INIT : Debut
Nov  5 14:04:59 horus zephir: QUERY-MAJ => FIN : 1 paquets à mettre à jour
Nov  5 14:05:08 horus zephir: MAJ => INIT : Debut
Nov  5 14:05:11 horus zephir: MAJ => FIN : Mise à jour OK
Nov  5 14:05:15 horus zephir: RECONFIGURE => INIT : Début de reconfiguration
Nov  5 14:06:00 horus zephir: RECONFIGURE => FIN : Reconfiguration Terminée
Nov  5 14:06:32 horus zephir: QUERY-MAJ => INIT : Debut
Nov  5 14:06:35 horus zephir: QUERY-MAJ => FIN : Aucune Mise à jour à faire
Nov  5 14:40:43 horus zephir: QUERY-MAJ => INIT : Debut
Nov  5 14:40:50 horus zephir: QUERY-MAJ => FIN : Aucune Mise à jour à faire
Nov  5 15:17:59 horus zephir: RECONFIGURE => INIT : Début de reconfiguration
Nov  5 15:18:56 horus zephir: RECONFIGURE => FIN : Reconfiguration OK -> reboot
Nov  5 15:22:30 horus zephir: RECONFIGURE => INIT : Début de reconfiguration
Nov  5 15:23:42 horus zephir: RECONFIGURE => FIN : Reconfiguration Terminée
Nov 14 14:07:44 horus zephir: QUERY-MAJ => INIT : Debut
Nov 14 14:07:57 horus zephir: QUERY-MAJ => FIN : 16 paquets à mettre à jour
Nov 14 14:26:25 horus zephir: QUERY-MAJ => INIT : Debut
Nov 14 14:26:28 horus zephir: QUERY-MAJ => FIN : 16 paquets à mettre à jour
 Appuyez sur Entrée pour continuer ...
```

la liste des dernières actions réalisées sur le serveur est affichée (mise à jour, reconfigure, etc.).

```
*** Test du module horus-2.2 (horus 0210056x) ***

RESEAU
Settings for eth0:
        Link detected: yes
Settings for eth1:
        Link detected: yes

*** Controle des interfaces
horus:        10.21.11.10 =>  Ok

*** Controle des services
# Services Locaux
.                   SSH =>  Ok
.              Annuaire =>  Ok
.               Partage =>  Ok
.            Impression =>  Ok
.                   SSO =>  Ok

# Outils d'administration
.                  EAD2 =>  Ok
.              EAD2 Web =>  Ok
.        Frontend Horus =>  Ok

# Services Distants
.        DNS 10.21.11.1 =>  Ok
.         Acces distant =>  Ok


L'annuaire ldap est initialisé

*** FIN DU DIAGNOSTIC ***
root@horus:~#
```

Enfin, on retrouve l'affichage standard de l'outil.

2 Problèmes à la mise en œuvre

Erreur lors du partitionnement

L'outil de partitionnement affiche la question suivante : "partitionner le disques > Nom de volume déjà utilisé" :

Cela indique juste que des partitions LVM* (issues d'une installation antérieure) ont été détectées sur le disque dur.

Vous pouvez cliquer sur "oui" pour continuer l'installation.

Erreur lors de l'installation des paquets

L'installeur s'arrête ou affiche un message d'erreur lors de l'étape : "choisir et installer des logiciels" :

C'est peut-être uniquement parce que le CD-ROM utilisé est mal gravé ou abîmé.

Pour connaître la nature exacte du problème, vous pouvez réaliser les manipulations suivantes :

- [ctrl F2] (affiche la console de débogage)
- [nano /var/log/syslog] (édite le fichier de log)
- [ctrl W], [ctrl V] (va à la fin du fichier)

puis utilisez la *flèche du haut* pour remonter dans le fichier jusqu'à trouver les lignes contenant des erreurs.

La présence de l'expression "I/O Error" indique qu'il y a eu des erreurs de lecture, dans ce cas, il faut graver un nouveau CD.

Erreur lors de la création des conteneurs

Il est possible de suivre le processus d'installation des conteneurs dans le journal d'activité **/var/log/isolation.log**

Problèmes lors de la configuration

Pour détecter les problèmes de configuration, il faut utiliser la commande diagnose.

Mais, avant tout, il est recommandé de lancer un reconfigure avant de chercher un éventuel problème.

3 Les journaux système

Lorsque des problèmes surviennent en exploitation, les journaux système (ou journaux de bord, fichiers de log, fichiers de journalisation) constituent une source incomparable d'informations. Ils contiennent la succession des événements ou des actions qui sont survenus sur un système informatique donné.

Ces fichiers sont au format texte, et sont généralement stockés en local dans le répertoire **/var/log**

L'outil de log utilisé par EOLE est **rsyslogd** et la configuration se trouve dans **/etc/rsyslog.conf**

Ce fichier définit les messages à enregistrer et le fichier cible, cela permet éventuellement de filtrer (ou répartir) les messages, par leur source et leur degré d'importance.

La plupart des logiciels disposent d'un paramètre "*log level*" permettant de régler la verbosité des informations journalisées.

En cas de problème, il est conseillé d'augmenter le niveau de journalisation du logiciel incriminé.

Les fichiers les plus couramment utilisés sont :

- **/var/log/messages** : contient tous les messages d'ordre général concernant la plupart des services et démons.
- **/var/log/syslog** : est plus complet que **/var/log/messages**, il contient tous les messages, hormis les connexions des utilisateurs.
- **/var/log/auth** : contient les connexions des utilisateurs.
- **/var/log/mail.log** : contient les envois et réception de mails.
- **/var/log/cron** : fichier log du service cron (planificateur système).

Truc & astuce

Il est possible de lire le contenu d'un fichier avec la commande **less** :

```
less /var/log/syslog
```

Pour n'afficher que les dernières ligne d'un fichier, utiliser la commande **tail** :

```
tail -n 50 /var/log/syslog
```

La commande **tail** permet également d'afficher en temps réelle les nouvelles entrées dans un fichier. Pour cela, ajouter l'option *-f* :

```
tail -f /var/log/syslog
```

4 Générer un rapport

La commande [gen_rpt] permet de générer une archive de débogage incluant :

- les fichiers de configuration EOLE du serveur ;
- le diagnostic étendu ;
- la liste des processus en cours sur le serveur ;
- les règles de pare-feu appliquées sur le système ;
- l'historique des commandes système ;
- la liste des paquets installés ;
- plusieurs fichiers de journalisation ;
- le rapport d'extraction (Module Scribe) ;
- le rapport de sauvegarde (Module Scribe/Horus/Eclair).

L'archive nommée **<module>-<numéro-etab>.tar.gz** est enregistrée dans le répertoire courant (celui depuis lequel la commande a été lancée).

Si une passerelle de courrier a été définie sur le serveur, l'archive pourra être directement envoyée à l'équipe EOLE (merci de ne pas en abuser) ou à l'adresse de votre choix.

5 Trouver de l'information

les problèmes rencontrés fréquemment ont souvent déjà trouvés une solution, il existe diverses sources d'informations à votre disposition :

- les documentations ;
- la FAQ des documentations ;
- les archives des listes de diffusion ;
- recherche sur Internet ;
- équipes d'assistance académiques.

La plupart des logiciels fournit avec les modules EOLE sont largement utilisés en dehors de l'Éducation nationale.

Des documentations plus spécifiques à l'utilisation de la plupart des logiciels utilisés sont disponibles sur Internet (ex. http://doc.ubuntu-fr.org/cups).

Dans le cas de la mise en place d'une configuration avancée de l'un des logiciels, il est tout à fait indiqué de consulter sa documentation officielle (ex. http://www.cups.org/documentation.php).

Attention

Les documentations externes peuvent faire état de commandes systèmes à exécuter.

Il n'est pas forcément judicieux de suivre ces instructions car les modules EOLE disposent d'un système d'auto-configuration (Creole) qui risque d'écraser vos modifications ou même de ne plus fonctionner correctement.

En cas de doute, n'hésitez pas à demander.

Les fichiers de configuration

Certains logiciels libres manquent encore de documentation ou ne sont pas documentés du tout.

Dans ce cas, pensez à consulter le contenu de leur fichier de configuration.

Certains commentaires donnent des indications voire remplacent une documentation externe.

N'oubliez pas de consulter les pages de manuel installées sur le système avec la commande man :

```
# man man
```

```
# man commande
```

6 Quelques références

- site web officiel : http://eole.orion.education.fr ;
- accueil des listes de diffusion : http://eole.orion.education.fr/listes ;
- guide de survie : http://eole.orion.education.fr/wiki/index.php/EoleNG_GuideDeSurvie.

XIII Documentations techniques

1 Les dépôts EOLE

Architecture des dépôts EOLE

Le site de référence http://eoleng.ac-dijon.fr/eoleng propose pour chaque version de la distribution EOLE plusieurs catégories de paquets (les fichiers *.deb) :

- **eole-2.x-dev** : paquets en développement, même s'ils sont la plupart du temps fonctionnels ils peuvent parfois sérieusement endommager la stabilité du système. Ils ne doivent pas être installés sur une machine en production ;
- **eole-2.x-proposed** : paquets candidats, ces paquets sont éligibles pour passer en version stable mais attendent une validation des utilisateurs testeurs ;
- **eole-2.x-security** : paquets de sécurité, mises à jour de sécurité ;
- **eole-2.x-updates** : paquets de mises à jour, mise à jour fonctionnelles ;
- **eole-2.x** : paquets de la distribution tels que livrés sur le premier CD de la version majeure, aucun paquet n'y est ajouté après la publication.

Pour chaque catégorie de paquet, les paquets sont répartis par architecture :

- **all** : paquets compatibles avec toutes les architectures ;
- **i386** : paquets compilés spécifiquement pour l'architecture i386 ;
- **amd64** : paquets compilés spécifiquement pour l'architecture 64 bits.

Politique de publication des paquets

Les mises à jour sont composées de paquets dépendants les uns des autres. Avant toute publication sur le site de référence http://eoleng.ac-dijon.fr/eoleng et sur les miroirs académiques (ex. : ftp://ftp.crihan.fr), les paquets sont copiés sur le dépôt http://test-eoleng.ac-dijon.fr. Ce dépôt est réservé aux développeurs et aux contributeurs et permet d'avoir les paquets à disposition tels qu'ils le seront lors de la publication officielle.

Le délai de synchronisation des paquets entre les 2 dépôts varie en fonction du type de paquet :

- **eole-2.x-dev** : synchronisé en permanence ;
- **eole-2.x-proposed** : synchronisation deux fois par jour ;
- **eole-2.x-security** : synchronisation manuelle avec annonce préalable ;
- **eole-2.x-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.x** : aucune modification sur ce dépôt.

2 Gestion des logs

Architecture cible

Dans un souci d'harmonisation et de centralisation de l'information, la quasi totalité des logs est désormais rassemblée sur le maître dans le répertoire : **/var/log/rsyslog/local**

Par défaut, les logs des services installés dans un conteneur et qui utilisent rsyslog sont remontés sur le maître (fichiers de configuration : **/etc/rsyslog.d/99-aggregation.conf** dans les conteneurs).

L'utilisation de rsyslog laisse la possibilité de réaliser une configuration spécifique pour chaque service.

C'est déjà le cas pour `squid` par exemple (template : **80-squid.conf**).

Le répertoire **/var/log/rsyslog/remote** est quant à lui prévu pour recevoir les journaux de serveurs distants dans le cas de la mise en place d'un serveur de log centralisé (l'équivalent du serveur 2.2 : `ZéphirLog`).

Exceptions connues

A l'heure actuelle, plusieurs services ne sont pas directement pris en charge par rsyslog :

- les logs de `Samba` sont toujours stockés dans le répertoire : **/var/log/samba** et ne sont pas remontés sur le maître ;
- les logs de `ltsp-cluster-lbagent` et `ltsp-cluster-lbserver` sont toujours stockés dans le répertoire **/var/log** et ne sont pas remontés sur le maître.

Un lien symbolique permet toutefois d'accéder directement aux fichiers depuis le maître.

Rotation des logs

Les programmes dont les logs sont centralisés sur le maître doivent avoir une configuration *logrotate* avec les chemins adaptés sur le maître.

Attention

Si le service est susceptible d'être installé dans un conteneur et qu'il doit être redémarré, il faut penser à adapter les commandes.

La commande `CreoleService` permet, par exemple, de gérer un service y compris si celui-ci est dans un conteneur :

```
CreoleService -c <conteneur> <service> restart
```

XIV Les sauvegardes

1 Généralités sur la sauvegarde

La **sauvegarde** (*Backup*, en anglais) 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** (l'opération inverse de la sauvegarde) :

- la restauration de tout ou partie du SI, suite à une *dégradation* importante du SI, voire une *destruction* (disaster recovery) ;
- 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, à des fins de restauration rapide, ou elle peut être *archivée*, voire *externalisée*.

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.

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.

1.3. Sauvegarde différentielle

Une **sauvegarde différentielle** réalise une copie des fichiers crées ou modifiés, en se basant sur les différences constatées avec la **dernière sauvegarde totale** (quelles que soient les sauvegardes intermédiaires).

Attention

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.

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

2 La sauvegarde EOLE

EOLE utilise l'outil de sauvegarde libre **Bacula**.

Bacula permet de sauvegarder :

- des fichiers/dossiers
- les droits POSIX*
- les ACLs *

Bacula 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.

Bacula supporte, entre autres, la possibilité de faire des sauvegardes sur plusieurs unités de stockage, si la capacité est insuffisante.

2.1. Le vocabulaire Bacula

Bacula utilise un nombre important de ressources pour définir une sauvegarde.

http://www.bacula.org/5.0.x-manuals/en/main/main/What_is_Bacula.html

Quelques définitions

Job

L'objet le plus élevé est la définition d'un **Job**, représentant une "sauvegarde" au sens Bacula du terme.

Un Job Bacula est une ressource de configuration qui définit le travail que Bacula 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://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00183000000000000000

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://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00185000000000000000

Volume

Un **Volume** est une unité d'archivage, usuellement une cartouche ou un fichier nommé sur disque où Bacula stocke les données pour un ou plusieurs **jobs** de sauvegarde. Tous les volumes Bacula ont un **label** unique (logiciel) écrit sur le volume par Bacula 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 Bacula 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://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00181500000000000000

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://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00187000000000000000

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://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00181400000000000000

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://www.bacula.org/5.0.x-manuals/en/main/main/Storage_Daemon_Configuratio.html#SECTION00203000000000000000

Catalog

La ressource Catalog précise quel catalogue utiliser pour le job courant. Actuellement, Bacula ne peut utiliser qu'un type de serveur de bases 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 Bacula.

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 Bacula, 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 Bacula se fait à deux niveaux:

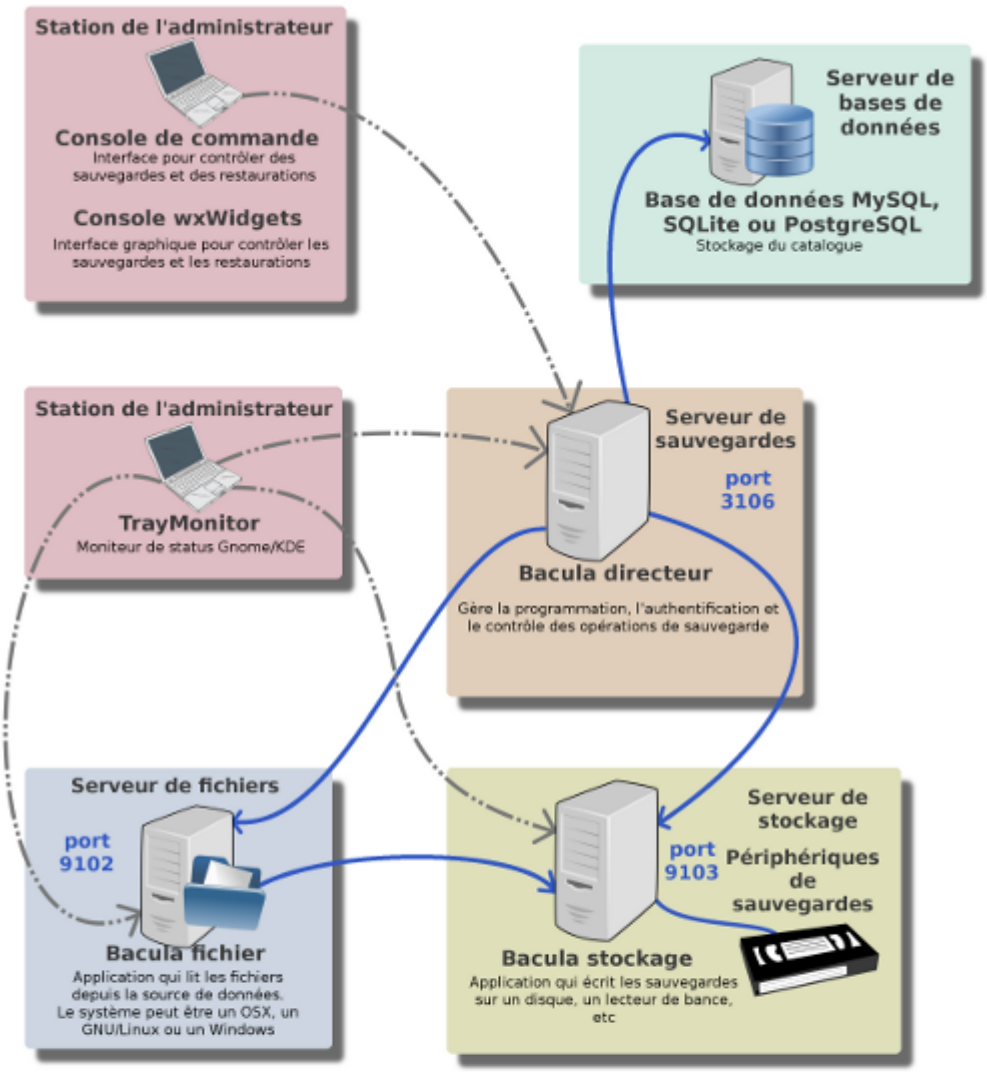
- les fichiers de configuration ;
- la base de données.

Bacula 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 Bacula, donc il faut préférer le résultat des commandes console aux valeurs des fichiers.

http://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00181600000000000000

2.2. Architecture de Bacula

Bacula est construit suivant une **architecture distribuée** :



Architecture distribuée de Bacula

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 defaut et peuvent être changés.

- 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 **bacula-director** ;
- 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 **bacula-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 **bacula-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 Bacula 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 :

- bacula-director
- bacula-sd
- bacula-fd

Truc & astuce

Plusieurs directeurs peuvent envoyer les données sur un unique serveur de stockage en établissement.

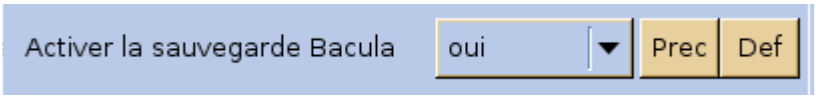
Il est également possible de copier les sauvegardes au travers d'autres protocoles réseau : rsync, samba, ssh, *etc*.

2.3. Configuration des sauvegardes

La configuration des sauvegardes consiste en une activation sur le module et en une configuration qui peut se faire soit par l'EAD soit en ligne de commande.

2.3.1. Activation et configuration de Bacula

Avant tout, vérifier que Bacula est bien activé dans l'onglet Services de l'interface de configuration du module.



Suite à l'activation, un onglet Bacula apparaît dans l'interface de configuration du module.

Dans cet onglet il faut activer localement le directeur, définir si le serveur de stockage est distant ou local et configurer les périodes de rétention.

Configuration du directeur

Si le directeur n'est pas activé localement sur le module, aucune sauvegarde ne sera effectuée.

Le nom du directeur est une information importante.

Ce nom est utilisé en interne dans le logiciel mais, surtout, il est nécessaire pour configurer un client Bacula ou pour joindre un serveur de stockage externe.

Attention

Ne changez jamais le nom du directeur après l'instanciation du serveur.

Cette variable est utilisée dans les noms des fichiers de sauvegarde.

Ensuite, il est nécessaire de définir les durées de rétention* 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.

Exemple

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.

Attention

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

Afin de prendre en compte la nouvelle valeur, il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et ré-initialiser la base de données Bacula avec la commande :

```
# /usr/share/eole/posttemplate/00-bacula instance
Le catalogue Bacula a déjà été initialisé, voulez-vous le réinitialiser ? [oui/non] oui
```

Truc & astuce

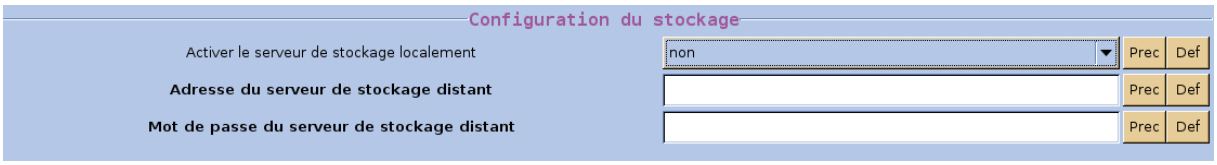
En mode expert, il est possible de définir l'algorithme de compression utilisé pour le stockage.

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.

Configuration du stockage

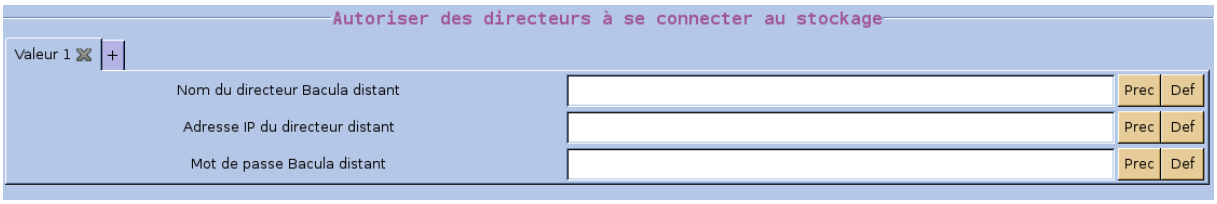
Le stockage peut être local ou distant.

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



Autoriser des directeurs à se connecter au stockage

Il peut être intéressant de connecter un directeur Bacula distant au serveur de stockage local.



Pour ce faire il faut autoriser une ou plusieurs adresses IP à se connecter sur le serveur.

Le mot de passe est par défaut régénéré à chaque reconfiguration, il est donc nécessaire de le fixer si l' on veut pouvoir connecter un client.

Attention

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 serveur est nécessaire avec la commande : [reconfigure].

2.3.2. Configuration depuis l'EAD

Une fois le stockage Bacula 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 supports 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**

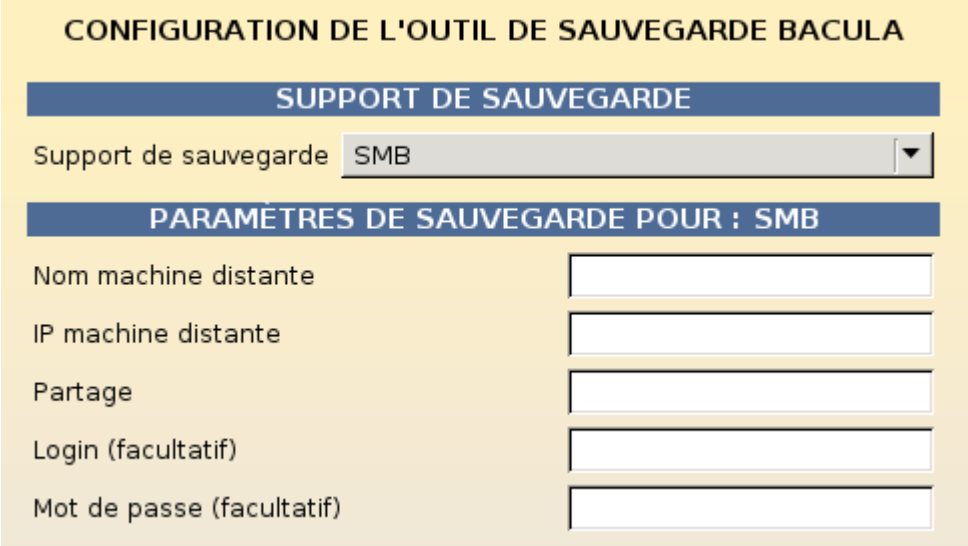
- **SMB** : la sauvegarde se fait à travers un partage SMB*.

  Il est préférable de déporter le serveur de stockage Bacula plutôt que d'utiliser le protocole SMB*.

  Ce type de sauvegarde sera utilisé, par exemple, pour les NAS*.

  Les informations suivantes sont demandées :

  - **Nom de machine de la machine distante** ;
  - **IP de la machine distante** ;
  - le nom du **Partage** ;
  - optionnellement le **Login**, le **Mot de passe**.

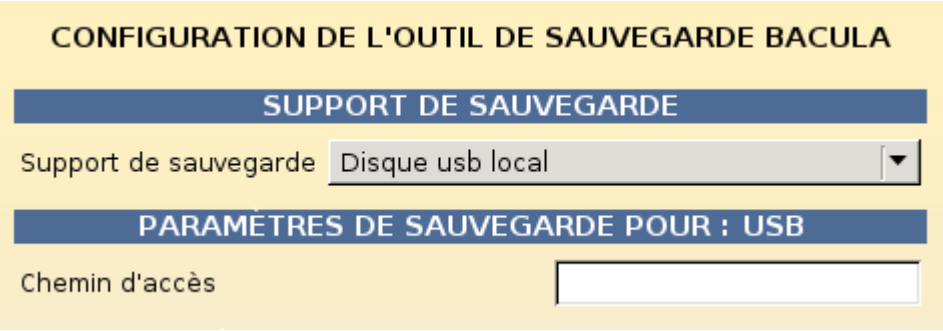


Attention

Les informations stockées dans les sauvegardes sont sensibles, il donc préférable de toujours authentifier l'accès aux partages contenant les données.

- **Disque USB local** : la sauvegarde se fait sur un support nécessitant un montage (disque USB, disque interne, etc.), contrôlé avant chaque sauvegarde.

  Le chemin d'accès à saisir correspond au nœud du périphérique (par exemple **/dev/hda1**).



Attention

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 Bacula. 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 **baculasupport.conf** est dans **/usr/share/eole/creole/distrib/**

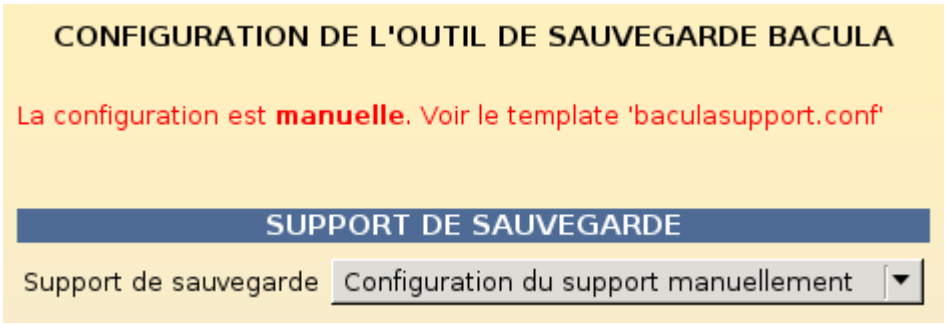
Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE*.

Consulter la documentation sur la personnalisation d'un serveur à l'aide de Creole

Voir la documentation officielle de Bacula pour le paramétrage :

http://www.bacula.org/5.0.x-manuals/en/main/main/Supported_Tape_Drives.html

http://www.bacula.org/5.0.x-manuals/en/main/main/Getting_Started_with_Bacula.html



Attention

Le support doit être monté sur **/mnt/sauvegardes** et l'utilisateur `bacula` doit avoir les droits en écriture :

Pour connaître les périphériques qui sont montés

```
# mount
```

Pour monter le périphérique

```
# /usr/share/eole/bacula/baculamount.py --mount
```

Lire les droits du répertoire **sauvegardes** :

```
# ls -l /mnt
```

```
# rwxr-xr-x 2 bacula root 4096 févr. 20 11:08 sauvegardes
```

Si les droits ne sont pas bons, utiliser la commande suivante :

```
# chown -R bacula:root /mnt/sauvegardes
```

Paramètres pour l'envoi de rapports

L'envoi de courriels est proposé si le directeur Bacula est activé sur le serveur.

EOLE offre la possibilité d'envoyer deux types de courriel :

- les rapports d'erreurs de Bacula ;
- 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. Penser à configurer correctement votre relai SMTP*.

Truc & astuce

Il est possible de déclarer plusieurs destinataires en séparant les adresses par des virgules.

Exemple : `admin@ac-dijon.fr,technicien@ac-dijon.fr`

2.3.3. 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 [baculaconfig.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 :

```
# /usr/share/eole/bacula/baculaconfig.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 :

```
# /usr/share/eole/bacula/baculaconfig.py -s usb --usb_path=/dev/device_usb
```

- Si le support est à configurer manuellement :

```
# /usr/share/eole/bacula/baculaconfig.py -s manual
```

Vous devez ensuite configurer le support dans le fichier template **/usr/share/eole/creole/distrib/baculasupport.conf**

Pour que la solution soit pérenne il est nécessaire de créer un patch EOLE.

Truc & astuce

Pour tester le support de sauvegarde (USB local ou SMB), il est possible d'utiliser le script [baculamount.py] :

```
# /usr/share/eole/bacula/baculamount.py -t
Test de montage OK
```

En cas d'échec du montage, la commande donne un indice sur la cause :

- permissions : bacula n'a pas le droit d'écrire sur le support de sauvegarde monté ;
- point de montage : le périphérique monté sur /mnt/sauvegardes ne correspond pas à la configuration de bacula ;
- montage : aucun montage ne correspond à /mnt/sauvegardes

Paramètres pour l'envoi de rapports

La configuration de l'adresse courriel se fait de la façon suivante :

```
# /usr/share/eole/bacula/baculaconfig.py -m --mail_ok=adresse_courriel
--mail_error=adresse_courriel
```

Les paramètres --mail_ok et --mail_error ne sont pas obligatoires.

Attention

A chaque fois que vous configurez les adresses courriels, vous supprimez la configuration précédente.

Il n'est pas possible de modifier une seule des deux adresses `mail_ok` ou `mail_error`.

Si l'un des deux paramètres n'est pas spécifié, les adresses associées seront supprimées de la configuration de Bacula.

Afficher la configuration

Il est possible de lister l'ensemble des paramètres depuis la ligne de commande avec la commande [baculaconfig.py] :

```
# /usr/share/eole/bacula/baculaconfig.py -d
Support : {'usb_path': '/dev/sdb1', 'support': 'usb'}
Mail : {}
Programmation : non configuré
```

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.

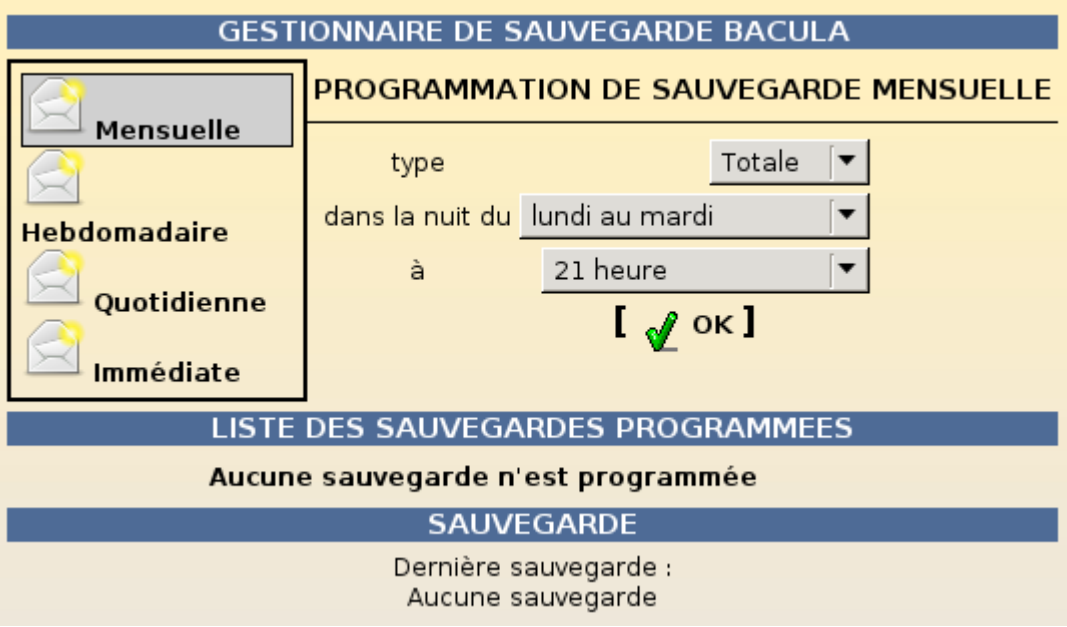
Si une autre sauvegarde est programmée la même nuit, celle-ci sera automatiquement reportée à la semaine d'après.

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.



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 :

/usr/share/eole/bacula/baculaconfig.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 :

/usr/share/eole/bacula/baculaconfig.py -n --level=Full

Il est possible de suivre l'évolution de la sauvegarde dans le fichier */var/log/rsyslog/local/bacula-dir/bacula-dir.err.log*

Truc & astuce

/usr/share/eole/bacula/baculaconfig.py --help donne la liste des options de **baculaconfig.py**

Il existe également des pages de manuel :

man bacula, *man bacula-dir*, ...

Afficher la configuration

Il est possible de lister l'ensemble de la configuration depuis la ligne de commande avec la commande [baculaconfig.py] :

```
# /usr/share/eole/bacula/baculaconfig.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 [baculaconfig.py] . Elle s'utilise comme suit :

```
# /usr/share/eole/bacula/baculaconfig.py -x <numéro_job>
```

ou encore :

```
# /usr/share/eole/bacula/baculaconfig.py --job_to_delete=<numéro_job>
```

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.

3.1. 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 niveau du serveur sauvegardé.

Mettre à jour les paquets :

[Maj-Auto -i]

Choix du mode conteneur ou non

Si le serveur sauvegardé était en mode conteneur, il faut re-créer les conteneurs, avec la commande [gen_conteneurs].

Configurer Bacula

- 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 Bacula pour un serveur non enregistré dans Zéphir

  ```
  # /usr/share/eole/bacula/baculaconfig.py -s usb --usb_path=/dev/device_usb
  ```

  Il est normal d'avoir le message suivant lors de l'utilisation de [baculaconfig.py] :

  ```
  Fichier template /var/lib/creole/baculasupport.conf inexistant
  ```

  Il peut être utile de configurer l'envoi des courriels en même temps que le support de sauvegarde.

  ```
  # /usr/share/eole/bacula/baculaconfig.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 :

```
# /usr/share/eole/bacula/baculamount.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 :

```
# /usr/share/eole/bacula/bacularestore.py --catalog nom_du_directeur
Restauration du catalog
Pas de fichier /var/lib/eole/config/baculajobs.conf dans le volume
nom_du_directeur-catalog-0003
Pas de fichier /etc/eole/bacula.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 :

```
# /usr/share/eole/bacula/baculamount.py --umount
```

Instanciation

Instancier maintenant votre serveur avec la commande : [instance zephir-restore.eol]

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 Bacula a déjà été initialisé, voulez-vous le réinitialiser ?
[oui/non]
```

Ne pas tenir compte du message d'erreur suivant :

```
ERREUR : /var/lib/eole/config/shedule.conf not exist
```

Restauration

Avant de lancer la restauration il est préférable de vérifier que le chemin du nœud du périphérique est toujours bon.

Il peut changer en fonction du nombre de périphériques connectés :

```
# /usr/share/eole/bacula/baculamount.py -t
```

Si le périphérique n'a plus le même nœud la commande [baculamount.py] renvoie :

```
ERREUR : le périphérique /dev/sdb1 n'existe pas
```

Il faut alors changer la configuration du support :

```
# /usr/share/eole/bacula/baculaconfig.py -s usb --usb_path=/dev/device_usb
```

Le test de montage doit renvoyer OK :

```
# /usr/share/eole/bacula/baculamount.py -t
Test de montage OK
```

Lister l'ensemble de la configuration :

```
# /usr/share/eole/bacula/baculaconfig.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 [bacularestore.py] :

```
# /usr/share/eole/bacula/bacularestore.py --all
```

Il est possible de suivre l'évolution des restaurations dans le fichier de log : **/var/log/bacula/restore.txt**

Les informations peuvent mettre un peu de temps avant d'apparaître car Bacula 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, re-configurez votre serveur avec la commande [reconfigure].

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` :

```
# /usr/share/eole/bacula/bacularestore.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 :

```
# /usr/share/eole/bacula/bacularestore.py --search nom_du_\*
```

Il est également possible de lister le contenu d'un répertoire sauvegardé avec l'option `--ls_folder` :

```
# /usr/share/eole/bacula/bacularestore.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 :

```
# /usr/share/eole/bacula/bacularestore.py --file /chemin_absolu/nom_du_fichier
```

Exemple :

```
# /usr/share/eole/bacula/bacularestore.py --file /etc/eole/config.eol
```

Pour restaurer un répertoire et l'intégralité de son contenu, on peut utiliser la commande :

```
# /usr/share/eole/bacula/bacularestore.py --folder
/chemin_absolu/nom_du_répertoire
```

Exemple :

```
# /usr/share/eole/bacula/bacularestore.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 :

```
# /usr/share/eole/bacula/bacularestore.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 :

```
# /usr/share/eole/bacula/bacularestore.py --help
```

Exemple

Pour restaurer l'annuaire :

```
# /usr/share/eole/bacula/bacularestore.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 :

```
# /usr/share/eole/bacula/baculamount.py -t
```

Si le périphérique n'a plus le même nœud la commande [baculamount.py] renvoie :

```
ERREUR : le périphérique /dev/sdb1 n'existe pas
```

Il faut alors changer la configuration du support :

```
# /usr/share/eole/bacula/baculaconfig.py -s usb --usb_path=/dev/device_usb
```

Le test de montage doit renvoyer OK :

```
# /usr/share/eole/bacula/baculamount.py -t
Test de montage OK
```

Lister l'ensemble de la configuration :

```
# /usr/share/eole/bacula/baculaconfig.py -d
```

La restauration manuelle s'effectue au moyen d'un programme en ligne de commande **bconsole** :

```
# bconsole -c /etc/bacula/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/bacula/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/bacula/restore.txt**

Les informations peuvent mettre un peu de temps avant d'apparaître car Bacula 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.

Attention

Pour conserver les droits étendus associés à un fichier (ACL), il faut restaurer un fichier issu d'une partition avec ACL (par exemple le répertoire **/home** sur le module Scribe) dans une partition supportant les ACL.

4 Diagnostic et rapport

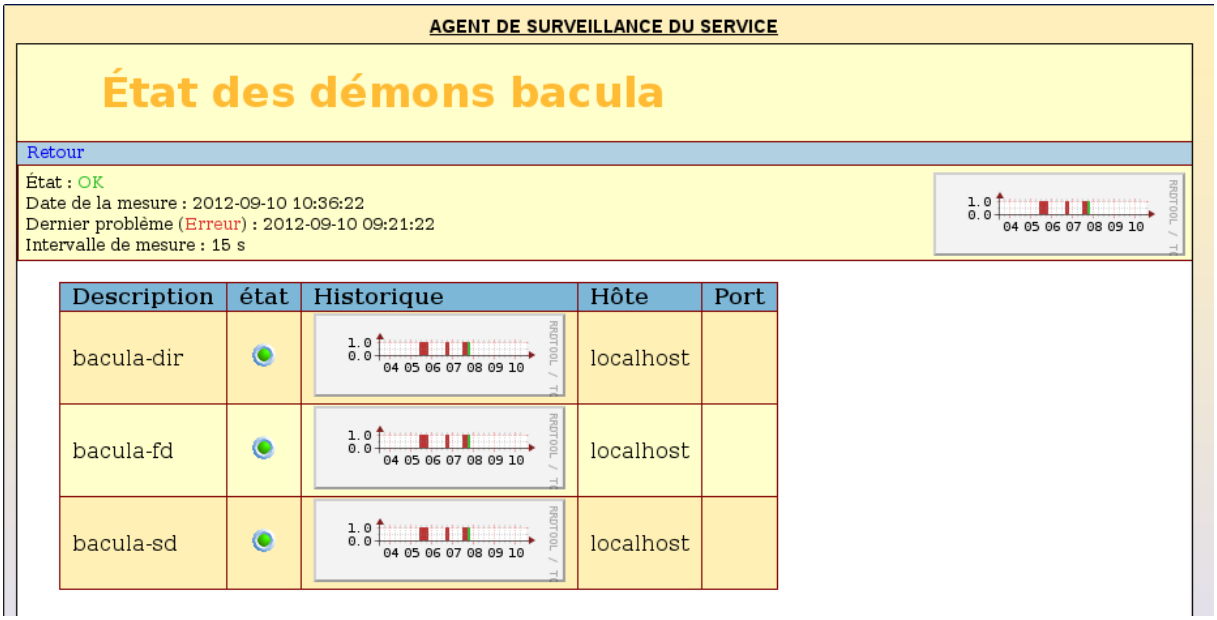
Parallèlement à l'envoi de courrier électronique, il est possible de connaître l'état de la dernière sauvegarde par l'utilisation la commande [diagnose]. Celle-ci liste également l'état des différents services de Bacula.

```
*** Sauvegarde
Test de Bacula Director :
.             Bacula Director => Ok
.    fichier de configuration => Ok
Test de Bacula Client :
.              Bacula Client => Ok
.    fichier de configuration => Ok
Test de Bacula Storage :
.             Bacula Storage => Ok
.    fichier de configuration => Ok
.          Montage du support => Erreur
Statut des sauvegardes :
.      sauvegarde principale => Erreur : Sauvegarde échouée le mercredi 05 septembre 2012 à 13:00.
.       sauvegarde catalogue => Ok : Sauvegarde terminée le lundi 27 août 2012 à 15:53.
```

L'EAD permet également de connaître l'état de la dernière sauvegarde dès l'arrivé sur la page d'accueil.

Le détail de la sauvegarde est disponible en cliquant sur [Afficher le rapport].

Par contre pour voir l'état des différents services Bacula il faut sélectionner [DETAILS] dans SERVICES, ETAT DES SERVICES de la page d'accueil, puis sélectionner [État des démons bacula].



Si l'un des services Bacula est arrêté, il est possible de le relancer avec la commande [service] :

```
root@eole:~# service bacula-director restart
* Stopping Bacula Director ... [ OK ]
* Starting Bacula Director ... [ OK ]
```

L'administration de Bacula peut se faire au travers d'une **console**, en mode texte elle se lance par la commande [bconsole] :

```
root@eole:~# bconsole
Connexion au Director 127.0.0.1:9101
1000 OK: scribe-dir Version: 5.0.1 (24 February 2010)
Tapez un point (.) pour annuler une commande.
*
```

Le prompt est une étoile (*), la console accepte la complétion, voici les commandes de base :

* `help` → pour avoir de l'aide
* `quit` → pour quitter
* `messages` → les messages en attente
* `status` → affiche les rapports, un menu propose plusieurs options qu'il est possible d'atteindre directement
* `status dir` → affiche les rapports du Director
* `status all` → affiche tous les anciens rapports, permet d'afficher les anciens messages

5 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/bacula/baculafichiers.d/**

Celui-ci ne doit comporter que les directives `Include` et `Exclude`, il ne faut pas, par exemple, spécifier le `Name` du FileSet car il est déjà défini dans le reste de la configuration.

Exemple d'un fichier de configuration pour la prise en charge de nouvelles données à sauvegarder :

```
Include {
   Options {
      # Sauvegarde des ACL
      aclsupport = yes
      # Tous les fichiers seront chiffrés en SHA1
      signature = SHA1
      # Compression des fichiers (niveau de com pression croissant de 0 à 9)
      compression = GZIP6
      # Permet de sauvegarder plusieurs systèmes de fichiers
      onefs = yes
   }
   File = /chemin/du/repertoire/ou/du/fichier/a/sauvegarder
   File = /chemin/du/repertoire/ou/du/fichier/a/sauvegarder
}
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 Bacula :

http://www.bacula.org/5.0.x-manuals/en/main/main/Configuring_Director.html#SECTION00187000000000000000

Attention

Pour que l'ajout d'un fichier de configuration soit pris en compte par Bacula il faut procéder à la reconfiguration du module avec la commande [reconfigure].

6 Annexes

Voici un complément d'information pour aller plus loin avec Bacula.

6.1. Autres outils d'administration pour Bacula

L'administration de Bacula 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 Bacula à distance.

Différentes versions existent :

- **bconsole** est la console en mode texte ;
- **Bacula Administration Tool** (BAT) est l'interface graphique standard qui permet d'exploiter bconsole, installable (25Mo) sur les modules EOLE avec la commande :

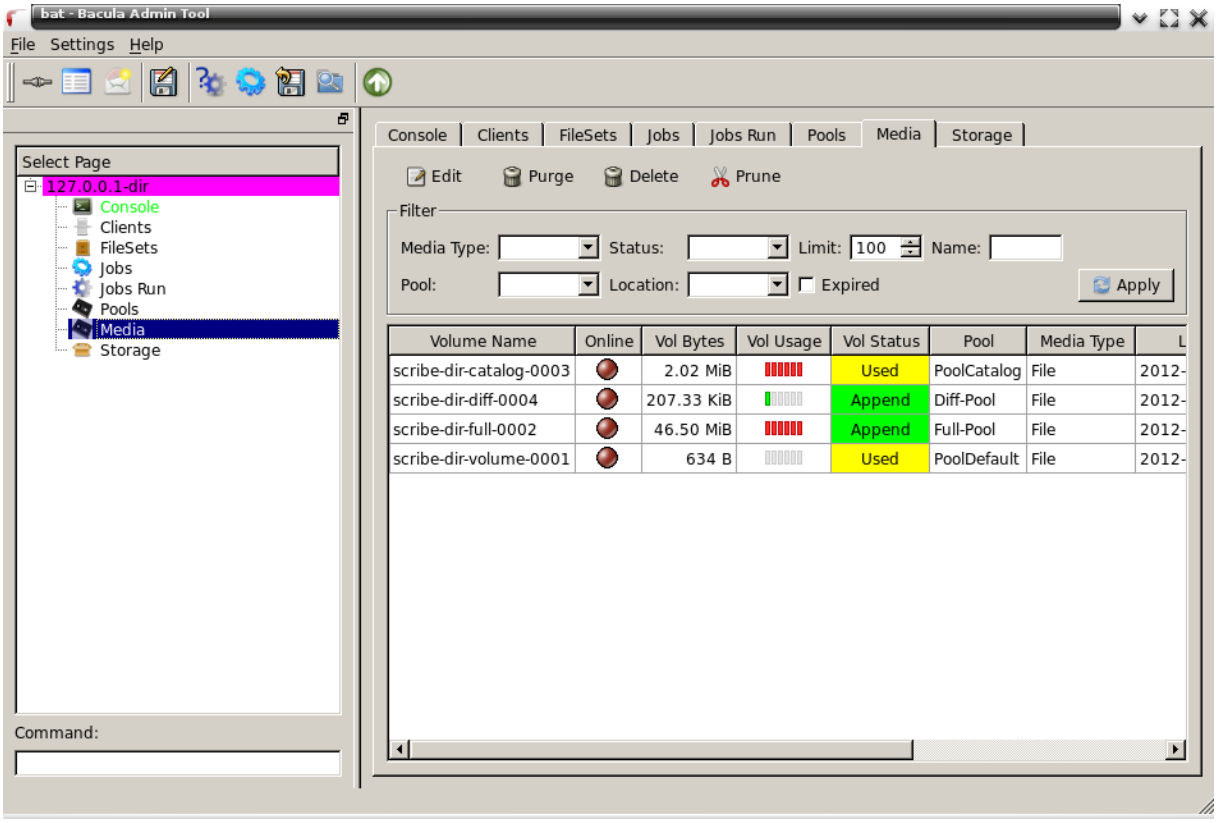
  [apt-eole install bacula-console-qt].

  BAT se lance avec la commande suivante :

  [bat -c /etc/bacula/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>
  ```



- **bgnome-console** est une console graphique (notamment pour les opérations de restauration), mais nécessite l'installation des librairies GNOME 2.x ;
- **bwx-console** est une version graphique utilisant wxWidgets

  L'installation de bwx-console est décrite pour Mandriva et pour Ubuntu à l'adresse suivante : http://m-k.cc/spip.php?rubrique3
- **bacula-win** (http://sourceforge.net/projects/bacula/files/) permet notamment d'installer :
  - un client Windows (File Daemon) ;
  - des consoles : BAT, bconsole et TrayMonitor.

Il existe aussi des versions Web comme **bacula-web** écrit en PHP ou **bweb** écrit en perl.

Pour avoir plus d'informations sur les outils mentionnés : http://www.bacula.org/manuals/en/console/console/GUI_Programs.html

6.2. Quelques références

- Définition de la sauvegarde : http://fr.wikipedia.org/wiki/Sauvegarde
- Le site officiel de Bacula : http://bacula.org
  - L'accès à la documentation : http://bacula.org/fr/?page=documentation

- Tutoriel : http://bacula.org/5.0.x-manuals/en/developers/developers/Developer_s_Guide.html
- Manuel utilisateur : http://bacula.org/2.4.x-manuals/en/main/index.html

Il existe des versions française et anglaise de ces documentations, en HTML mais aussi en PDF.

- Le wiki : http://wiki.bacula.org/doku.php
- Des présentations : http://bacula.org/en/?page=presentations

Définition des éléments de sauvegarde Bacula :

http://bacula.org/5.0.x-manuals/en/main/main/What_is_Bacula.html

6.3. Création d'un partage Windows XP

Introduction

EOLE permet 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 :

- création d'un "compte local" sur la station Windows ;
- partage du dossier et réglage des droits d'accès.

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).

Remarque

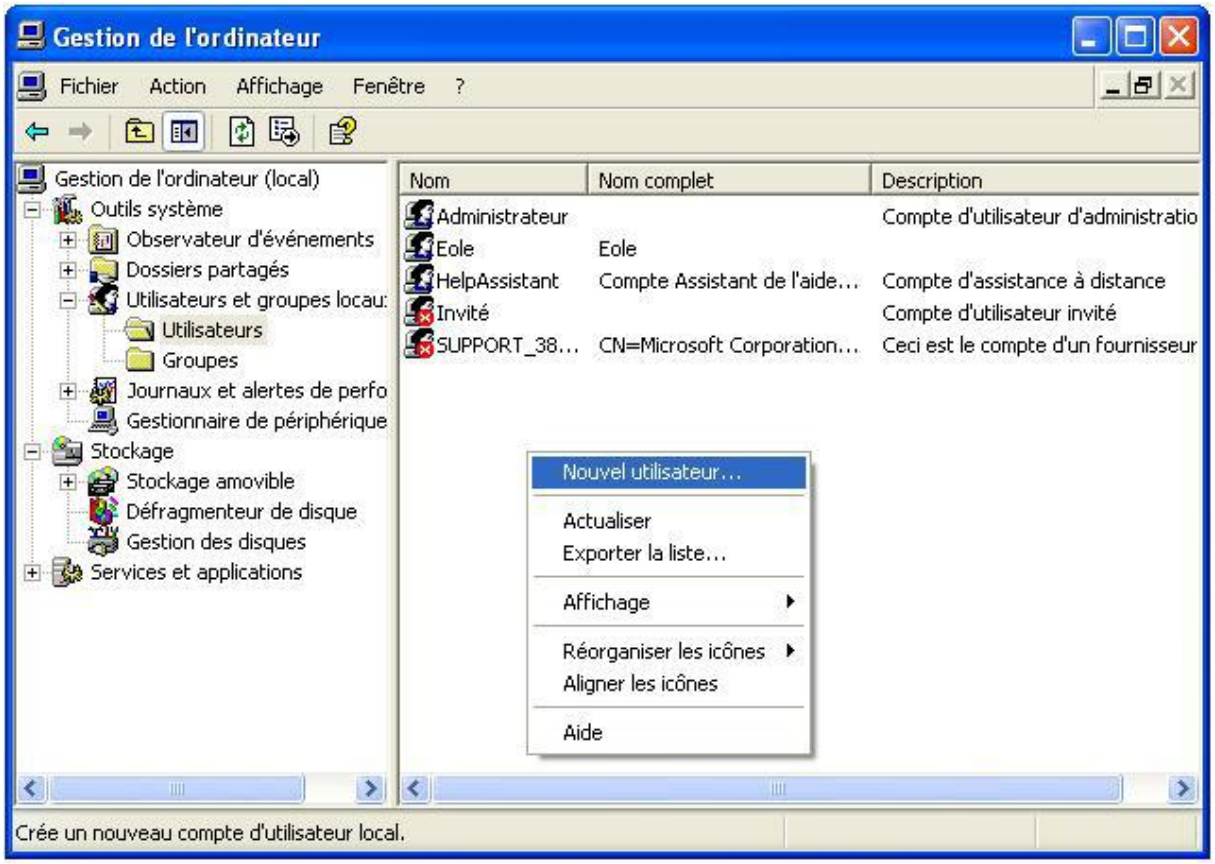
Il n'est pas impossible de donner des droits d'accès au partage à un compte du domaine mais cela pose problème pour les sauvegardes. Pour avoir accès au partage, la station va vérifier la validité de l'utilisateur et de son mot de passe auprès du contrôleur de domaine. Or, pour éviter qu'un fichier/dossier ne soit modifié pendant la sauvegarde, Bacula 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.

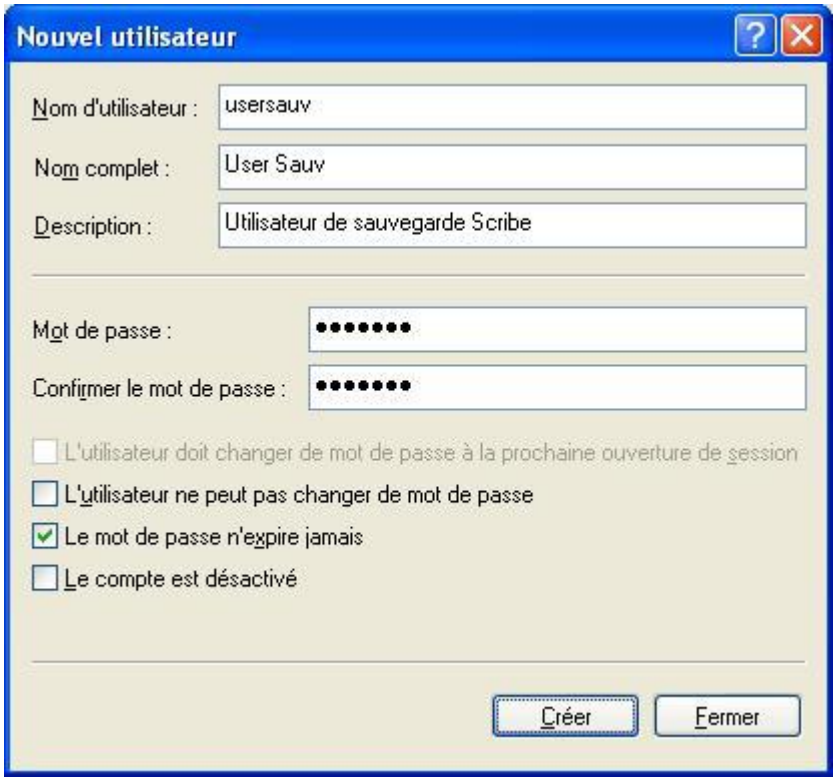
Création d'un compte sur le poste Windows

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)

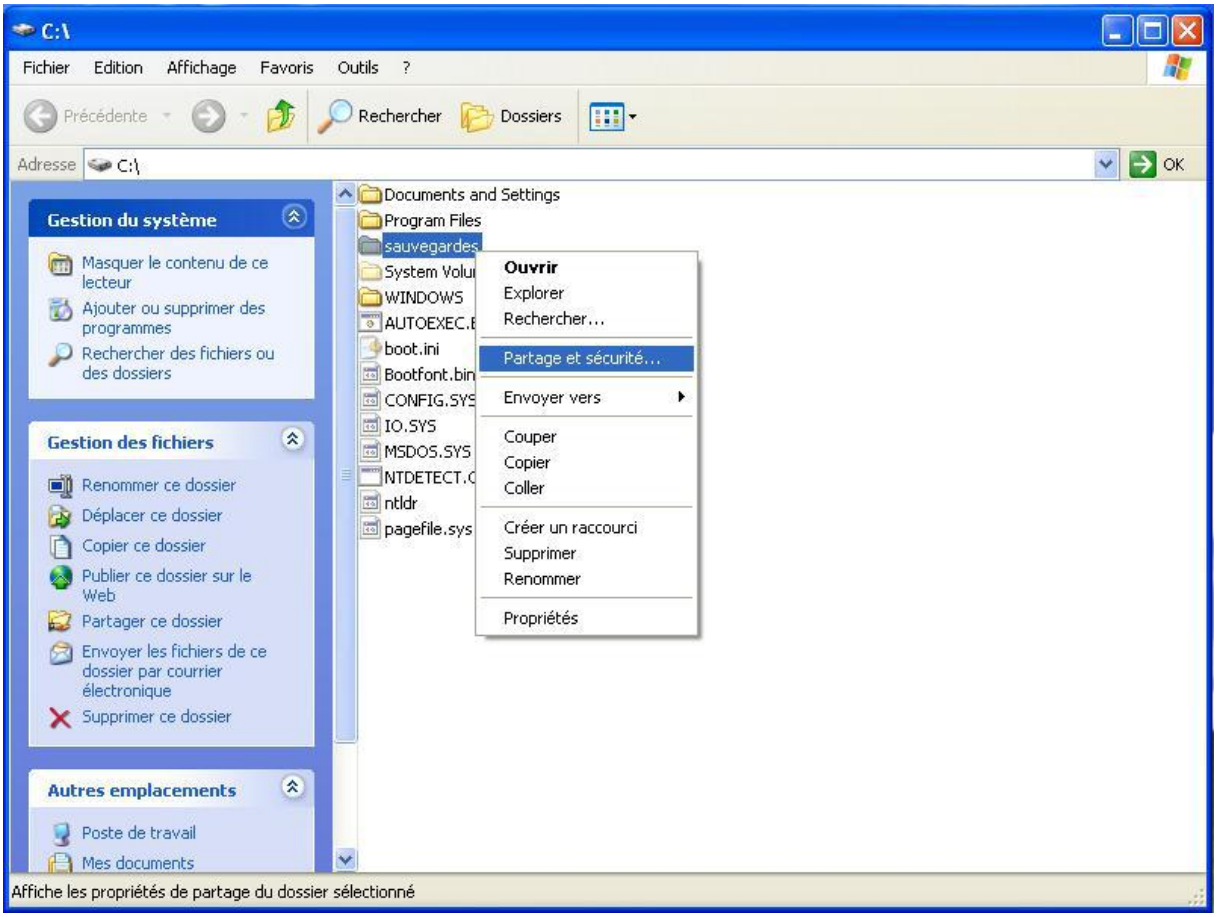


...avec les options configurées comme ceci :

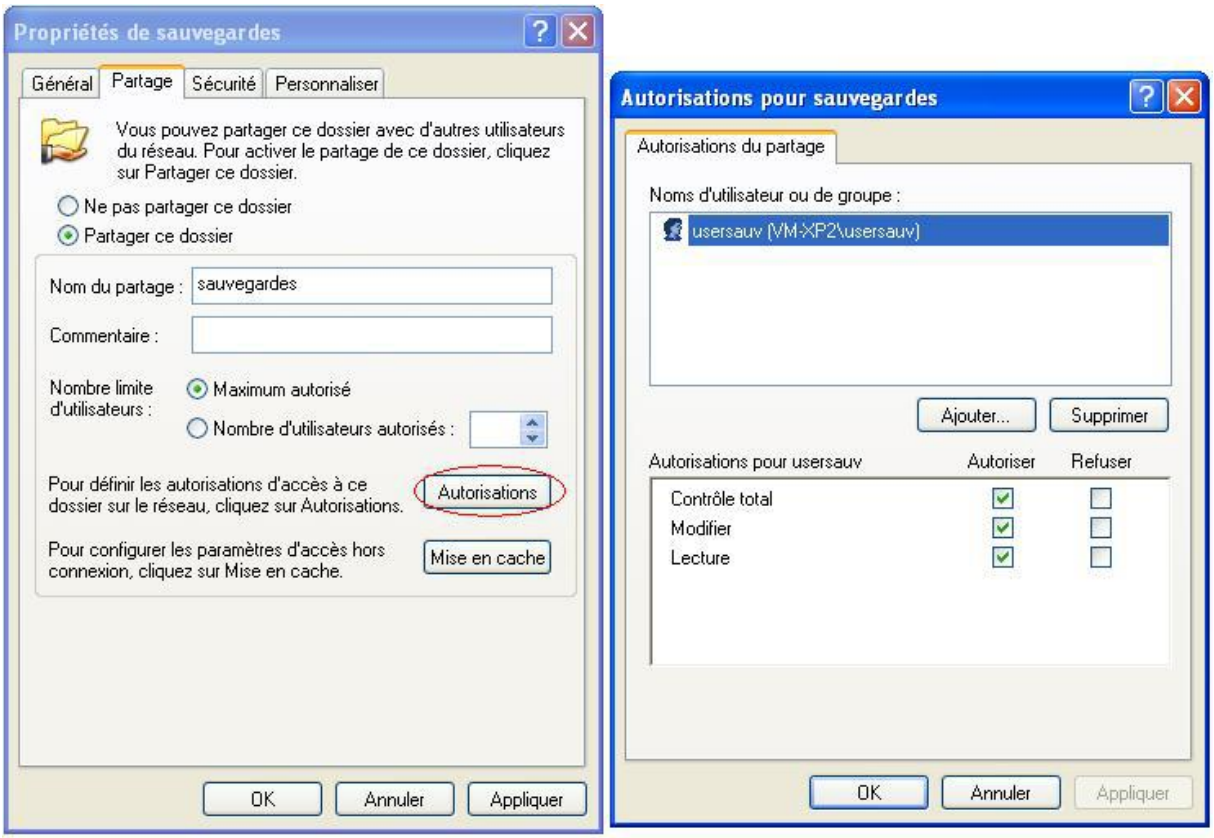


Partage du dossier et réglage des droits d'accès

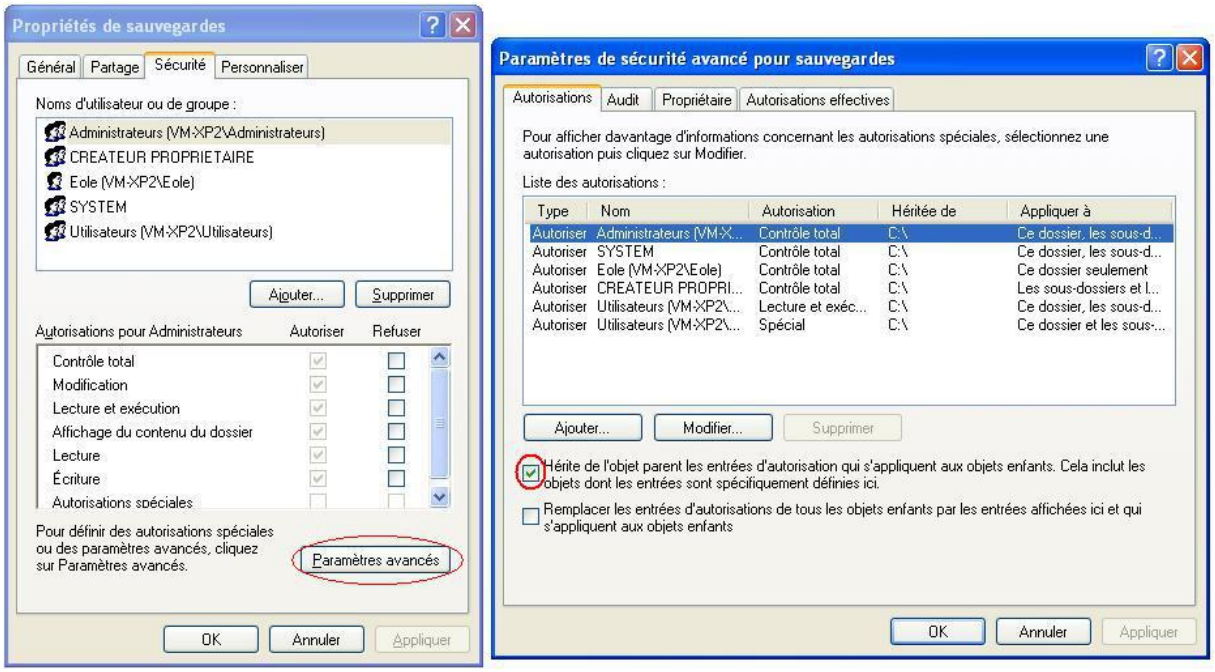
Après avoir créé un dossier "*sauvegarde*" à l'emplacement de votre choix, partagez-le (clic droit sur le dossier) :



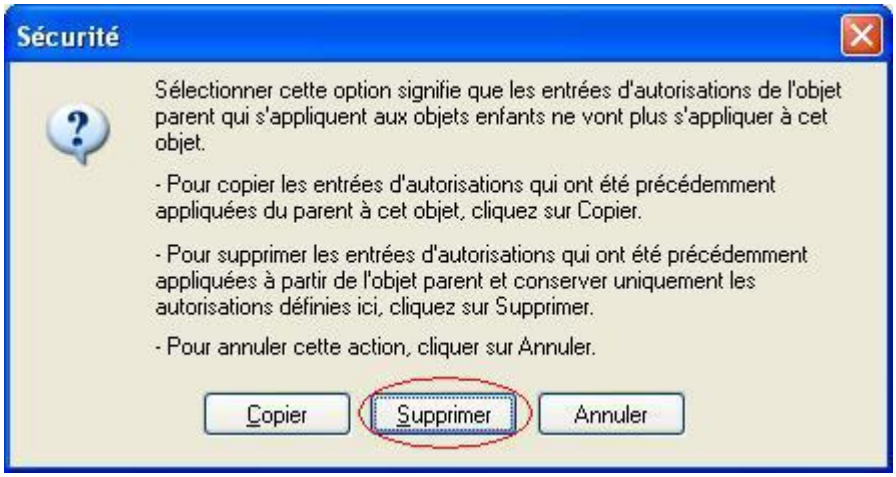
Puis cliquez sur **Autorisations**. Supprimez les autorisations par défaut ("*Tout le monde*") puis ajoutez "*usersauv*" avec "**Contrôle total**" :



Fermez la fenêtre des autorisations puis allez dans l'onglet "**Sécurité**" et cliquez sur "**Paramètres avancés**" :

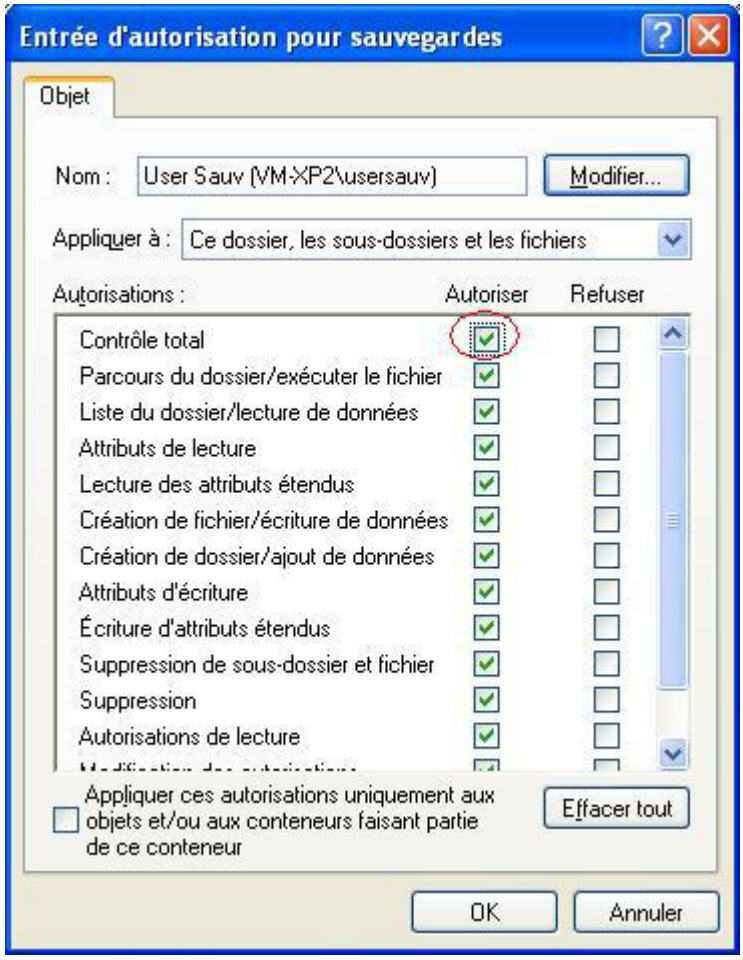


Décochez "**Hérite de l'objet parent...**", une fenêtre s'ouvre alors, sélectionnez "**Supprimer**" :



Ajoutez ensuite l'utilisateur "*usersauv*" toujours avec le "**Contrôle total**" :

Enfin, affectez le "**Contrôle total**" :



XV 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*.

Deux interfaces sont disponibles pour gérer les imprimantes :

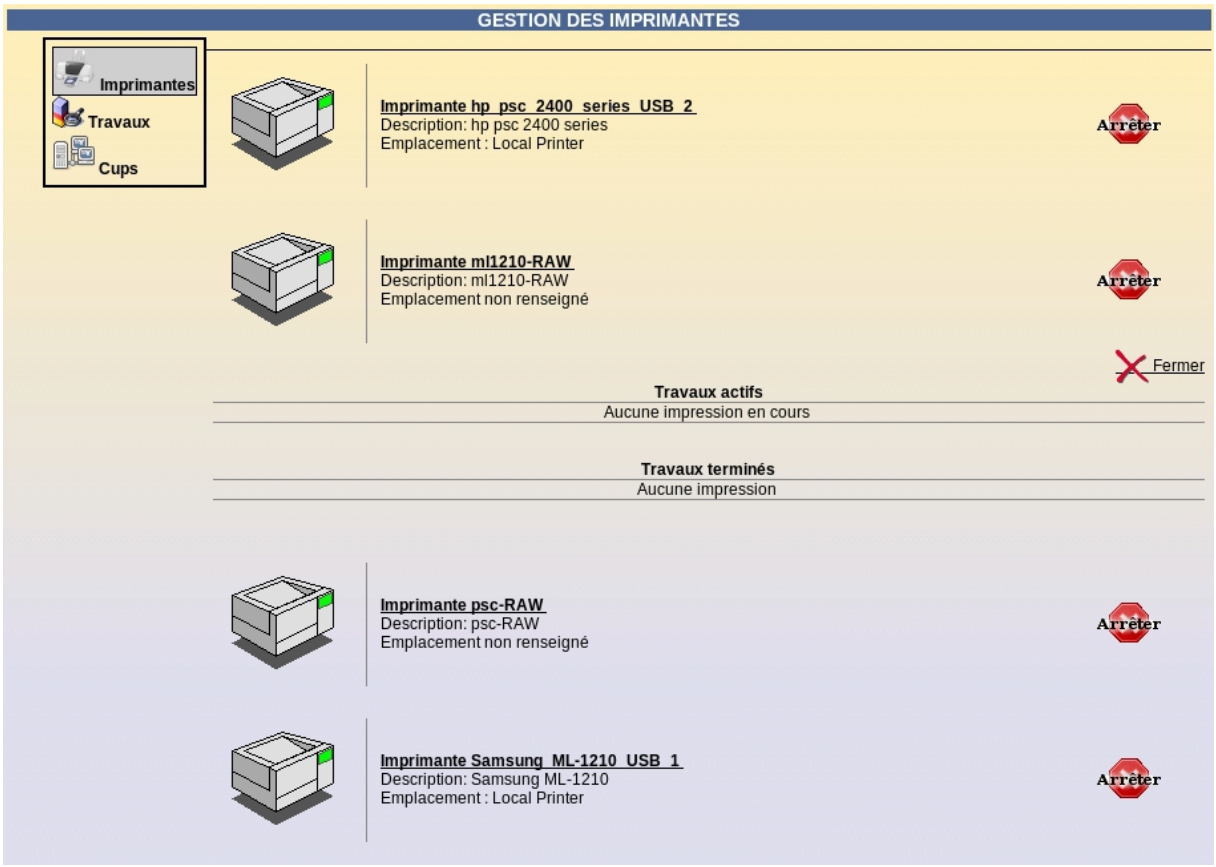
- l'interface simplifiée intégrée à l'EAD (gestion) ;
- l'interface de gestion CUPS (gestion et installation/configuration).

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.



2 L'interface de gestion CUPS

CUPS (Common UNIX Printing System) fournit une interface web pour faciliter l'installation et la gestion des imprimantes sur le serveur.

Cette interface est totalement accessible aux utilisateurs *root*, *<nom du module>*, *admin* et aux utilisateurs du goupe *PrintOperators*. Sur le module Scribe, elle est en accès restreint pour les professeurs, identique à celle proposées dans l'interface simplifiée de l'EAD.

CUPS est le serveur d'impression intégré à la solution EOLE.

Nous ne verrons ici que la partie serveur de la configuration des imprimantes.

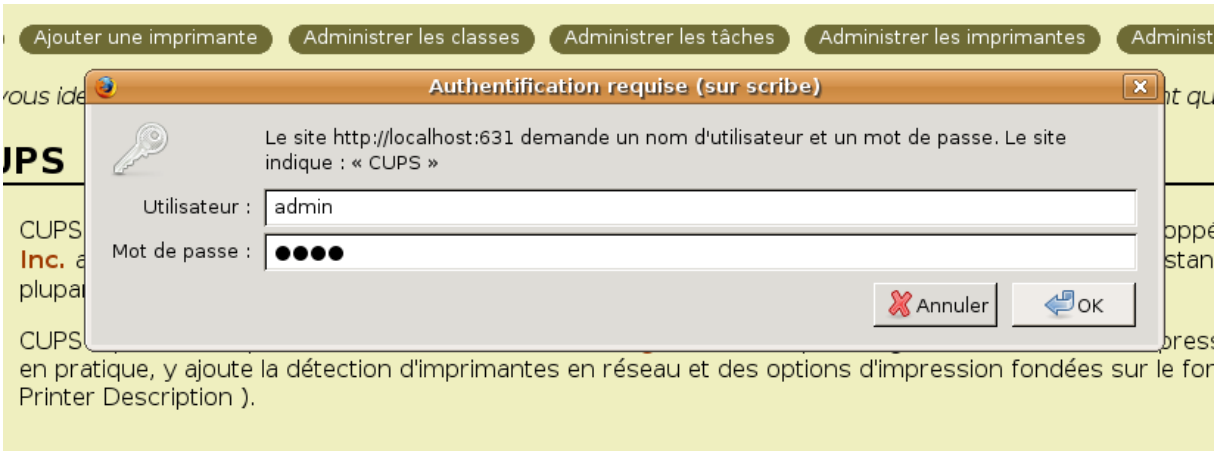
2.1. Création de l'imprimante

2.1.1. Ajouter une nouvelle imprimante

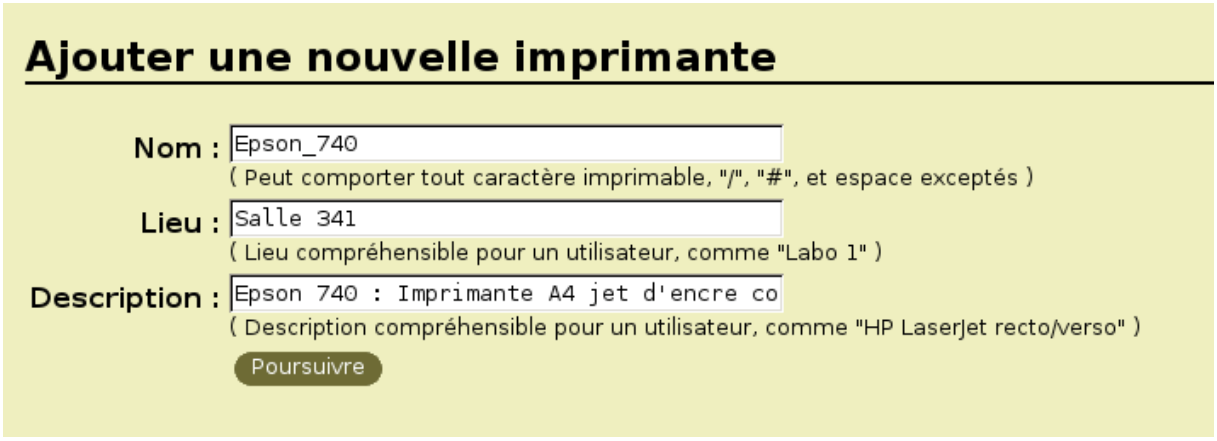
Dans l'EAD, le menu *Imprimantes/Imprimantes/CUPS* ouvre l'interface de configuration CUPS dans une nouvelle fenêtre.

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*.



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.



2.1.2. Choix du matériel

Il y a trois grands types d'imprimantes :

- les imprimantes locales (avec un port USB, parallèle, ...) ;

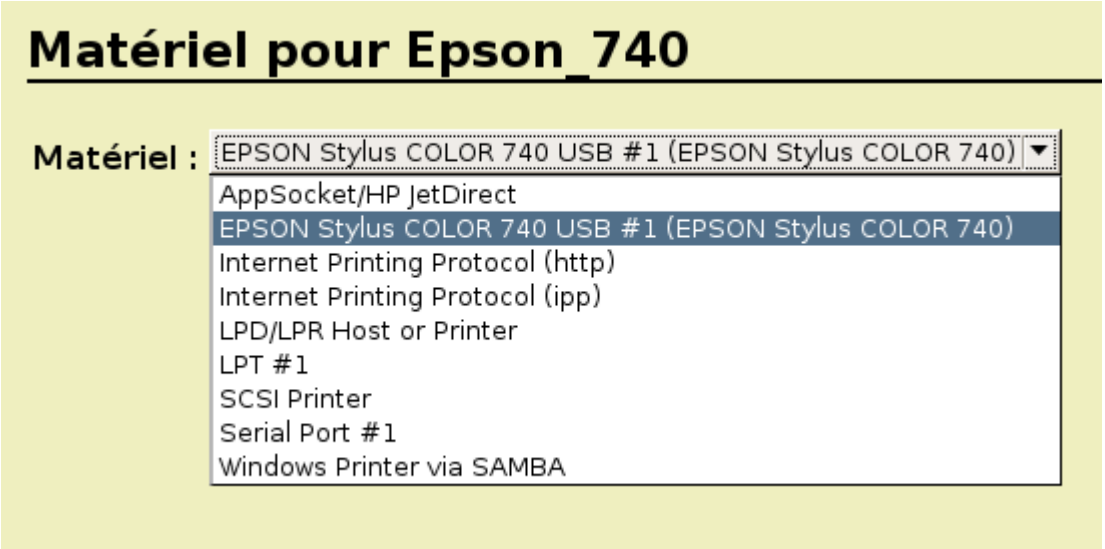
- les imprimantes réseaux ;

- les imprimantes partagées sur un poste client Windows.

i - 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.



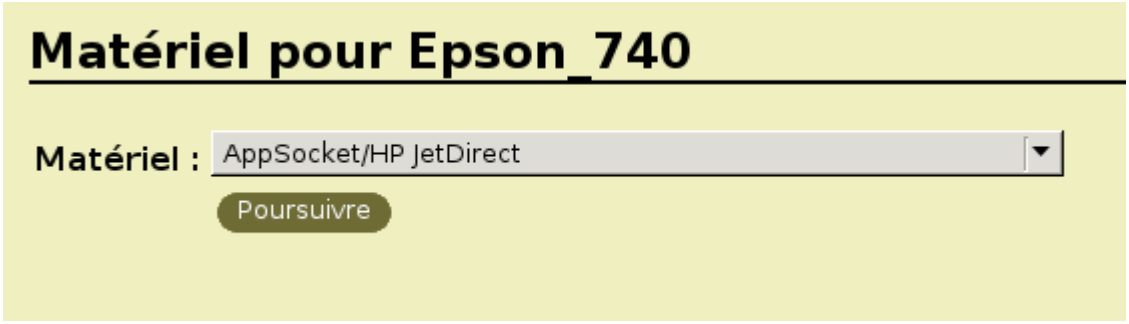
ii - Les imprimantes réseaux

Il existe un grand nombres de protocoles réseaux pour les imprimantes : AppSocket/HP JetDirect, Internet Printing Protocol (HTTP ou IPP). Généralement, les imprimantes réseaux sont capable de faire du JetDirect. En cas de doute, se reporter à la documentation de l'imprimante.

Imprimante compatible JetDirect

Choisir le matériel "*AppSocket/HP JetDirect*" et poursuivre. Indiquer ensuite une *URI du matériel* du type :

```
socket://192.168.230.123:9100
```



iii - Les imprimantes partagées sur un poste client Windows

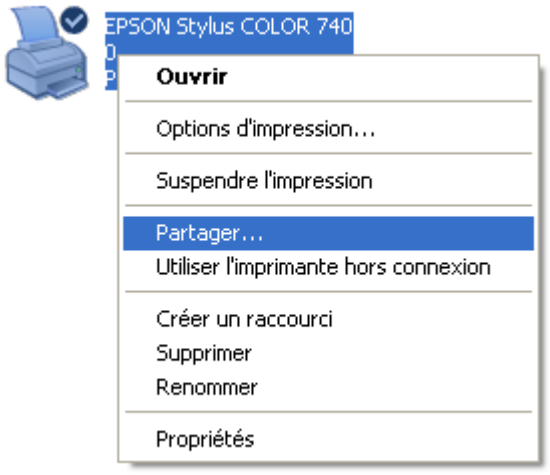
Création d'un partage d'imprimante sous Windows XP

Nous partons du principe que l'imprimante est fonctionnelle sur le système d'exploitation propriétaire Windows.

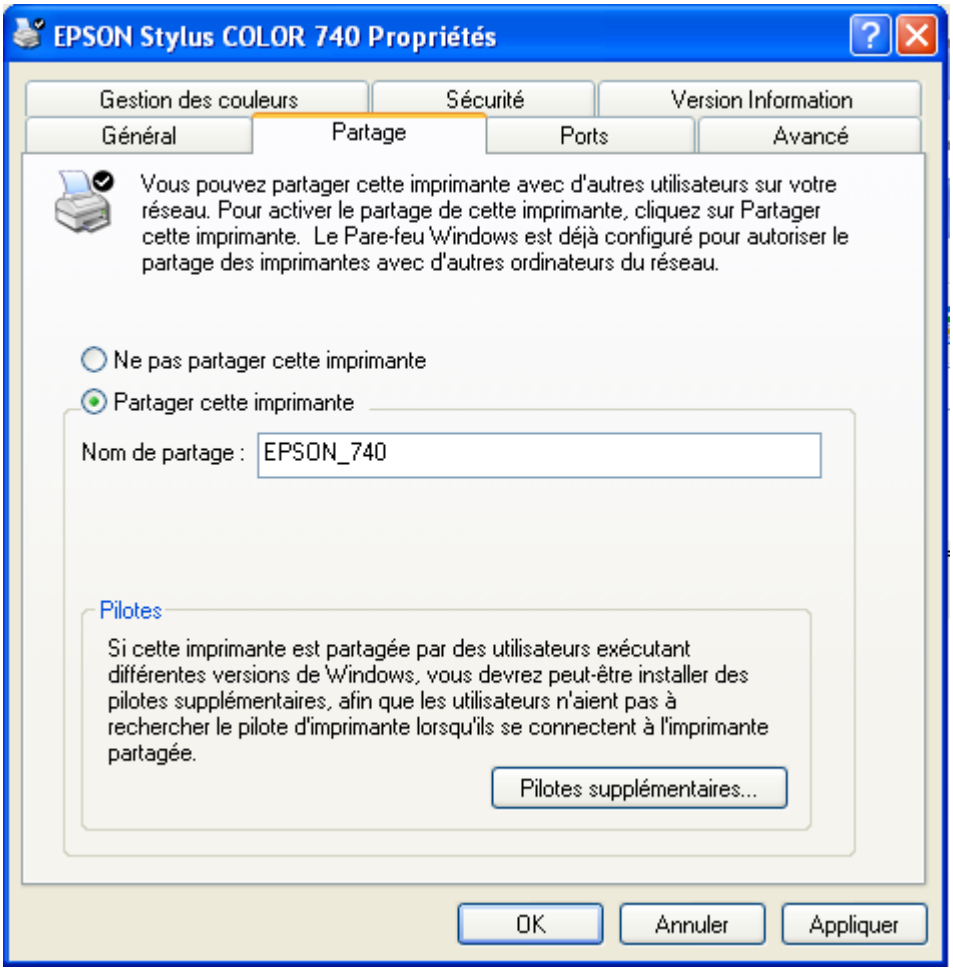
Remarque

Il est possible d'accéder directement à l'imprimante du poste sans passer par le serveur. Cette documentation ne traite pas de ce cas.

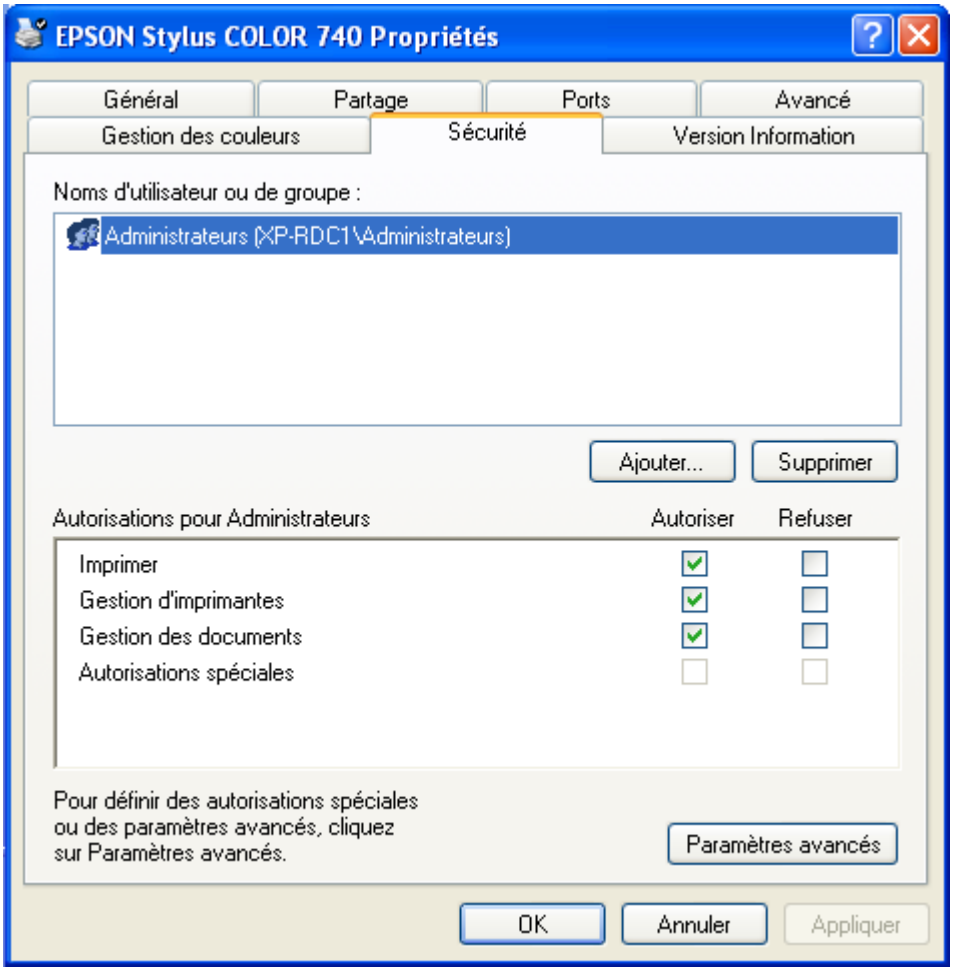
Dans le menu Windows *Démarrer/Imprimantes et télécopieurs* cliquer droit sur votre imprimante et choisir *Partager...*.



Il suffit alors de cocher *partager cette imprimante* et de donner un *Nom de partage*.



Enfin, dans l'onglet `Sécurité`, supprimer toutes les autorisations aux autres groupes et utilisateurs que *Administrateurs*. Ce groupe devant avoir toutes les autorisations.

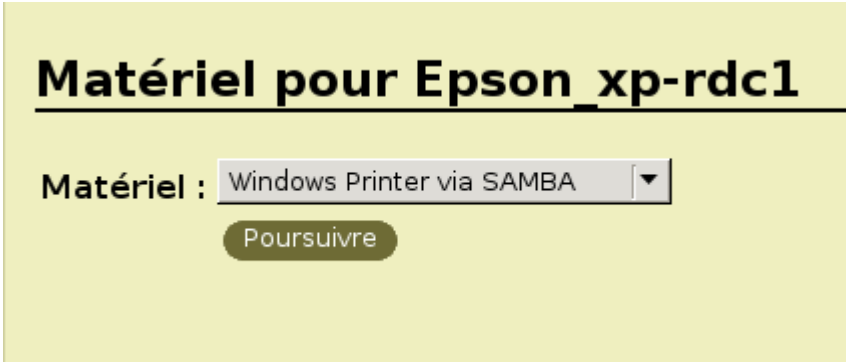


Configuration de CUPS

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
```



Remarque

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.

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.

2.2.1. 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.

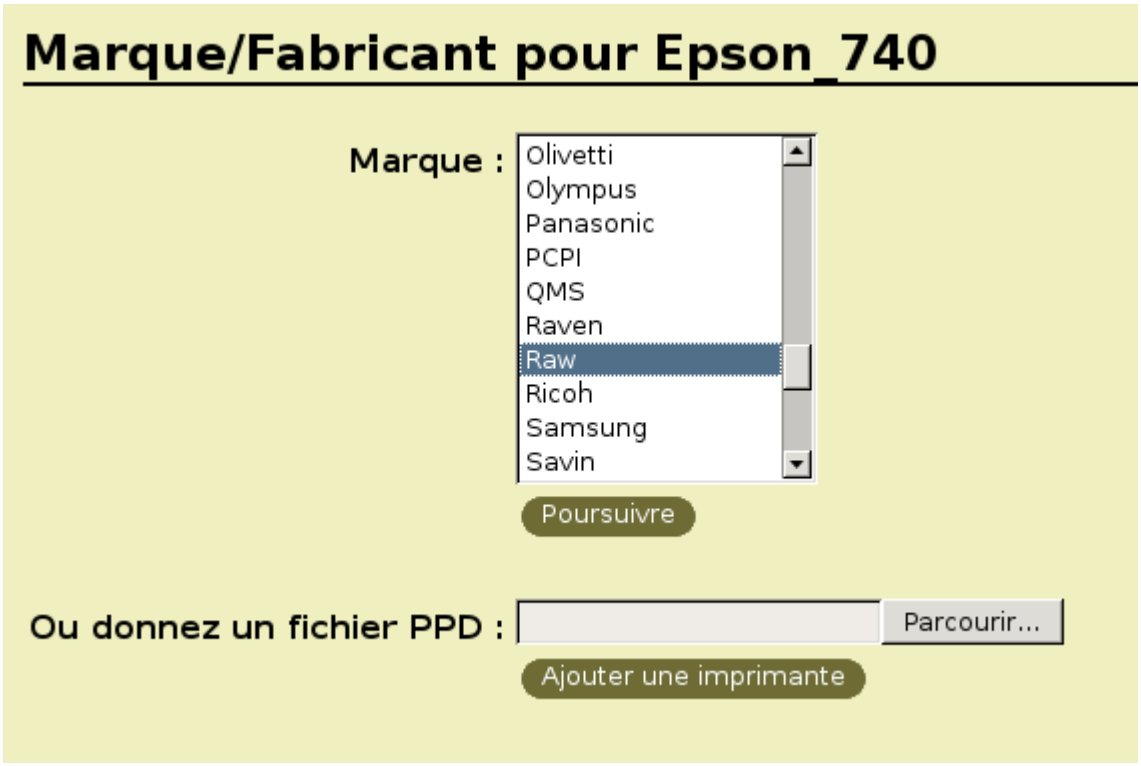
Le pilote CUPS est plus simple à mettre en place. Il est particulièrement adapté aux réseaux hétérogènes. Par contre, les pilotes ne sont souvent pas écrits directement par les constructeurs.

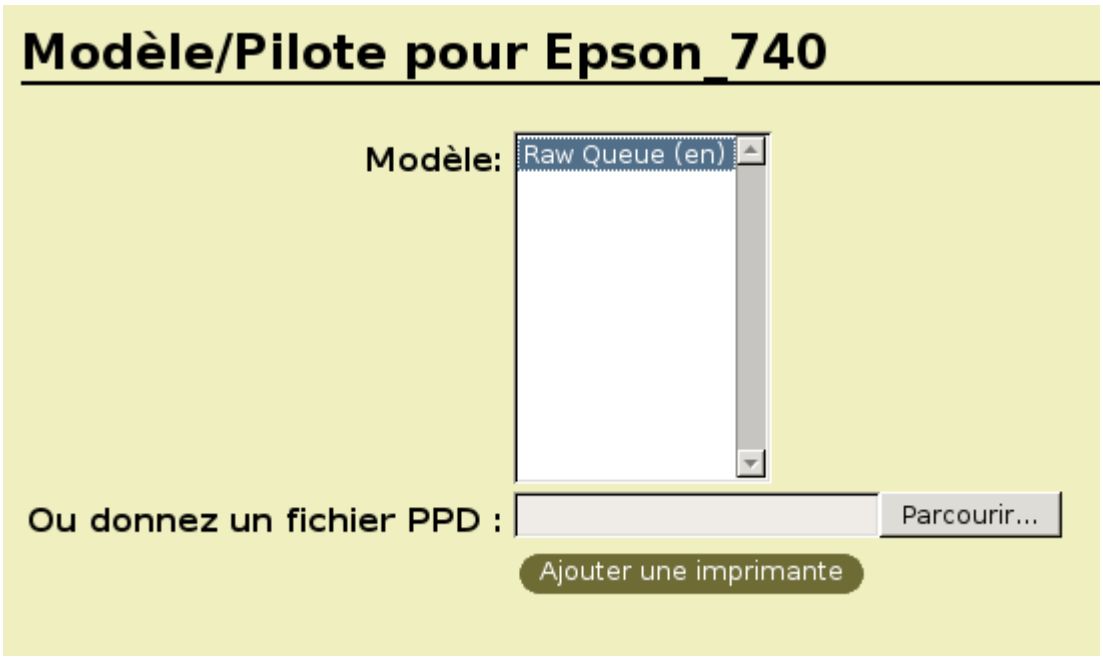
2.2.2. Utilisation des pilotes clients Windows

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.





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.

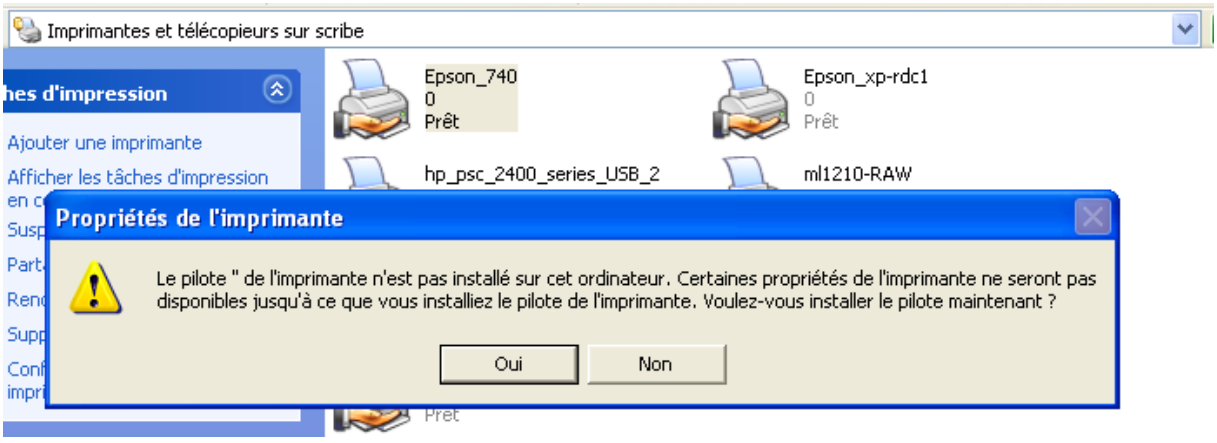
L'installation se fera depuis un poste client Windows intégré au domaine. Il faut se munir du pilote fourni par le constructeur de l'imprimante.

Il faut commencer par se connecter à un poste Windows en "*admin*" ou un utilisateur appartenant au groupe *PrintOperators*.

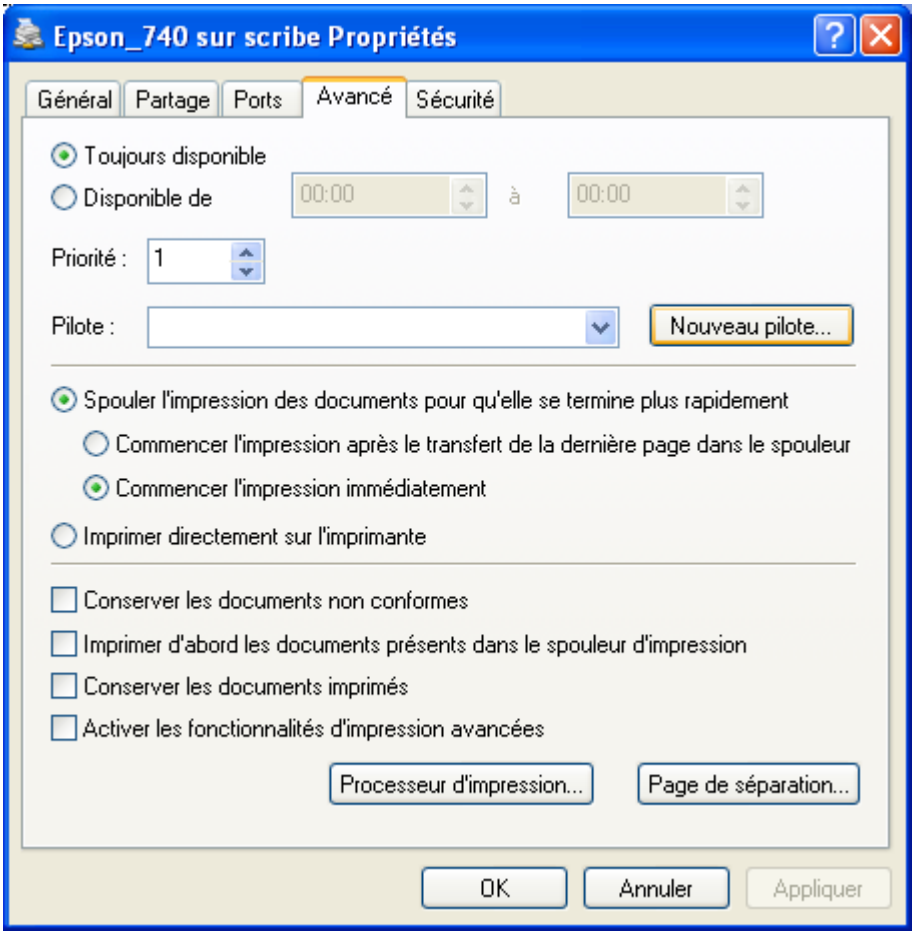
Ensuite, dans un navigateur de fichiers il faut se rendre sur le partage du serveur : `\\<nom du serveur>` puis choisir "*imprimantes et télécopieurs sur ...*".

Cliquer droit et choisir *propriétés*.

Répondre non à la question "*Voulez-vous installer le pilote maintenant*".



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*".



Attention

Il se peut que Windows change le nom de l'imprimante à cette étape. Vérifier que le nom correspondent à ce que vous souhaitez.

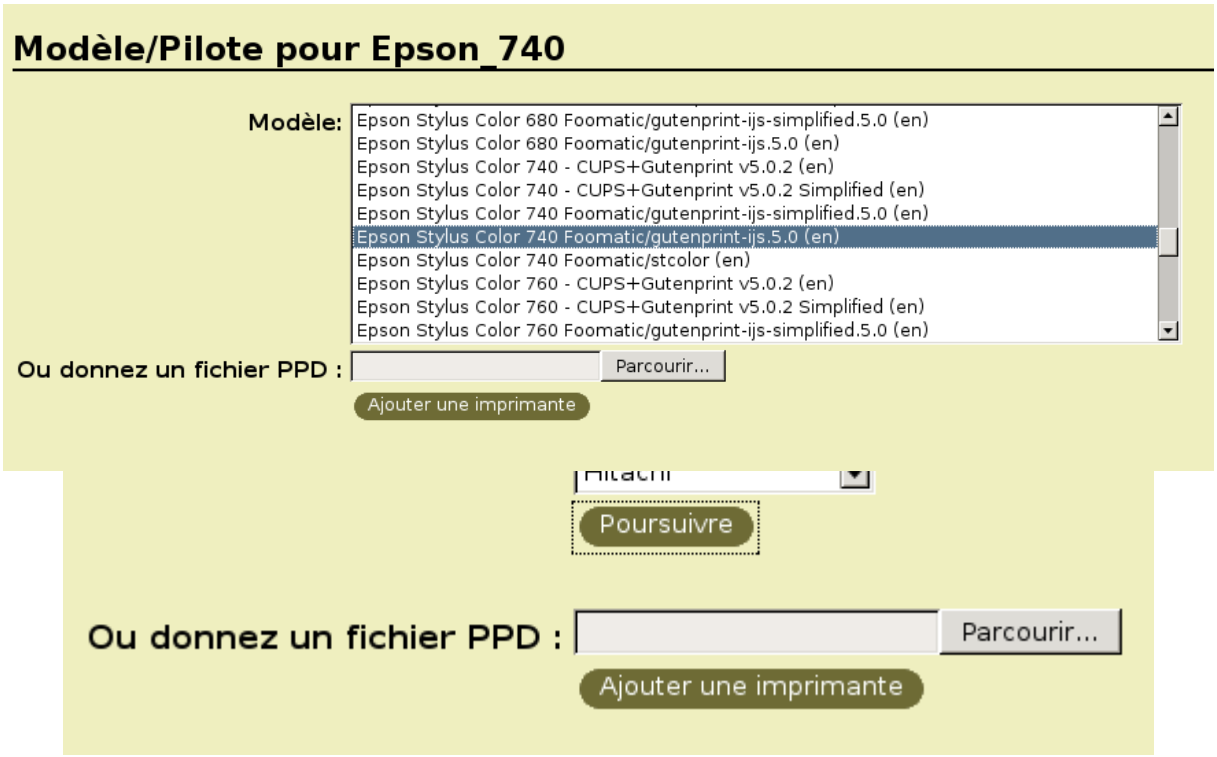
Remarque

Dans l'onglet "Partage" il est possible d'installer des "Pilotes supplémentaires..." pour les autres versions de Windows.

2.2.3. 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.



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 supérieurs ou égales à Windows 2000.

Si vous utilisez encore des versions de Windows inférieurs, il vous faudra, par exemple, les pilotes PostScript proposés par l'éditeur Adobe.

Il faut commencé par récupérer les pilotes PostScript Microsoft.

Les pilotes d'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.

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

3 Gestion des imprimantes sous Windows

Attention

Ceci ne concerne pas les postes Windows Millennium et inférieur et nécessite l'utilisation du logiciel 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.

4 Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse 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`

XVI 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

Complément

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

XVII Mise en place des sondes EQOS

EQoS permet à tout responsable, personnel de direction en établissement ou autorité académique, de mesurer la qualité de service de ses applications selon des critères objectifs.

Ces outils sont développés par pôle de Compétences Inter-Académique de Nancy-Metz (adresse à usage académique https://pole.in.ac-nancy-metz.fr).

Leur mise en place sur un module EOLE est simplifiée par la réalisation d'un paquet nommé `eole-eqos`, pour l'installer :

```
# Query-Auto
# apt-eole install eole-eqos
# reconfigure
```

Complément

Une documentation est disponible sur le site du pôle Compétences (adresse à usage académique) : https://pole.in.ac-nancy-metz.fr/wiki/EqosDispoInstallSonde

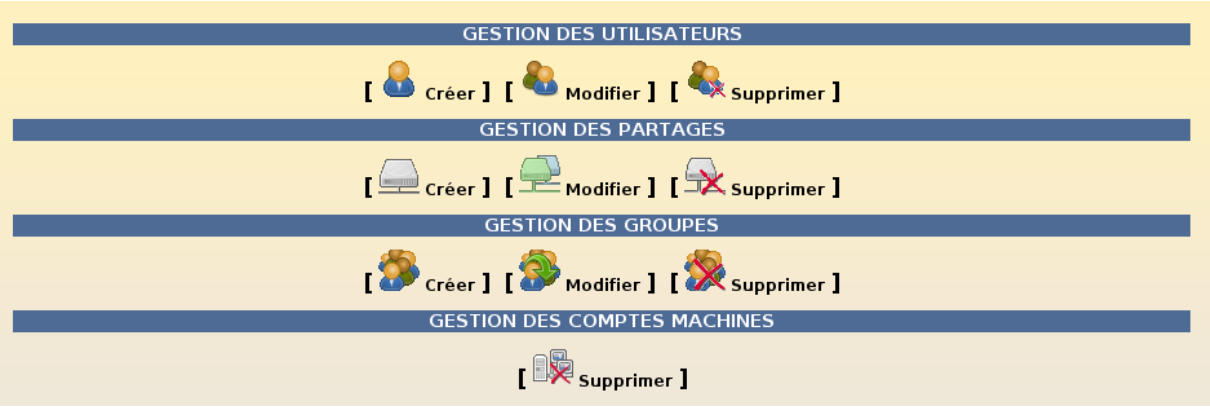
XVIII Fonctionnalités de l'EAD propres au module Horus

1 Groupes, utilisateurs et partages

Le menu Gestion est dédié à la gestion des utilisateurs, des groupes et des partages Horus.

Index

Le sous-menu *Index* présente sur une seule page des raccourcis vers toutes les actions possibles du menu Gestion.

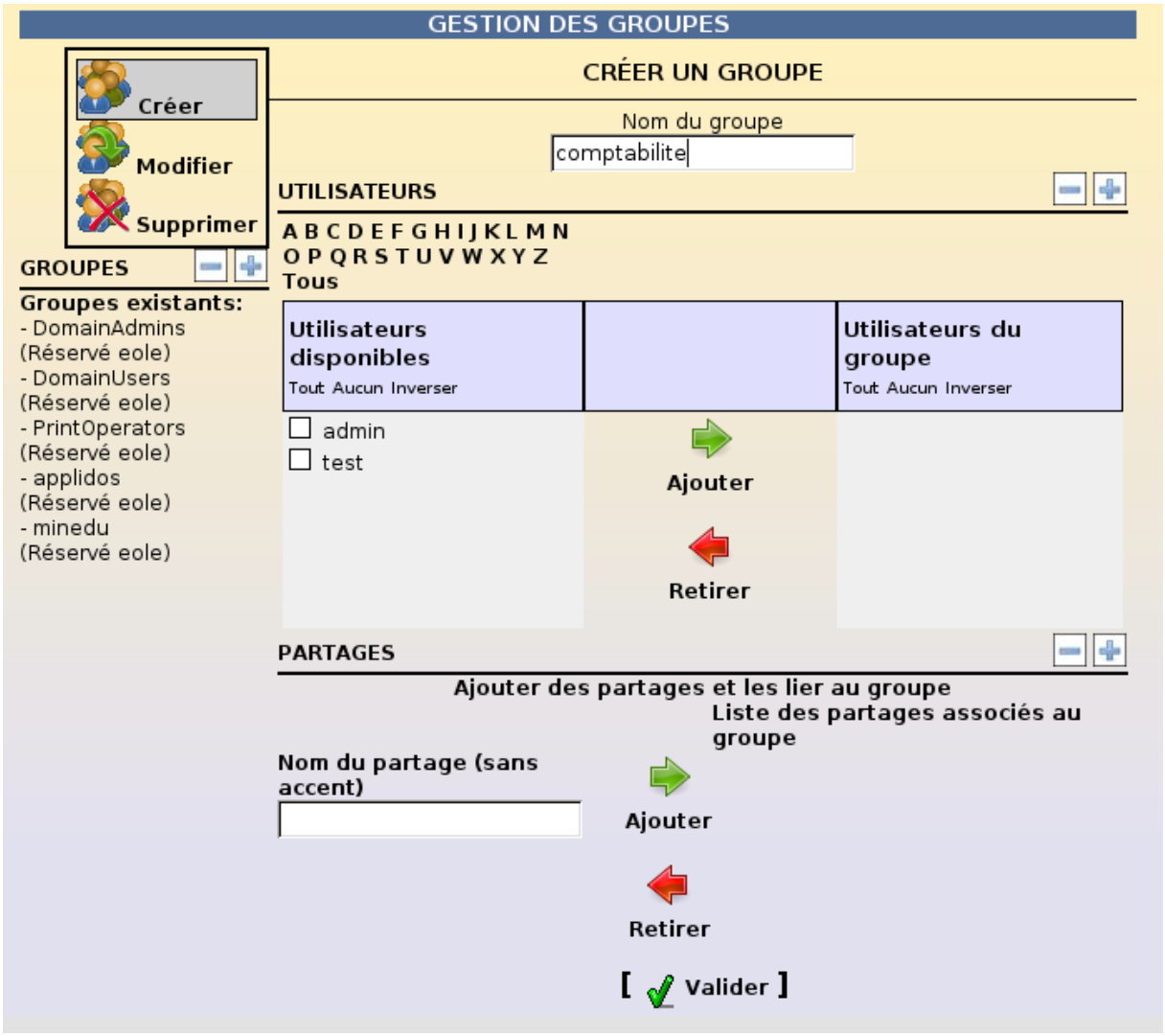


1.1. Groupes

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 :



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).

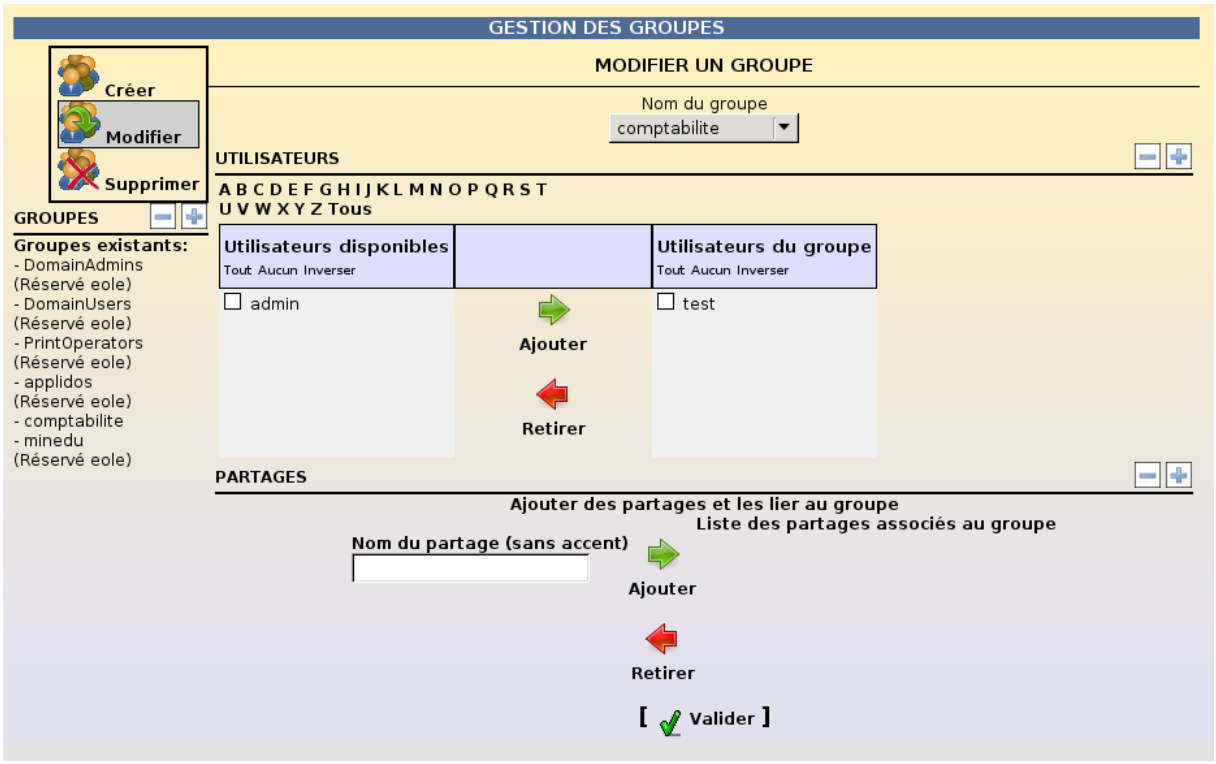
Il est enfin possible d'affecter un ou plusieurs nouveaux partages au groupe dès sa création (troisième bloc).

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.



Attention

Les groupes suivis de la mention `(Réservé EOLE)` sont des groupes spéciaux qu'il faut manipuler avec précaution.

Truc & astuce

Le fait de supprimer la liaison entre un partage et un groupe (ou de supprimer le groupe lui-même) entraine la suppression du partage dans l'annuaire mais pas celle de ses données.

Il est donc possible de les récupérer en créant un nouveau partage du même nom (ou un partage utilisant le même chemin).

Pour ce genre de manipulation, il est préférable d'utiliser les actions du sous-menu *Partages*.

Supprimer un groupe

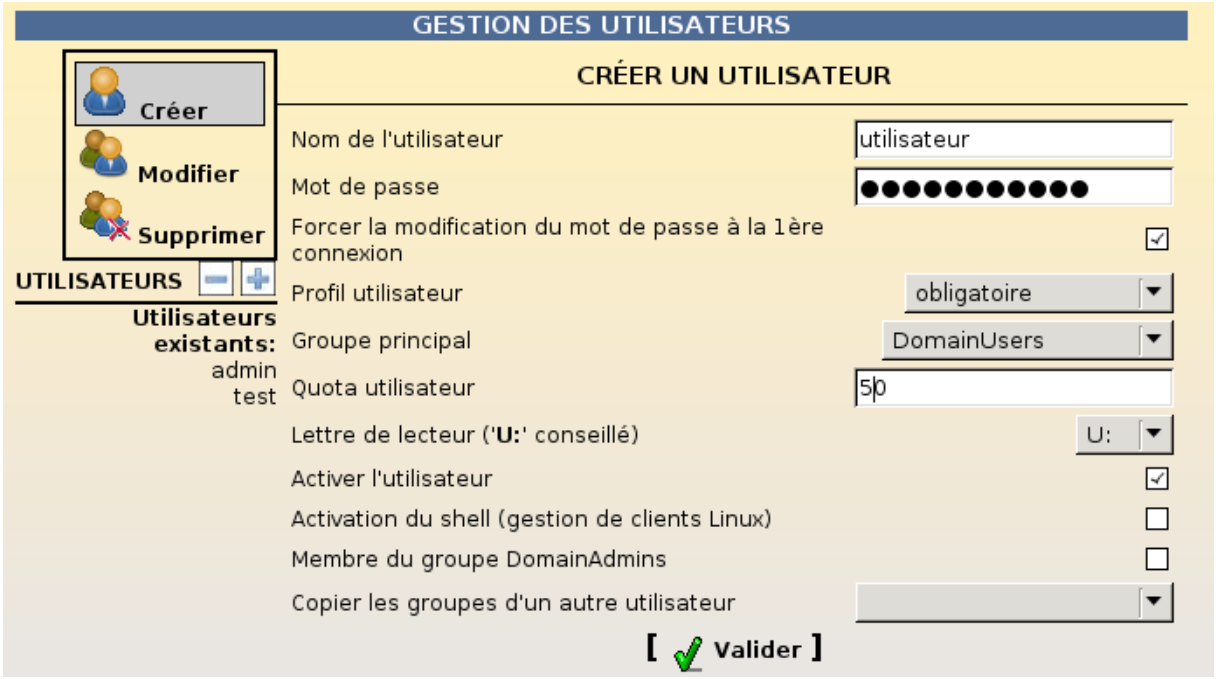
Une liste déroulante permet de sélectionner le groupe à supprimer.

Les groupes spéciaux ne sont pas supprimables et n'apparaissent pas dans cette liste.

1.2. Utilisateurs

Le sous-menu *Utilisateurs* permet de créer, modifier et supprimer les utilisateurs Horus.

Le formulaire de création d'utilisateur Horus est assez simple.



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).

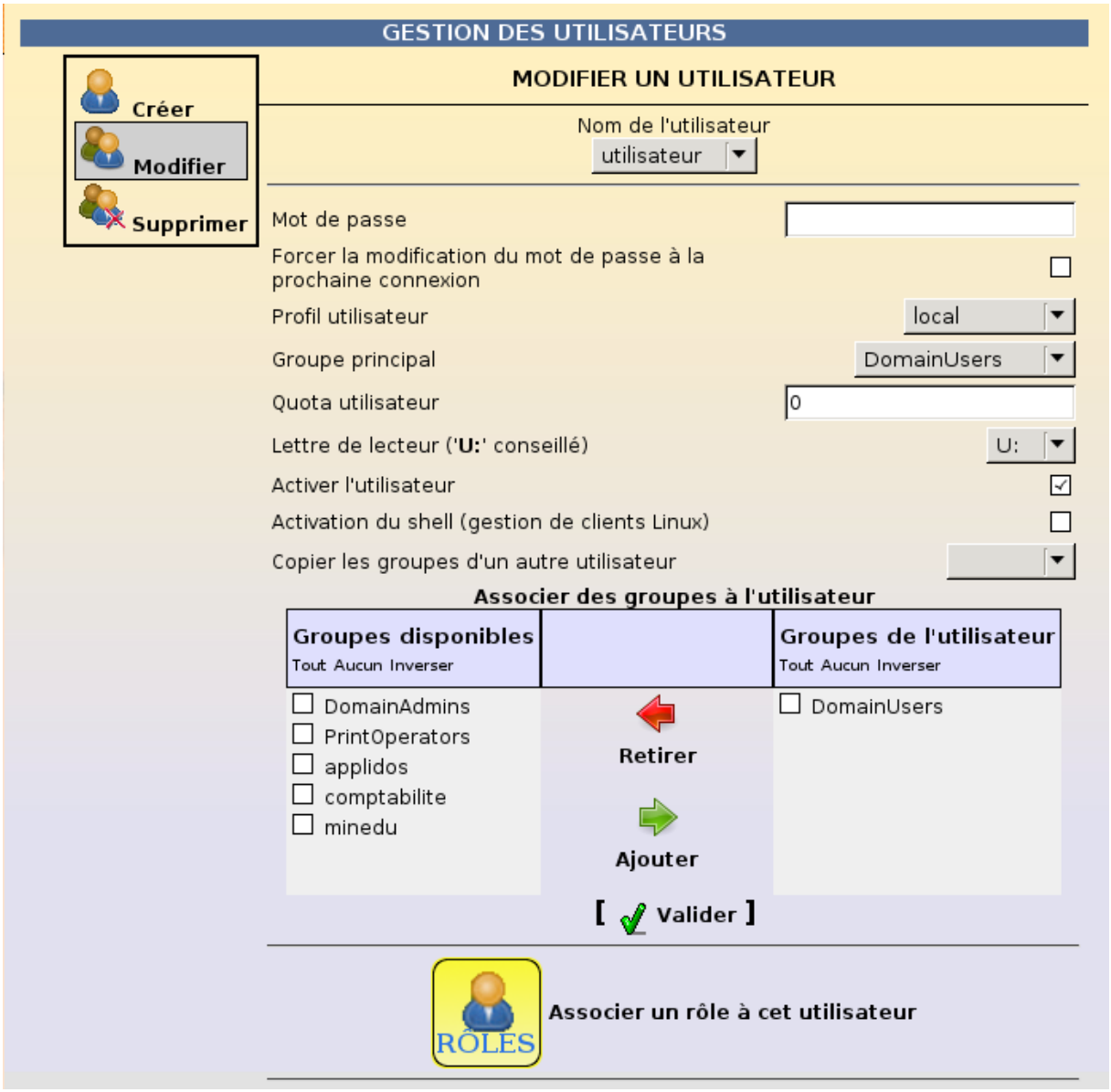
Modifier un utilisateur

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`).



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.

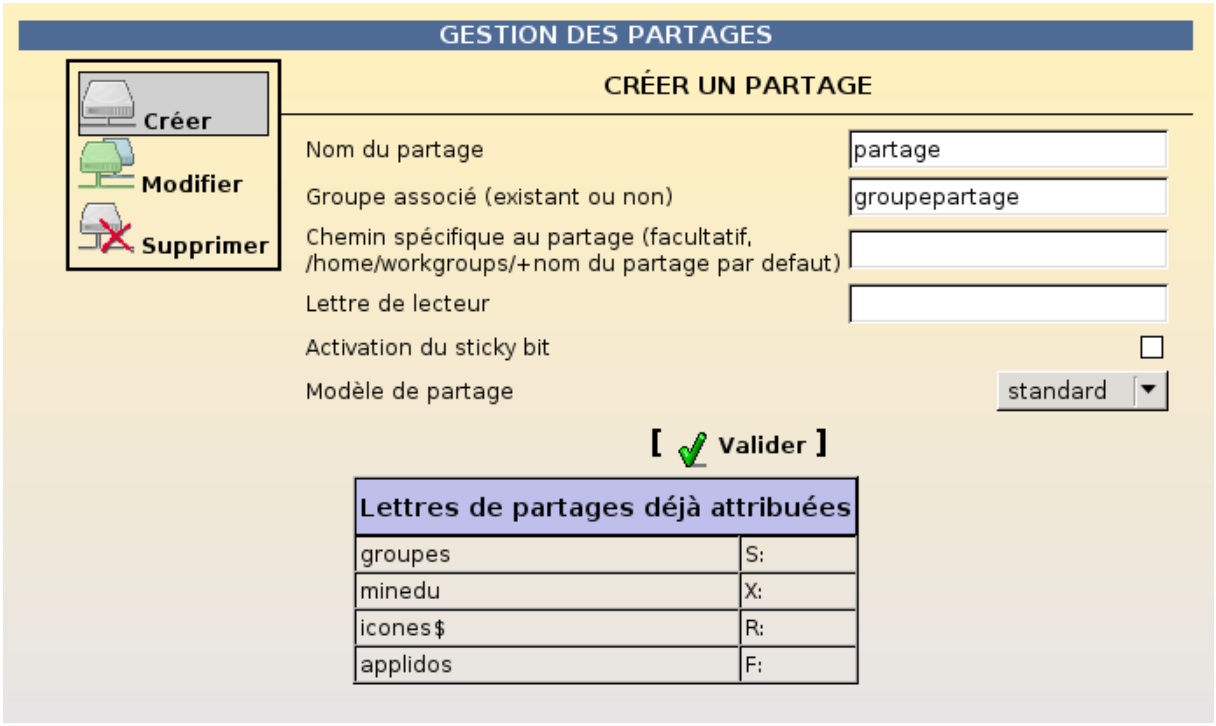
Vous pouvez choisir de conserver ou de supprimer le répertoire personnel (fichiers et répertoires) de l'utilisateur.

1.3. 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.



Pour créer un partage, seuls les *Nom du partage* et nom du *Groupe associé* sont requis.

Si le groupe associé au partage n'existe pas, il sera créé avec les paramètres par défaut.

Il est également possible de préciser :

- le chemin du partage sur le serveur Horus (par défaut : **/home/workgroups/<partage>**) ;
- une lettre de lecteur à associer à ce partage (exemple : `L :`) ;
- si le *sticky bit* doit être activé sur le partage (seul le propriétaire du fichier pourra effacer ces fichiers) ;

- le modèle de partage à utiliser pour générer la section associée au partage dans la configuration Samba.

activation du sticky bit

Le "sticky bit" était nécessaire au fonctionnement de certaines applications mais il ne devrait plus être utilisé.

Les modèles de partage

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

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

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

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.

Vous pouvez choisir de conserver ou de supprimer les données (répertoire) du partage .

2 Machines

Machines

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.

Truc & astuce

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.

3 Les ACLs

Des ACLs* sont utilisées sur le système de fichiers pour permettre un réglage fin des droits d'accès aux partages et à leur contenu.

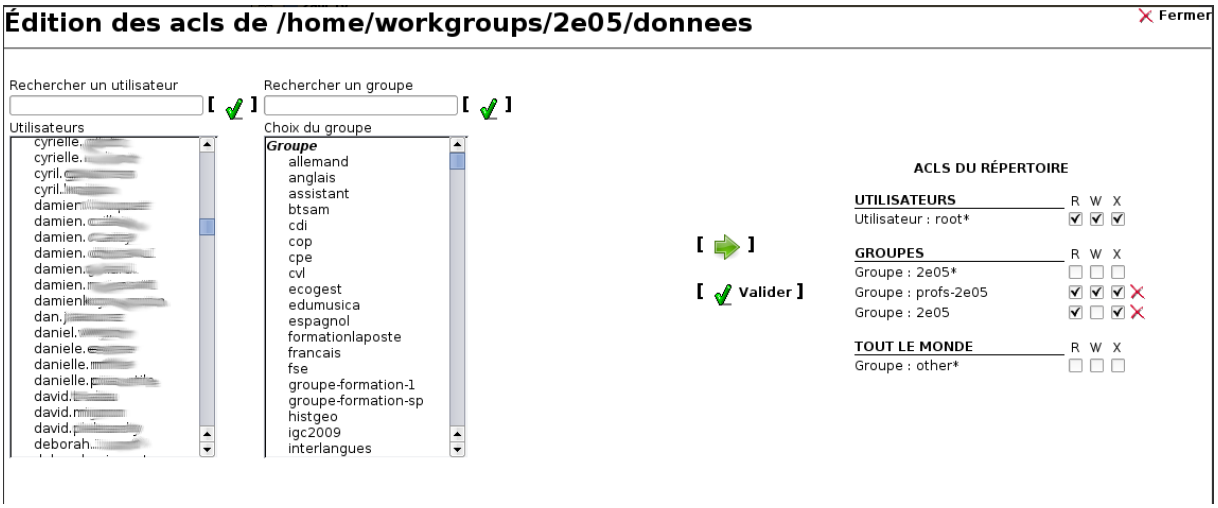
Modification des ACL sous Windows

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* (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.

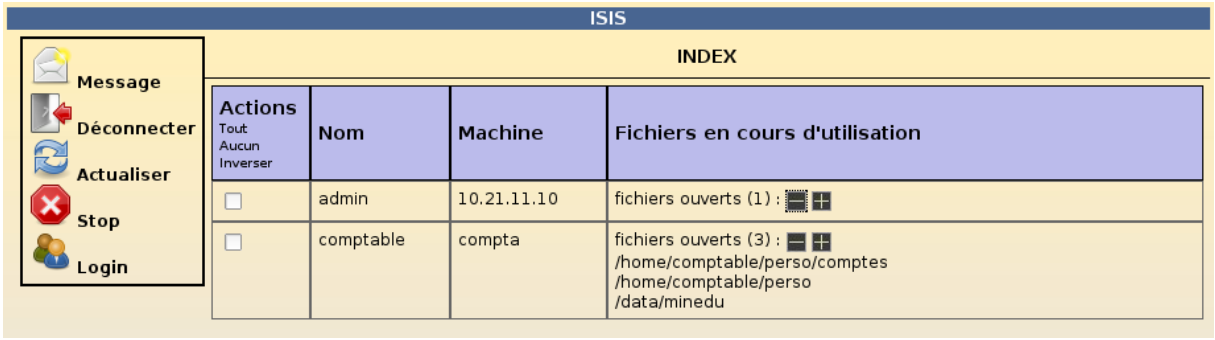


Le caractère "*"

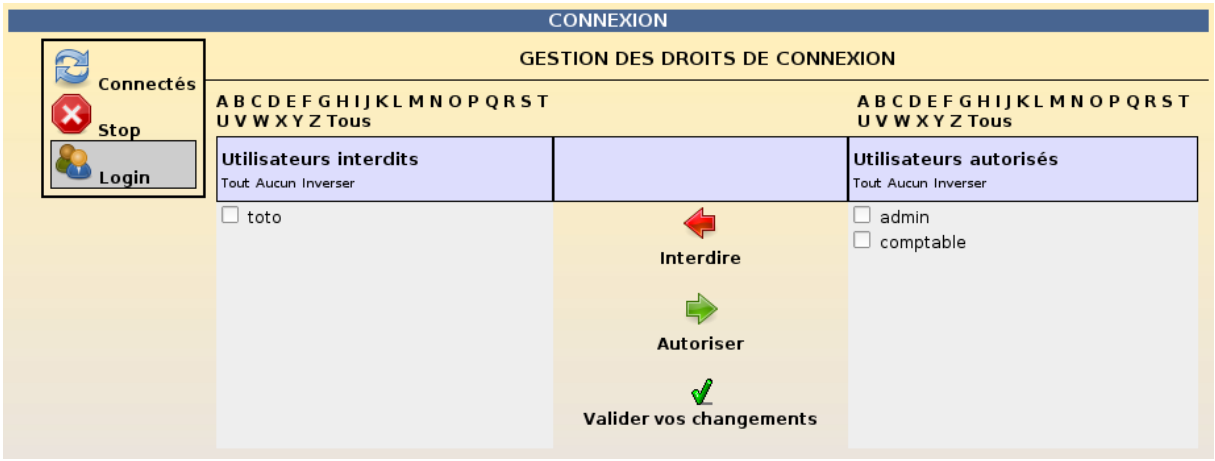
L'étoile indique que l'utilisateur ou le groupe en question est propriétaire du fichier ou du répertoire au niveau des droits Unix.

4 Connexion

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.



- 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 :



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.

5 Machines du réseau

Le sous-menu *Machines du réseau* permet d'afficher les stations actives du réseau selon certains critères.

Les critères proposés sont :

- *Toutes les stations* : les stations sur le même sous-réseau que l'Horus et ayant un service partage de fichiers actif
- *Maîtres explorateurs* : les machines possédant l'attribut *__MSBROWSE__*
- *Contrôleur de domaine* : les serveur SMB/CIFS ayant l'attribut *1B*

6 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.

Remarque

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.

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

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.

Truc & astuce

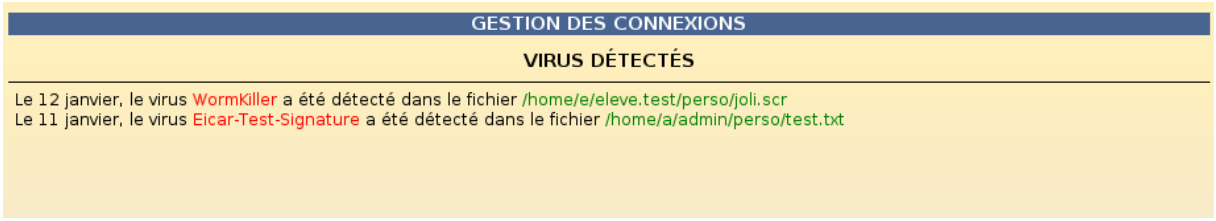
Pour le module Horus, il faut remplacer `/home` par `/data`.

7 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.



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.

Remarque

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**

8 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).

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.

Truc & astuce

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=`

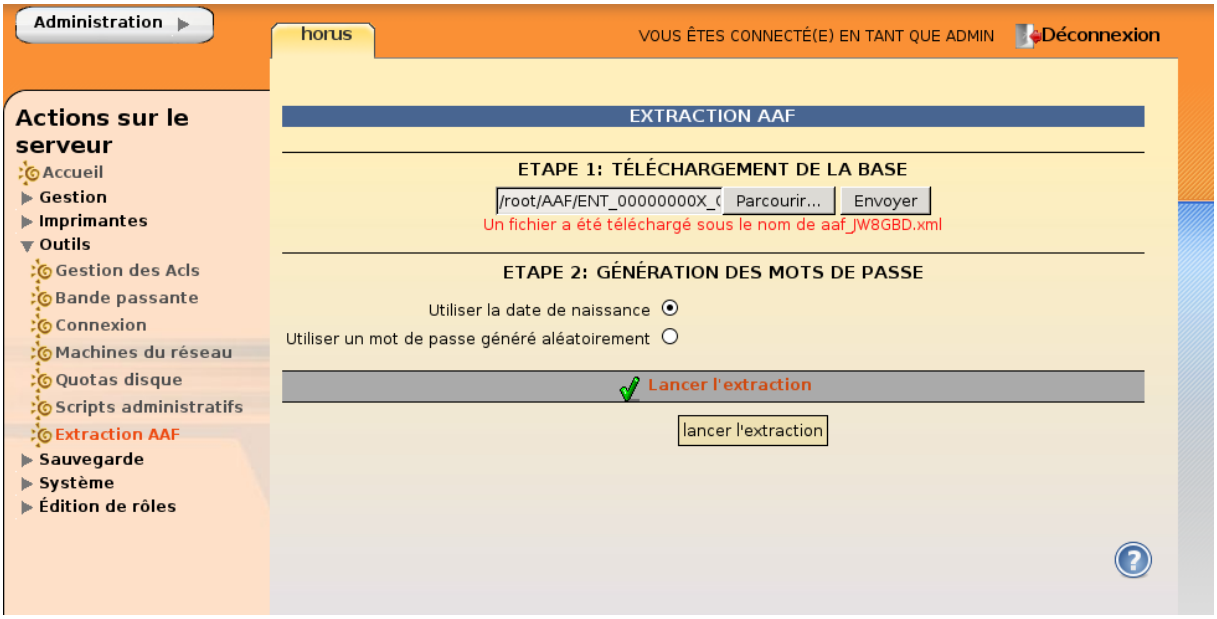
9 Extraction AAF

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



Attention

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,...).

Attention

Dans la version actuelle du programme, les mots de passe attribués aux nouveaux utilisateurs sont stockés dans le fichier **/tmp/passwords.csv** .

10 Réservation d'adresse 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.

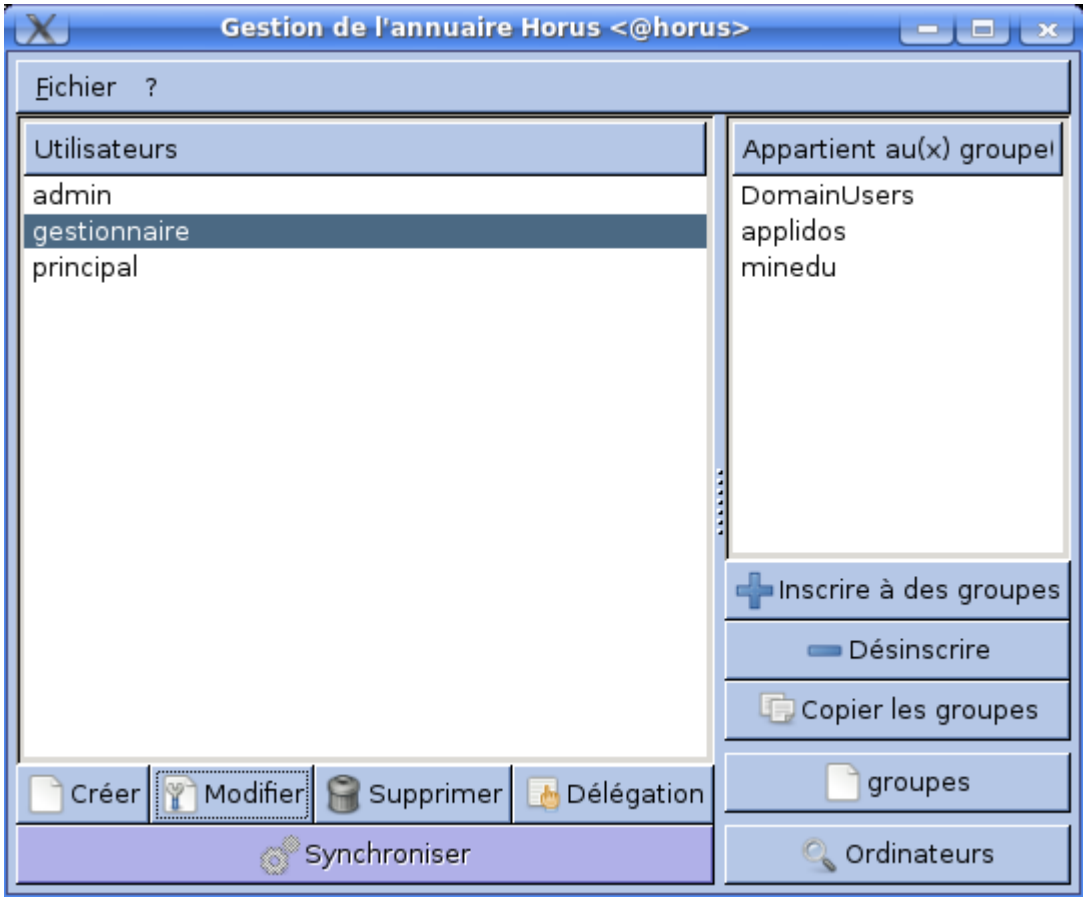
Pour associer un nom et une adresse IP à une machine, il faut connaître son adresse MAC.

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`*.

XIX Frontend Horus

L'outil `frontend-horus` est une interface graphique GTK permettant de gérer facilement les utilisateurs, les groupes et les partages d'un serveur 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 attribuée

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 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`

Serveur

La partie serveur est installée sur Horus.

Le client ne peut être utilisé que si le serveur est activé.

Son activation est possible via l'interface [gen_config], dans l'onglet Services, répondre "oui" à la question : *Activation du service horus_frontend*.

Le client et le serveur utilisent le port 7080 pour communiquer.

Truc & astuce

L'état d'activation du serveur associé à l'outil `frontend-horus` est disponible par la commande [diagnose].

Client Linux

Le client **/usr/bin/frontend_horus** est préinstallé sur le serveur Horus (paquet frontend-horus).

Il peut évidemment être installé sur une autre machine.

Le client Linux est téléchargeable sur notre site ftp à l'adresse :

ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-ng.tar.gz

Il suffit ensuite de le dépaqueter :

```
tar xvzf frontend-horus-ng.tar.gz
```

puis, pour le lancer :

```
cd frontend-horus
```

```
./frontend.py
```

Remarque

L'application requiert que python, python-gtk2 et python-glade2 soient installés sur la machine.

Truc & astuce

Des scripts proposant des fonctionnalités équivalentes sont disponibles dans le répertoire **/usr/share/eole/backend**.

Client Windows

Le client Windows est téléchargeable sur notre site ftp à l'adresse :

ftp://eoleng.ac-dijon.fr/pub/Outils/Horus/frontend-horus-setup.exe

XX Les différents clients Horus

1 Installation et configuration des clients Windows

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.

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).

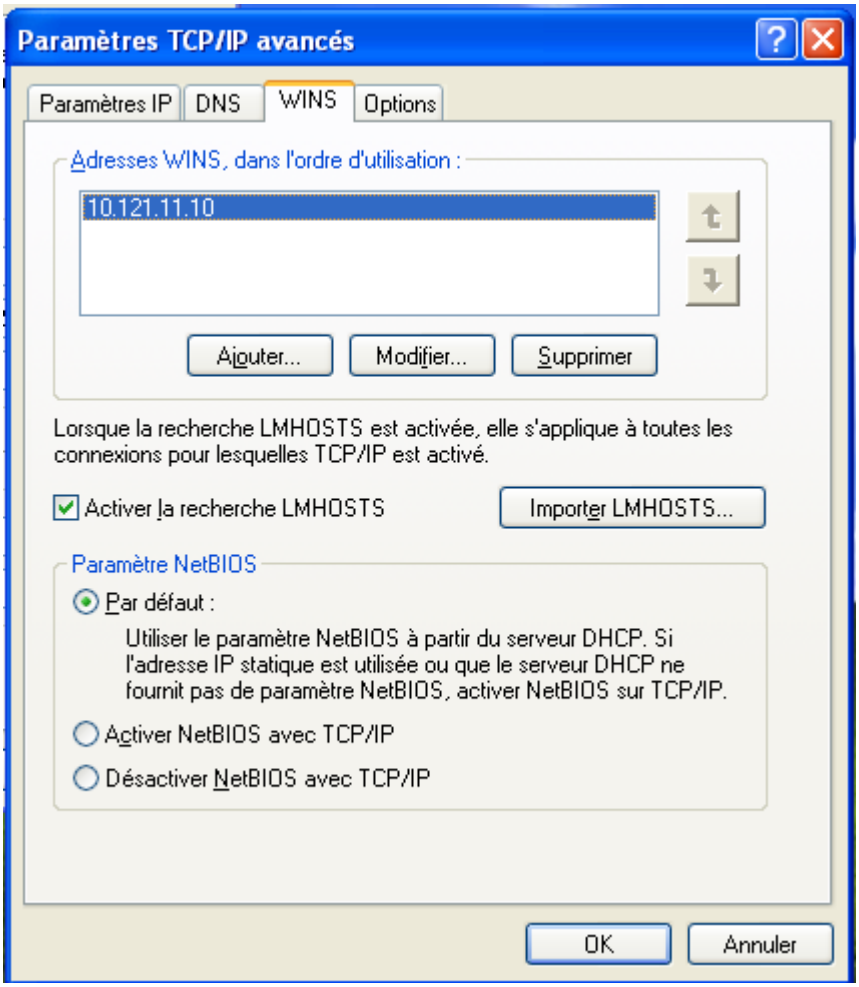
Plusieurs cas sont possibles :

- 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* ;

- 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*.

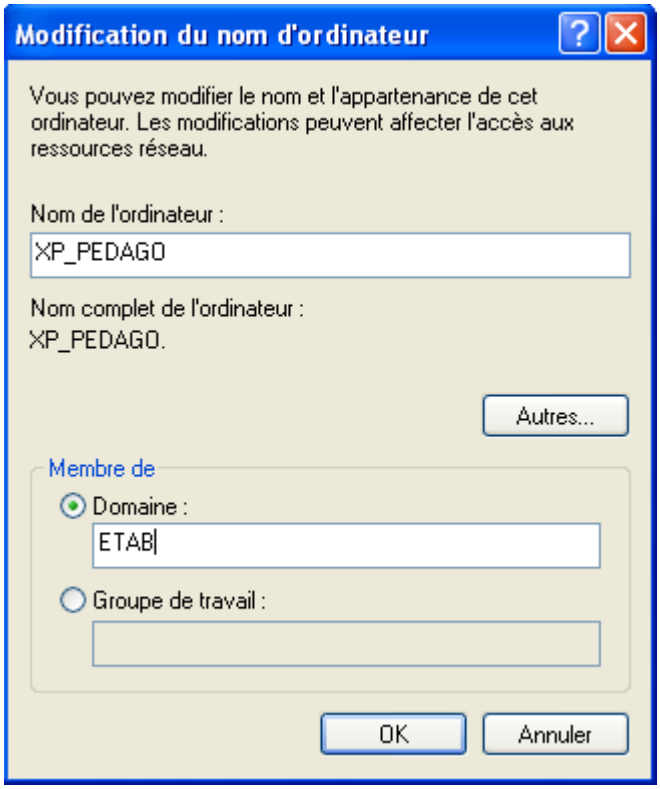


Intégration au domaine

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.



Particularité de Windows 7

L'intégration au domaine d'une station Windows 7 nécessite l'application préalable des clés de registre suivantes :

```
HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
DWORD DomainCompatibilityMode = 1
DWORD DNSNameResolutionRequired = 0
```

Le fichier *reg* nécessaire est mis à disposition dans :

/home/esu/Console/Win7_Samba3DomainMember.reg

2 Administration des clients Windows

2.1. Scripts personnalisés

Lorsqu'un utilisateur ouvre une session Windows sur le domaine Horus, le serveur génère un fichier `\\horus\netlogon\<login>.bat`

Ceci est réalisé par l'intermédiaire du programme **/usr/share/eole/fichier/dyn-logon.py** qui génère le script `<login>.bat` en fonction de l'utilisateur, de ses groupes d'appartenance et du système d'exploitation de la station cliente (Win9X, Win2K, WinXP, Vista).

Par défaut, sur le module Horus, seul les lecteurs réseaux des partages de l'utilisateur sont montés par ce script.

Pour ajouter des instructions au fichier `<login>.bat`, il est possible d'utiliser des scripts personnalisés pour :

- un utilisateur particulier : **\\horus\netlogon\users\<login>.bat**
- une machine particulière : **\\horus\netlogon\machines\<machine>.bat**
- un groupe particulier : **\\horus\netlogon\groups\<group>.bat**
- un système d'exploitation particulier : **\\horus\netlogon\os\<os>.bat**
- un groupe et un système d'exploitation : **\\horus\netlogon\os\<os>\<group>.bat**
- un utilisateur et un système d'exploitation : **\\horus\netlogon\os\<os>\<login>.bat**

Le contenu de ces fichiers sera ajouté au fichier **\\horus\netlogon\<login>.bat**

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

Truc & astuce

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`

Attention

- 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.

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.

Truc & astuce

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.

2.2.1. 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.

Remarque

Ces préconisations peuvent être adaptée suivant votre expérience et vos besoins.

Ajout d'un utilisateur spécifique

Il est conseillé d'utiliser un utilisateur fictif pour créer le profil obligatoire.

Cet utilisateur doit être configuré avec un **profil local** et être membre du groupe **DomainAdmins**.

C'est l'utilisateur spécifique **admin.profil** qui sera utilisé pour la suite.

Préparation de la station

Nettoyage de la station

Si des profils autre que locaux (exceptés les profils admin et admin.profil) sont déjà présents sur la machine, il est préférable de les supprimer.

Afin d'éviter des effets de bords, n'installer que les logiciels nécessaires à la génération du profil.

Il arrive que certains logiciels mal programmés paramètrent des valeurs qui provoquent une erreur lorsque le profil est appliqué sur une station où le logiciel n'est pas installé.

Installation des programmes à pré-paramétrer dans le profil obligatoire

Toutes les applications n'ont pas forcément besoin d'être paramétrées dans le profil obligatoire. Il peut arriver que certaines applications n'apprécient pas ce mode de fonctionnement. Il est nécessaire de faire des tests pour en déterminer la liste.

Truc & astuce

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.) ;
- 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 mode **`Détails`**.

La validation d'une licence

Par exemple le logiciel privateur Acrobat Reader demande, lors de son premier lancement, de valider sa licence.

Cette question est posée une fois par session à un utilisateur avec **`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.*

Remarque

Ce type de comportement (validation, paramètres non retenus d'une session à l'autre) est généralement lié au profil obligatoire. Les informations sont enregistrées dans une partie du profil fourni par le profil obligatoire.

Ceci est à opposer aux informations stockées dans le répertoire **Applications Data** redirigé par défaut par ESU dans le répertoire **U:\.Config\Applications Data**.

Ces dernières informations sont donc retrouvées lors de la prochaine ouverture de session. Par exemple, LibreOffice enregistre la validation de sa licence une fois pour toutes.

Le fond d'écran bénéficie d'une gestion particulière dans ESU :

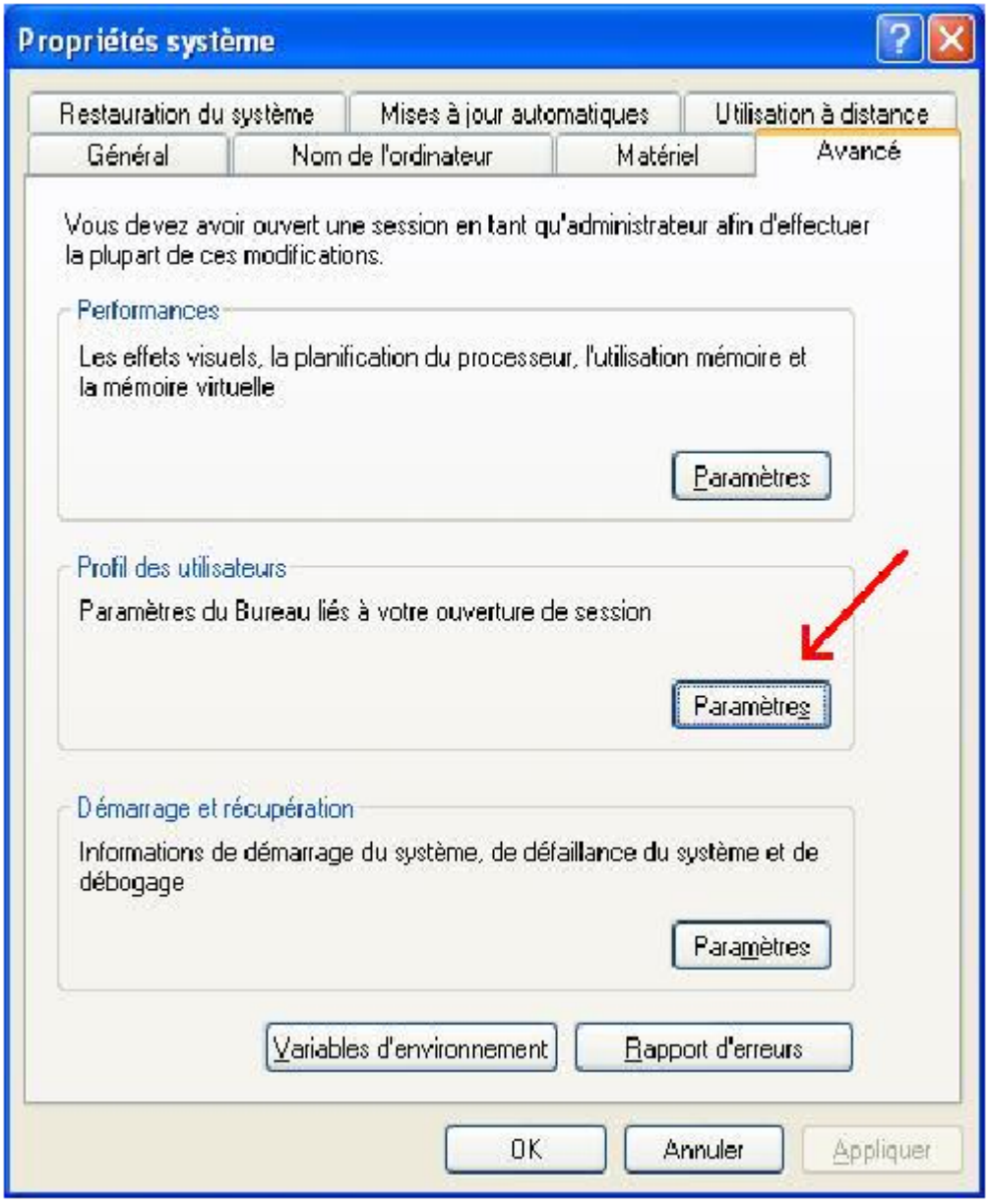
- la spécification d'un fichier image à afficher
- l'ajout d'informations textuelles en haut à droite.

Les deux étant incompatibles, il vaut mieux le désactiver pour éviter tout effet de bord. Pour se faire sélectionner *Aucun* dans *Propriétés de l'affichage/Bureau/Arrière-plan*.

Copie du profil

Ouvrir une session avec l'utilisateur **admin**. Aller dans le *Panneau de configuration* → *Système* → *Propriétés* → *Avancé*. Dans le cadre **Profil des utilisateurs** cliquer sur Paramètres.

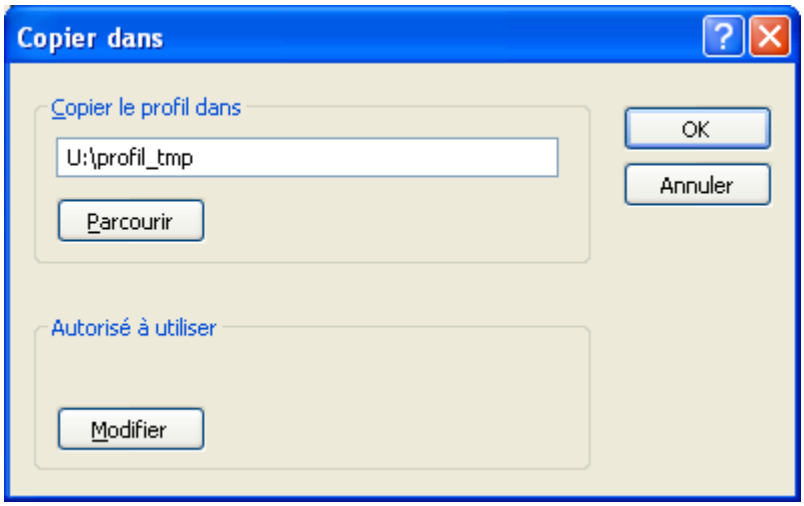
Dans la nouvelle fenêtre, sélectionner le profil correspondant à l'utilisateur **admin.profil**.



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).

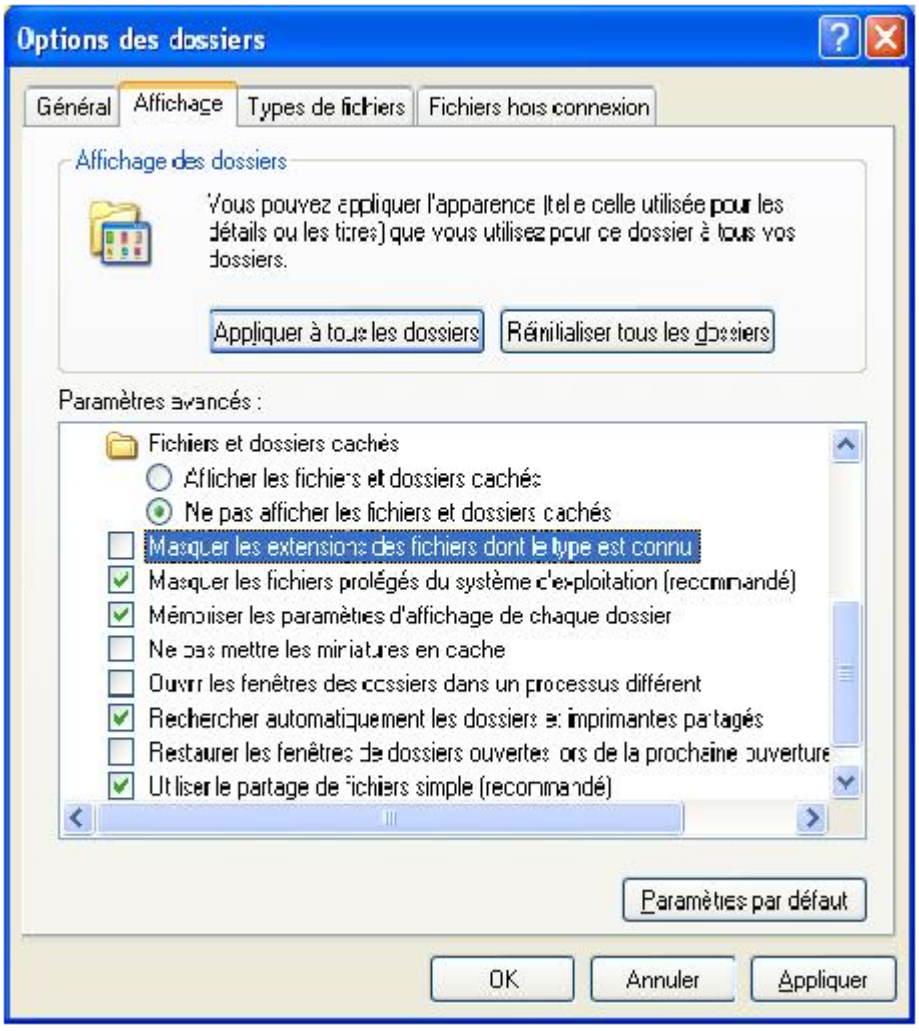
Remarque

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.

Truc & astuce

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.

2.2.2. 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`.

- http://www.yamprod.net/index.php?tag/Windows%207%20Seven%20profil%20copy%20copie%20profile%20microsoft%20default%20user%20enabler%20Copier%20dans
- http://www.angelfire.com/falcon/speedload/Enabler.htm

Sous Windows 7 SP1, pour que `Windows Enabler` fonctionne, il faut impérativement désactiver l'UAC* et redémarrer la machine.

Attention

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.

Truc & astuce

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.

2.2.3. Les sessions locales

Si des chemins ont étés modifiés par ESU (*Groupe de machine → Windows → Dossiers*), à l'ouverture d'une session locale le programme **logon.exe** redéfinit les chemins d'accès aux icônes du *Menu démarrer* et du *Bureau* avec leurs valeurs par défaut.

En effet, les lecteurs réseaux peuvent être indisponibles lors de l'ouverture d'une session locale.

Remarque

Sous Windows Vista et Windows 7 ce processus nécessite une élévation de droits au niveau de l'U*AC*.

Le programme **logon.exe** affiche alors la question : `Ré-initialiser le Menu démarrer et le Bureau ?` suivit par celle de l'UAC* (si il est activé) pour la validation de l'action.

L'UAC* 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.

2.3. Gestion des configurations clientes avec ESU

2.3.1. Introduction

Présentation

ESU* 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.

2.3.2. La console ESU

i - 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 :

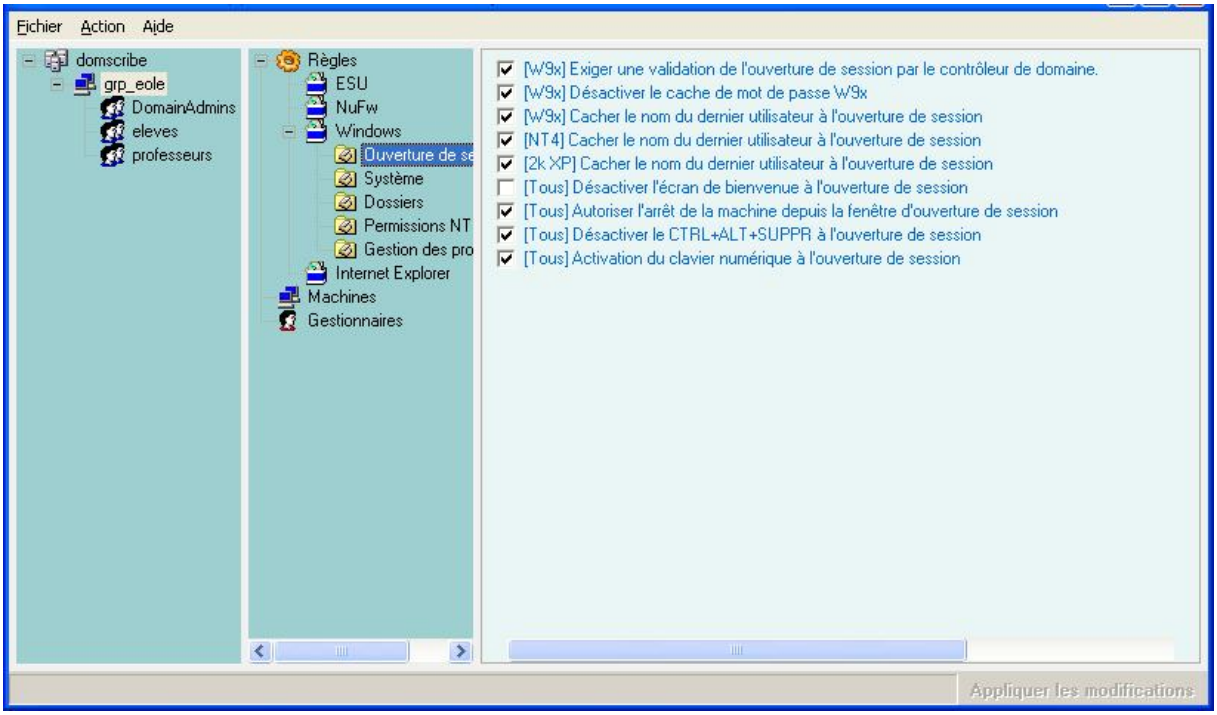
- la première liste les groupes de machines du domaine, et les utilisateurs/groupes gérés dans ce groupe de machines ;
- la seconde contient les différentes catégories de règles. Ces catégories peuvent comporter des sections ;
- la troisième partie affiche les règles et leur paramétrage.

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.



ii - Les groupes de machines

Création d'un nouveau groupe de machines

Les groupes de machines servent à regrouper les machines dans une même configuration en fonction de leur nom.

A l'installation du module, ESU est pré-configuré avec un groupe de machines *grp_eole* paramétré afin de prendre en compte toutes les machines du domaine (Simplement le caractère "*").

Ce groupe de machines a été pré-créé afin de servir d'exemple et pour que l'installation du client Scribe soit suffisante pour obtenir une station pleinement fonctionnelle dès la première ouverture de session.

Pour créer votre propre groupe, faites un clic droit sur le *domaine* et sélectionnez "**Nouveau groupe de machines**" ou sélectionnez le domaine et utilisez le raccourci clavier [Ctrl+N].

Renseignez le nom du groupe de machine (ici *technologie*) et paramétrez les noms des machines à ajouter au groupe.

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.).

Truc & astuce

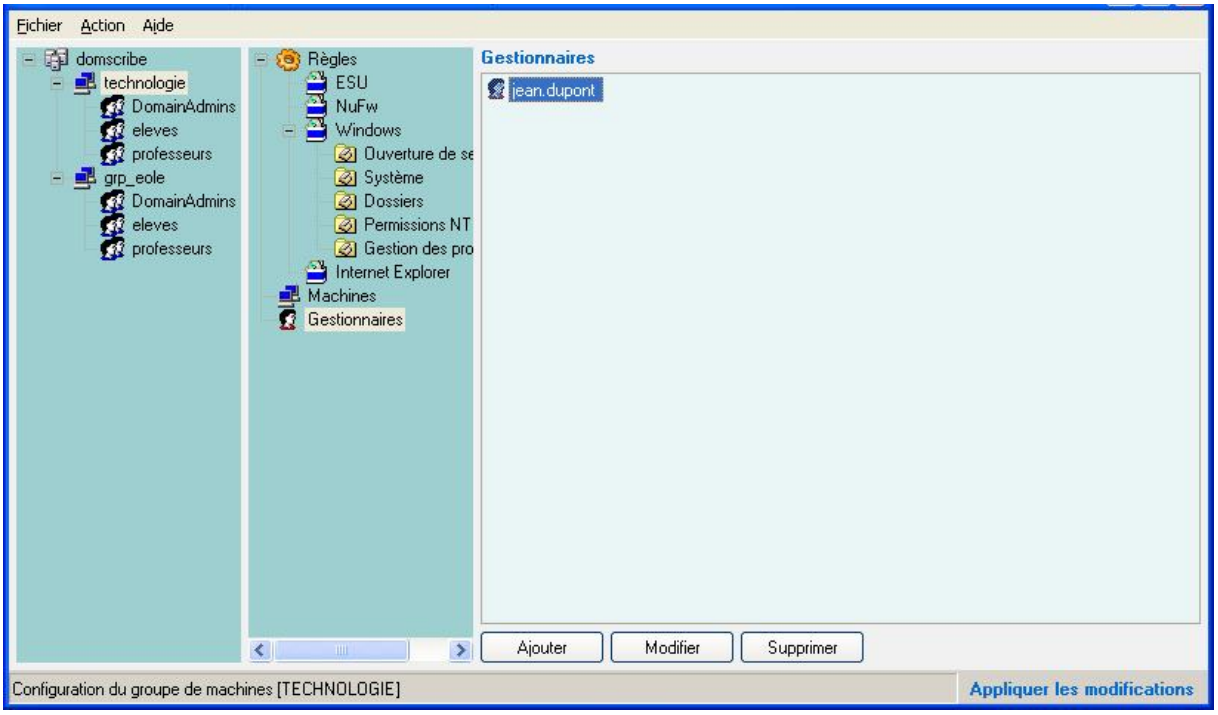
Il est possible de prendre en compte plusieurs machines en une fois en utilisant le caractère étoile, exemple : "techno*".

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**".

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>**).



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

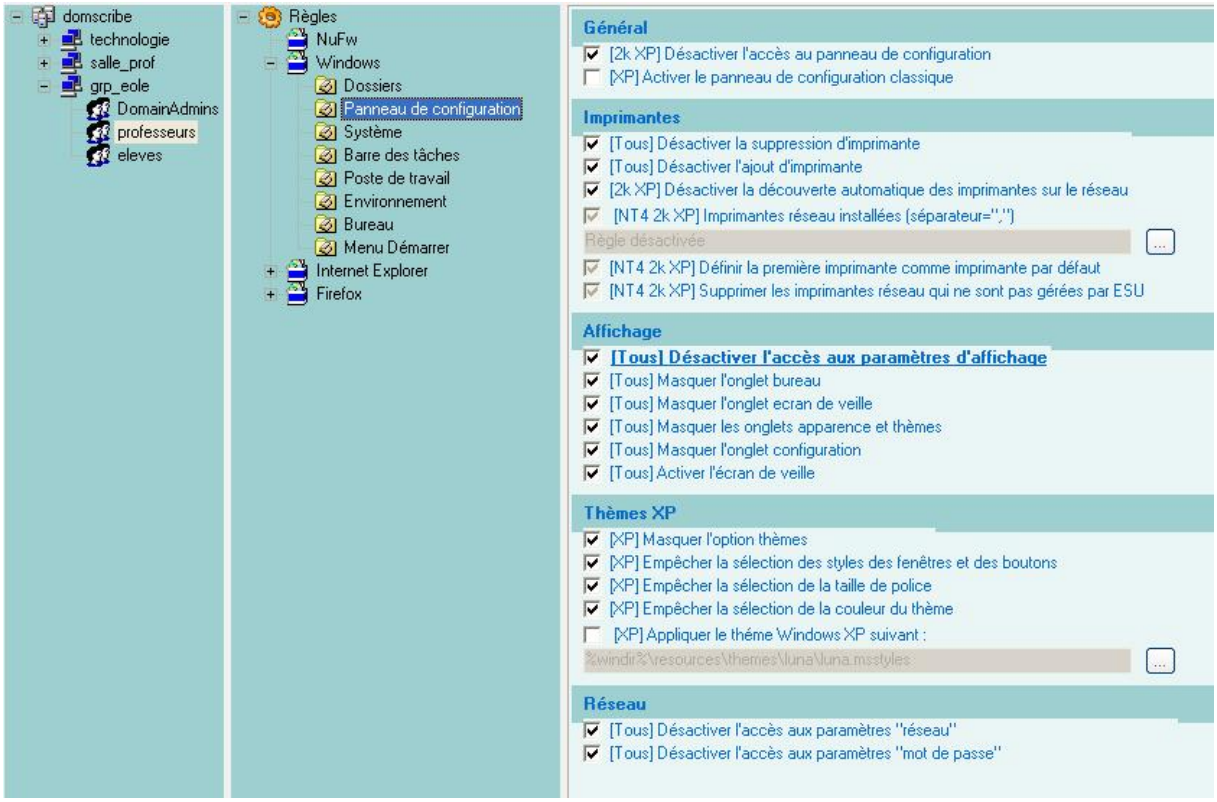
Le groupe DomainAdmins

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.).

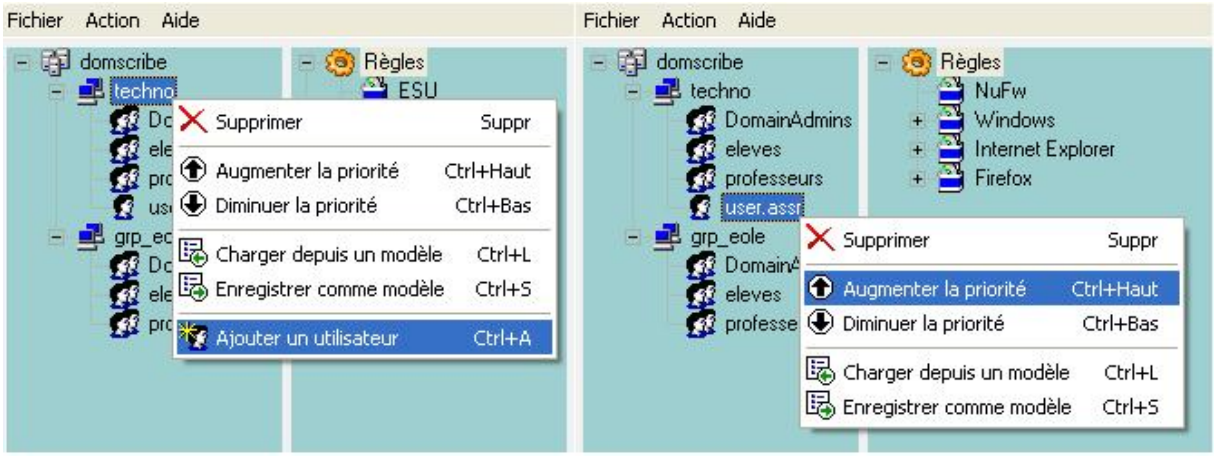
iii - Les utilisateurs et groupes d'utilisateurs

Un environnement différent peut être appliqué en fonction du nom de l'utilisateur ou des groupes auxquels il appartient.



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.



Comme pour les groupes de machines, les utilisateurs et groupes sont parcourus de haut en bas. ESU s'arrête à la première correspondance.

Ici, l'utilisateur *user.assr* fait partie du groupe *eleves*. Pour lui appliquer une configuration spécifique, il faut lui affecter une priorité supérieure à celle du groupe *eleves*.

iv - Les imprimantes

Attention

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.

v - Le proxy

Depuis la version EOLE 2.3, la configuration du proxy ESU s'effectue dans l'interface de configuration du module.

Configuration du proxy ESU

vi - Trucs et astuces

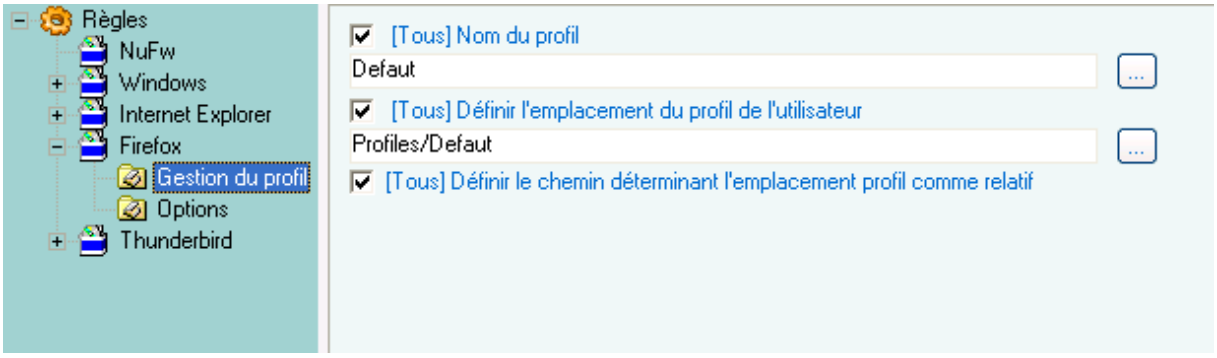
Les dossiers d'icônes

- 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

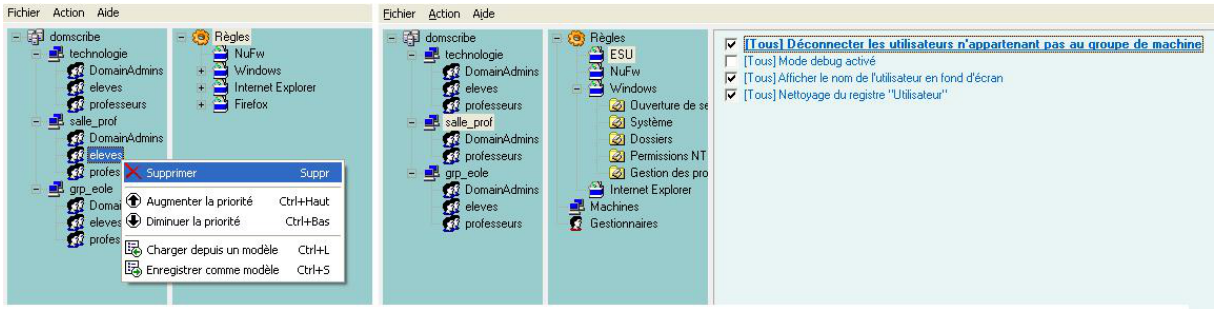
Afin de paramétrer correctement la *Gestion du profil* Firefox avec ESU, il faut sélectionner au moins une *Option*, la page de démarrage par exemple.



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.



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.

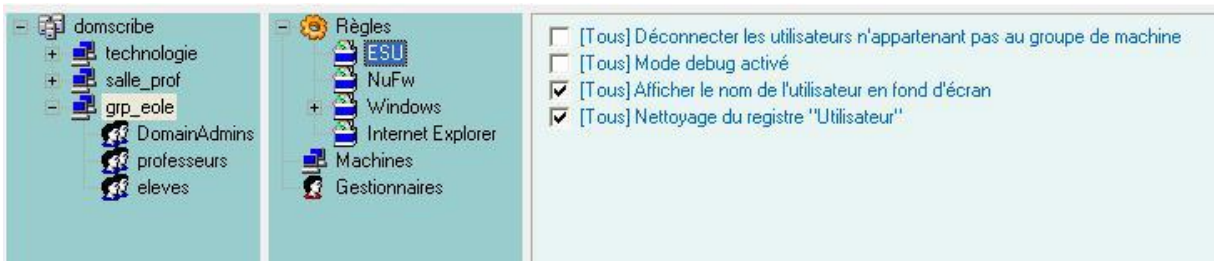
Pour les groupes d'utilisateurs

- **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*).

2.3.3. 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%
- %GROUPES%
- %SID%
- %IP%

Exemple de configuration personnalisée du texte en fond d'écran

Contenu du fichier :

USERLNAME == %USERLNAME%

COMPUTERNAME == %COMPUTERNAME%

ESU_OS == %ESU_OS%

ESU_GU == %ESU_GU%

GROUPES == %GROUPES%

IP == %IP%

NUMBER_OF_PROCESSORS == %NUMBER_OF_PROCESSORS%

PROCESSOR_IDENTIFIER == %PROCESSOR_IDENTIFIER%

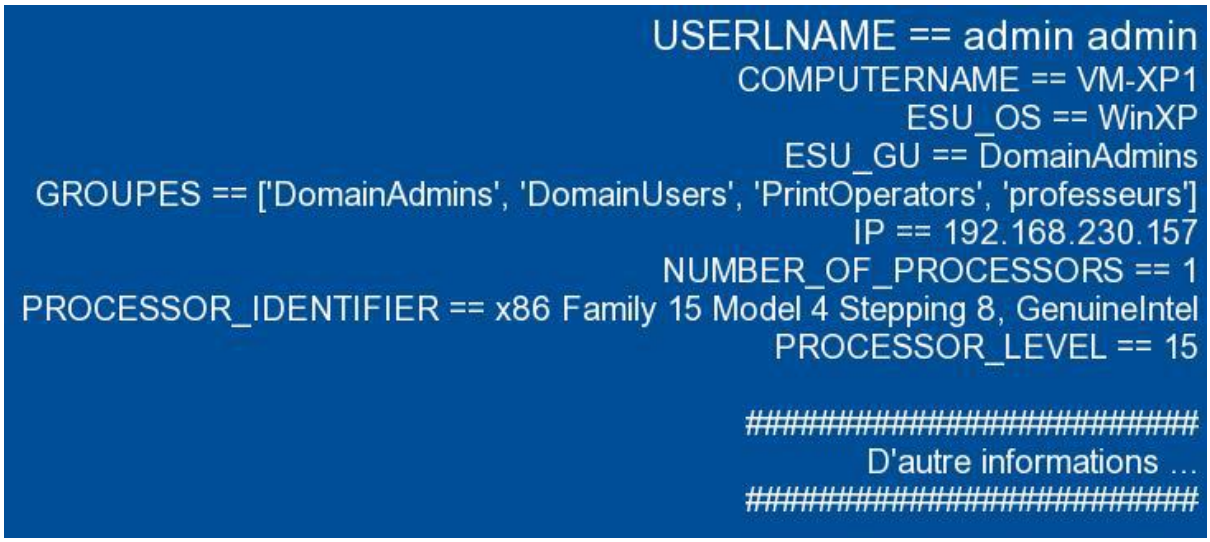
PROCESSOR_LEVEL == %PROCESSOR_LEVEL%

##########

D'autre informations ...

##########

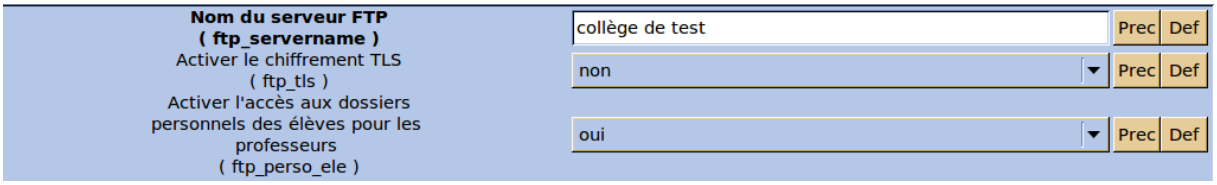
Résultat :



3 Clients FTP

Le serveur FTP est activable/désactivable dans l'onglet *Services* par l'intermédiaire de l'option : **Activer l'accès FTP**.

L'onglet *Ftp* n'apparaît en mode expert que si le service est activé.



Il est possible 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.

Il est possible de passer l'option **Activer le chiffrement TLS** à **oui** mais son utilisation est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

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.

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**.

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 (Ajaxplorer sur le module Scribe).

Pour accéder aux documents avec un navigateur web il faut préciser le protocole dans l'URL :

ftp://user@<adresse_serveur>/

ou

ftp://<adresse_serveur>/

Pour accéder aux fichiers par l'application web Ajaxplorer il faut l'activer dans l'onglet *Applications web*. 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>/ajaxplorer/** moyennant l'authentification (mire EoleSSO).

Attention

- 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.
- L'utilisation du chiffrement TLS est déconseillée car les échanges réalisés avec du FTP sécurisé ne passent pas ou passent difficilement les pare-feux.

XXI 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 (http://envole.ac-dijon.fr/).

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.

Attention

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.

1 SSO

L'authentification unique

EOLE propose un mécanisme d'authentification unique par l'intermédiaire d'un serveur SSO*.

Ce serveur est compatible CAS*, SAML* et OpenID*.

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 (local) ou 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.

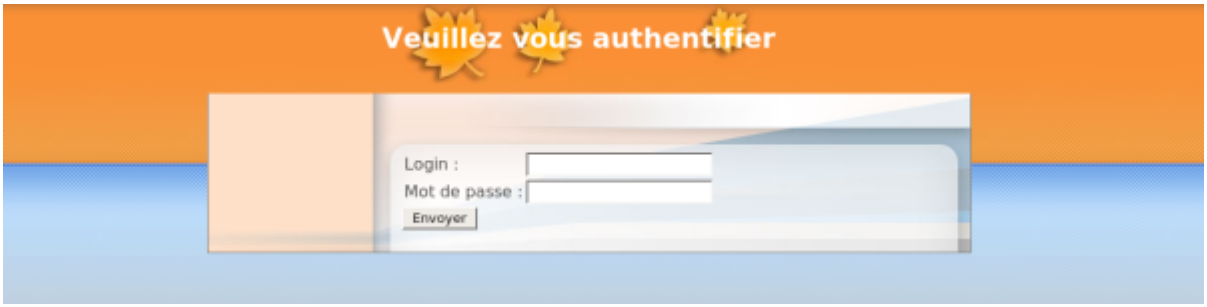
Cette opération nécessite la reconfiguration du module par la commande [reconfigure].

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 :



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**.

2 Applications pré-installées

Il est possible d'ajouter au module Horus des applications web pré-installées.

Il y différentes méthodes de mise en œuvre et les rôles des utilisateurs sont très différents d'une application à l'autre.

Reportez-vous à la documentation de chacune d'elles pour plus d'informations.

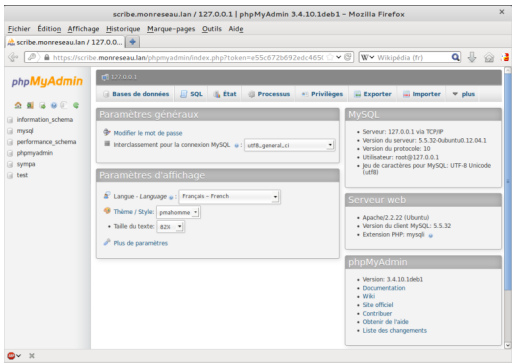
Reconfiguration du module

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].

2.1. phpMyAdmin

Présentation



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.

Truc & astuce

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].

Remarque

Pour les modules en mode conteneur il faut se placer dans le conteneur web pour pouvoir effectuer les commandes :

```
# ssh web
```

```
# a2dissite nom_de_l'application
```

```
# service apache2 reload
```

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.

Attention

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'IP ou la plage d'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 :

[/usr/share/eole/mysql_pwd.py]

Truc & astuce

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.

3 Applications pré-packagées

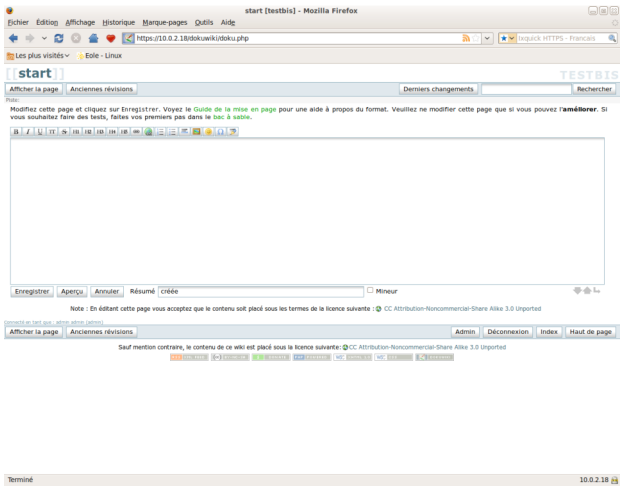
Il est possible d'ajouter au module Horus des applications web pré-packagées dont l'installation est laissée à votre initiative.

Il y différentes méthodes de mise en œuvre et les rôles des utilisateurs sont très différents d'une application à l'autre.

Reportez-vous à la documentation de chacune d'entre elles pour plus d'informations.

3.1. Dokuwiki

Présentation



DokuWiki est un Wiki simple d'utilisation. Il permet l'édition et la rédaction commune entre plusieurs utilisateurs.

http://www.dokuwiki.org/

Installation

DokuWiki s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-dokuwiki
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande [reconfigure].

Attention

Il existe un paquet **dokuwiki** qu'il ne faut pas confondre avec le paquet **eole-dokuwiki**.

Truc & astuce

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].

Remarque

Pour les modules en mode conteneur il faut se placer dans le conteneur web pour pouvoir effectuer les commandes :

```
# ssh web
```

```
# a2dissite nom_de_l'application
```

```
# service apache2 reload
```

Accéder à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/dokuwiki/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Les élèves, les enseignants et les administrateurs ayant un compte sur Scribe possèdent un accès à l'application.

- **administrateur**

  Seul l'utilisateur `admin` est administrateur de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer se rôle à un autre utilisateur mais aussi à un groupe d'utilisateurs.

  Il peut aussi, ajouter des privilèges à un ou plusieurs utilisateurs.

- **@ALL**

  Toute personne ayant un compte authentifié sur Scribe est "ALL" mais n'a aucun droit.

- **@professeurs**

  Les enseignants peuvent créer des nouvelles pages et éditer.

- **@eleves**

  Les élèves ont le droit de lecture sur l'ensemble du wiki.

- **@administratifs**

  Les administratifs n'ont pas de droit sur le wiki

- **visiteur anonyme**

  Ne peut pas accéder à l'application.

Sur le module Horus, l'utilisateur `admin` est administrateur de l'application et les autres utilisateurs n'ont par défaut aucun droit.

Remarque

Les rôles sont directement modifiables dans l'application par l'administrateur :

`http://<adresse_serveur>/dokuwiki/doku.php?id=start&do=admin&page=acl`

Remarques

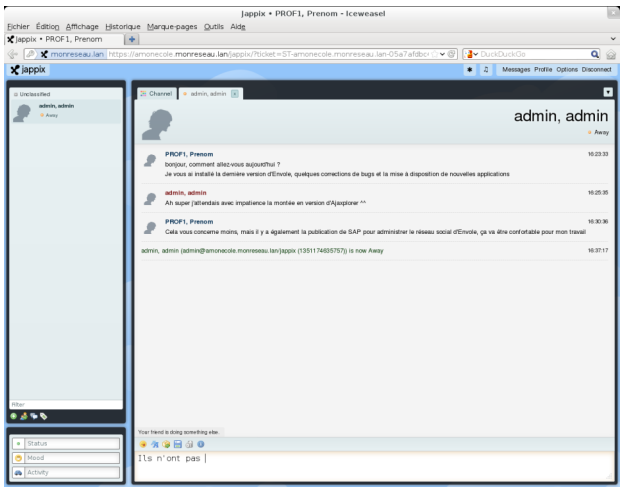
Les données utilisateurs relatives à l'application sont stockées dans le répertoire **data/** de l'application et sont sauvegardées par Bacula.

Il existe 3 fichiers de configuration pour Dokuwiki :

- **dokuwiki.php** → le fichier principal ;
- **local.php** → le fichier secondaire est vide pour utilisation ultérieure ;
- **local.protected.php** → le fichier protégé qui contient les configurations sensibles :
  - la méthodes d'authentification ;
  - les informations relatives à l'annuaire LDAP ;
  - l'emplacement du répertoire qui contient les données de Dokuwiki.

3.2. Jappix

Présentation



Jappix est un client web de communication instantanée. Il est libre et basé sur XMPP*.

Il permet une communication en temps réel entre les personnes possédant un compte XMPP.

Cette communication se fait simplement en utilisant un navigateur web moderne.

Un canal est à disposition pour laisser des messages de statut.

http://jappix.com

Installation

Jappix s'installe manuellement, saisir les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-jappix
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande [reconfigure].

Si le serveur Jabber n'est pas installé un conteneur supplémentaire doit être créé, il faut donc exécuter la commande `gen_conteneurs` comme le propose la commande reconfigure.

Cette commande doit être suivi de la ré-instanciation du module avec la commande instance :

```
# instance /etc/eole/config.eol
```

Attention

L'application nécessite que le service **ejabberd** soit activé.

Dans l'interface de configuration du module, onglet Services, mettre *Activer le serveur de messagerie instantanée ejabberd* à **oui**.

L'application est très sensible à la configuration réseau mise en œuvre et son fonctionnement requiert notamment des noms DNS.

La configuration recommandée est donc la suivante :

domain_jabber_etab = *eolesso_adresse* = *web_url* = *ssl_subjectaltname_ns* = "nom_de_domaine"

Si cette configuration n'est pas respectée, l'erreur suivante s'affichera :

Erreur » Service indisponible

Attention la modification de certains de ces paramètres nécessite de régénérer les certificats.

Truc & astuce

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].

Remarque

Pour les modules en mode conteneur il faut se placer dans le conteneur web pour pouvoir effectuer les commandes :

```
# ssh web
# a2dissite nom_de_l'application
# service apache2 reload
```

Accéder à l'application

Pour accéder à l'application se rendre à l'adresse : `http://<adresse_serveur>/jappix/`

Rôles des utilisateurs

Tous les utilisateurs présents dans l'annuaire ont un accès à l'application.

Remarques

Par défaut il n'est pas possible de téléverser des fichiers dans le canal car il n'y a pas de gestion des quotas et la partition du conteneur pourrait se remplir très vite :

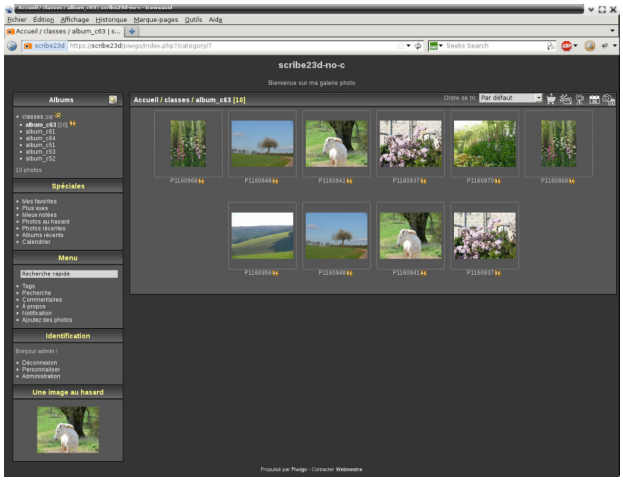
En attendant, il est tout de même possible d'activer cette fonctionnalité en créant un répertoire accessible en écriture à Apache :

```
# ssh reseau
# mkdir /usr/share/jappix/store/share
# chown www-data:root /usr/share/jappix/store/share
```

[ctrl + d] pour sortir de la connexion SSH.

3.3. Piwigo

Présentation



Piwigo est une application de gestion de galerie photo en ligne.

http://fr.piwigo.org/

Installation de Piwigo

Piwigo s'installe manuellement, en saisissant les commandes suivantes :

```
# Query-Auto
```

```
# apt-eole install eole-piwigo
```

L'application n'est pas disponible immédiatement après l'installation.

L'opération nécessite une reconfiguration du serveur avec la commande [reconfigure].

Truc & astuce

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].

Remarque

Pour les modules en mode conteneur il faut se placer dans le conteneur web pour pouvoir effectuer les commandes :

```
# ssh web
```

```
# a2dissite nom_de_l'application
```

```
# service apache2 reload
```

Accès à l'application

Pour accéder à l'application, se rendre à l'adresse : `http://<adresse_serveur>/piwigo/`

L'authentification se fait **obligatoirement** par le biais du serveur SSO, ce service doit donc être actif.

Rôles des utilisateurs

Par défaut les rôles des utilisateurs sont assignés comme suit :

- **Administrateur**

  Seul l'utilisateur `admin` est "webmaster" de l'application.

  Il a un accès complet à l'application et à sa configuration.

  Il peut déléguer ce rôle en donnant les droits "administrateur" à un utilisateur.

- **Enseignant**

  Les enseignants peuvent téléverser des nouvelles images dans les galeries de leurs classes d'appartenance.

- **Élèves**

  Ils peuvent consulter la galerie de leur classe d'appartenance.

- **Autres**

  Par défaut, les autres utilisateurs peuvent se connecter à l'application mais n'ont pas accès à la consultation des galeries.

Remarques

Les comptes sont créés dans Piwigo lors de la première connexion à l'application (initialisation du compte).

L'application est configurée pour que chaque classe ait sa propre galerie photo.

Les galeries portant le nom d'une classe ne se créent qu'à l'initialisation d'un compte enseignant ou élève de cette classe.

4 Ajout d'applications web

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 http://sourceforge.net/projects/egroupware/files/egroupware/eGroupware-1.6.002/eGroupware-1.6.002.tar.gz/download
```

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

```
tar xzvf eGroupware-1.6.002.tar.gz
```

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 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/tmp
  ```

- sur le module AmonEcole :

  ```
  ssh reseau
  chown -R www-data: /var/www/html/egroupware/tmp
  ```

  [ctrl + d] pour sortir du conteneur

Attention

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

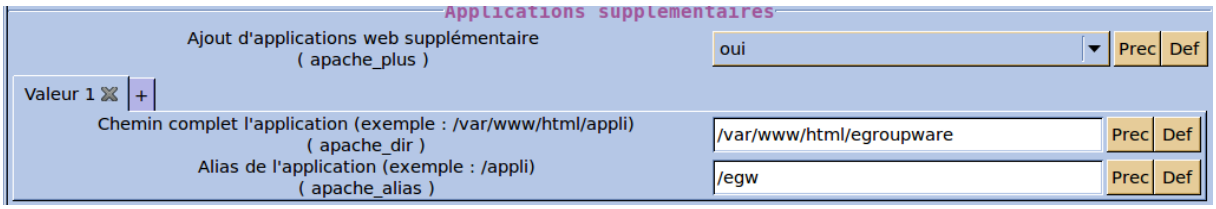
Installation manuelle de paquets

4.2. Configuration Apache

Méthode Creole

Dans l'interface de configuration du module :

- aller dans l'onglet *apache* en mode expert ;
- et indiquer le chemin complet de l'application et l'alias de l'application ;



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

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">
    AllowOverride None
    DirectoryIndex index.php
    Order Allow,Deny
    Allow from All
</Directory>
```

- recharger la configuration d'Apache à l'aide de la commande CreoleService* :

  CreoleService apache2 reload

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

Remarque

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.

4.3. Configuration MySQL

Méthode EOLE

Utiliser le script **/usr/share/eole/sbin/mysql_pwd.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
```

Remarque

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 **/usr/share/eole/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.

Conseil

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.

Attention

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`.

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*

Truc & astuce

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.

Définition de filtres d'attributs

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

Truc & astuce

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* 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**

Le compte en lecture seule

> "cf Utilisateurs spéciaux", page 399.

XXII Réplication LDAP

Avec le modules 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).

Attention

Il est déconseillé de répliquer des serveurs Scribe et des serveurs Horus sur le même client Seshat.

1 Pré-requis

Serveur Scribe ou Horus

- la réplication LDAP (fournisseur) doit être activée dans l'interface de configuration du module (dans l'onglet `Openldap`, en mode expert).

Réseau

- le port 389 et/ou le port 636 (selon la configuration mise en place) doit être ouvert du serveur Seshat vers le serveur Scribe ou Horus et si possible dans le sens inverse.

2 Mise en place

Sur Scribe ou Horus, lancer la commande **/usr/share/eole/active_replication.py** .

Cela génère un fichier de configuration nommé **/root/replication-<numero_etab>.conf** .

Mise en place manuelle

Il faut ensuite copier le fichier **/root/replication-<numero_etab>.conf** dans le dossier **/etc/ldap/replication** du serveur Seshat.

Puis, sur Seshat, lancer la commande **/usr/share/eole/gen_replication.py**.

Mise en place via Zéphir

Si le serveur Scribe (ou Horus) et le serveur Seshat sont enregistrés sur le même serveur Zéphir, celui-ci peut se charger de la mise en place de la configuration sur le serveur Seshat.

Si le serveur Scribe (ou Horus) est enregistré, la connexion à Zéphir est proposée automatiquement en fin d'exécution du script :

```
Veuillez saisir votre identifiant Zéphir (rien pour annuler l'envoi) :
```

Il est impératif de connaître l'identifiant Zéphir du serveur Seshat pour finaliser la transaction.

```
Identifiant Zéphir du serveur de réplication (rien pour annuler l'envoi) :
```

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.

Truc & astuce

Les configurations envoyées *via* Zéphir sont stockées dans le répertoire **/etc/ldap/replication/zephir** du serveur Seshat.

3 Suivi et débogage

Truc & astuce

Pour obtenir des informations concernant la réplication, il faut paramétrer slapd avec le *log level* : 16384.

Attention, ce mode est très verbeux.

XXIII 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 2.3 ont été répartis dans des paquets distincts, ce qui rend leur installation complétement indépendante.

Un module EOLE 2.3 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 un module EoleBase.

1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un serveur OpenLDAP.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

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 et Seshat, 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-antivirus

Le paquet **eole-antivirus** permet la mise en place d'un serveur antivirus.

Attention

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://eoleng.ac-dijon.fr/documentations/eole-antivir.

Logiciels et services

Le paquet **eole-antivirus** s'appuie sur les services clamav-daemon et clamav-freshclam.

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirales (freshclam) s'installe sur le maître.

Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.

Sur 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)**.

Attention

C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.3. 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.

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.

1.4. eole-fichier

Le paquet `eole-fichier` permet la mise en place d'un serveur de fichiers complet.

Attention

Il est probable que ce paquet soit, un jour, découpé en plusieurs sous-paquets (un par logiciel) afin d'améliorer la modularité et la maintenance des outils qu'ils contient.

Logiciels et services

Le paquet `eole-fichier` permet de gérer les services suivants :

- smbd, nmbd et scannedonly (serveur de fichiers) ;
- nscd (cache) ;
- cups (serveur d'impressions) ;
- proftpd (serveur FTP) ;

Historique

Les services fournis sont spécifiques aux modules Horus et Scribe.

Grâce au paquet `eole-fichier`, 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)`.

Attention

En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.5. 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.

Historique

Utilisé à la base sur les modules Horus, Scribe et Sentinelle, le paquet **eole-mysql** est désormais 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)**.

1.6. eole-web

Le paquet **eole-web** permet la mise en place d'un serveur web.

Attention

L'installation d'**eole-web** entraîne celle d'**eole-mysql**.

Logiciels et services

Le paquet eole-web s'appuie principalement sur le service apache2.

Il permet également d'activer l'application phpMyAdmin.

Historique

A 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.

1.7. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de bases de données Interbase.

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]

Attention

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)
- 4333/tcp : creole_serv
- 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
- 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 un numéro de port standard peut être trouvée dans le fichier **/etc/services**.

3 L'annuaire LDAP d'Horus

L'annuaire LDAP* d'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.

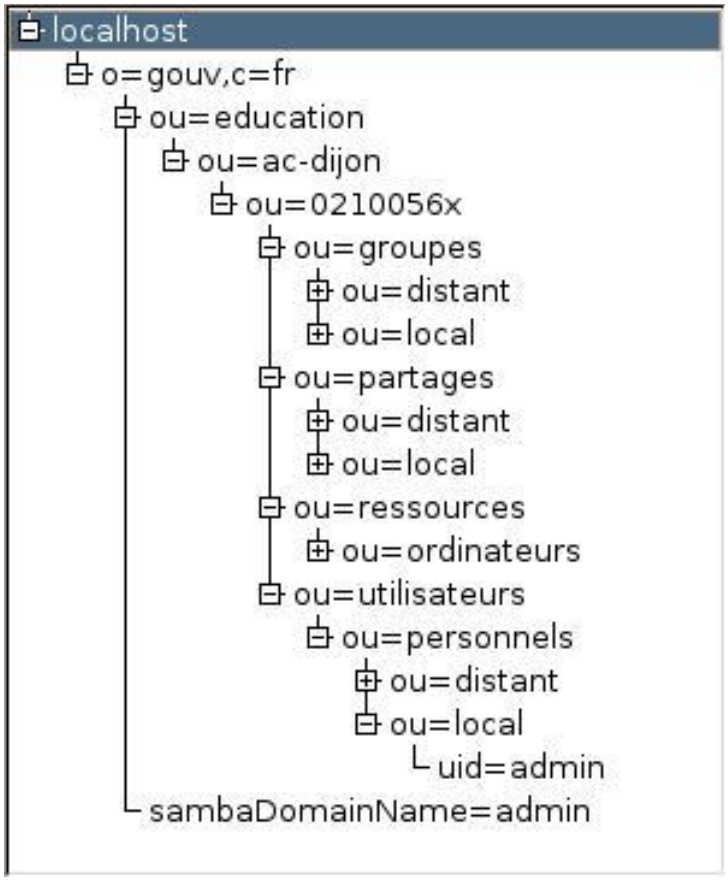
Le groupe `DomainComputers` est le groupe principal pour les stations intégrées au domaine.

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.



3.2. Utilisateurs spéciaux

Le compte d'administration

L'administrateur LDAP* 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

Attention

Ne pas confondre l'utilisateur `admin` de l'annuaire LDAP avec l'utilisateur `admin` du module Scribe ou Horus. Celui-ci est considéré dans l'annuaire comme étant un enseignant.

Le compte en lecture seule

Afin de répondre à certains besoins applicatifs, le compte en lecture seule `reader` a été ajouté :

cn=reader,o=gouv,c=fr

L'utilisation de ce compte par les applications leurs permettent d'accéder aux attributs LDAP protégés par des ACL*. 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**

Truc & astuce

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=gouv
,c=fr
```

Classes d'objet

Les ordinateurs héritent des classes d'objet suivantes :

- posixAccount (**nis.schema**)
- sambaSAMAccount (**samba.schema**)
- account (**cosine.schema**)

Attributs

Remarque

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)

XXIV Questions fréquentes

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

1 Questions fréquentes communes aux modules

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 *Système* / *Mise à jour* de l'EAD.

Dans un terminal

```
[python -c "from creole import maj; print maj.get_maj_day()"]
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section *Système* / *Mise à jour* de l'EAD.

Dans un terminal

Activation de la mise à jour hebdomadaire :

[/usr/share/eole/schedule/manage_schedule post majauto weekly add]

ou :

[python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"]

Désactivation de la mise à jour hebdomadaire :

[/usr/share/eole/schedule/manage_schedule post majauto weekly del]

ou :

[python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"]

Le mot de passe par défaut ne fonctionne pas

Suite à une nouvelle installation le mot de passe par défaut ne fonctionne pas.

Truc & astuce

Le mot de passe à saisir comprend les dollars devant et derrière : `$eole&123456$`

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 :

  ```
  UPDATE user SET Password=PASSWORD('MOT_DE_PASSE_RECUPERE_AVEC_GREP')
  WHERE User='debian-sys-maint' ;

  FLUSH PRIVILEGES ;
  ```

- quitter la console :

  `\quit` ou [Ctrl + d]

- relancer MySQL :

  ```
  # killall mysqld
  ```

  attendre quelques secondes

  ```
  # service mysql start
  ```

En mode conteneur il faut :

- se connecter au conteneur bdd :

  ```
  # ssh bdd
  ```

- récupérer le nouveau mot de passe MySQL :

  ```
  # grep password /etc/mysql/debian.cnf
  ```

- se connecter à la console MySQL :

  ```
  # mysqld_safe --skip-grant-tables & mysql -u root mysql
  ```

- mettre à jour le mot de passe :

  ```
  UPDATE user SET Password=PASSWORD('MOT_DE_PASSE_RECUPERE_AVEC_GREP')
  WHERE User='debian-sys-maint' ;

  FLUSH PRIVILEGES ;
  ```

- quitter la console :

  `\quit` ou [Ctrl + d]

- relancer MySQL :

  ```
  # killall mysqld
  ```

  attendre quelques secondes

  ```
  # service mysql start
  ```

- quitter le conteneur :

  ```
  # exit
  ```
  ou [Ctrl + d]

3 Questions fréquentes propres à la sauvegarde

La sauvegarde programmée est en échec

Relancer les services

Il faut en premier lieu enlever le verrou :

```
# /usr/share/eole/bacula/baculaconfig.py --unlock
```

Si tout n'est pas passé au vert dans l'EAD, il faut relancer les services :

```
# service bacula-director stop
# service bacula-sd stop
# service bacula-fd stop
# service bacula-director start
# service bacula-sd start
# service bacula-fd start
```

Modification de la configuration de Bacula non prise en compte

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

Afin de prendre en compte la nouvelle valeur, il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et ré-initialiser la base de données Bacula.

Ré-initialisation de la base Bacula

```
# /usr/share/eole/posttemplate/00-bacula instance
Le catalogue Bacula a déjà été initialisé, voulez-vous le réinitialiser ?
[oui/non]
[non] : oui
```

Réinitialisation de la sauvegarde

Pour réinitialiser la sauvegarde il faut vider le support de sauvegarde ou prendre un support de sauvegarde ne contenant aucun volume et surtout il faut ré-initialiser la base de données de Bacula.

Ré-initialisation de la base Bacula

```
# /usr/share/eole/posttemplate/00-bacula instance
Le catalogue Bacula a déjà été initialisé, voulez-vous le réinitialiser ?
[oui/non]
[non] : oui
```

Supprimer le verrou de sauvegarde

Truc & astuce

Il faut utiliser la commande suivante :

```
# /usr/share/eole/bacula/baculaconfig.py --unlock
```

Paramètres de la commande baculaconfig.py

Truc & astuce

Pour afficher la liste des paramètres de la commande [baculaconfig.py] :

```
# /usr/share/eole/bacula/baculaconfig.py --help
```

Problème de droit sur le point de montage des sauvegardes

Il peut survenir un problème de droit sur le point de montage des sauvegardes dans les cas où la configuration du support choisie est `Configuration manuelle du support` ou sur `Disque USB local`.

Appliquer manuellement les bons droits sur le point de montage

Lire les droits du répertoire **sauvegardes** :

```
# ls -l /mnt
# rwxr-xr-x 2 bacula root 4096 févr. 20 11:08 sauvegardes
```

Si les droits ne sont pas bons, utiliser la commande suivante :

```
# chown -R bacula:root /mnt/sauvegardes
```

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 ?

Truc & astuce

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 Bacula : **bconsole**.

Voici un aperçu des manipulations à réaliser :

```
# bconsole
(pour lancer la console de bacula)
*status dir
(pour voir les jobs en cours)
JobId Level Name Status
======================================================================
23 Full Complet.2010-09-03_23.00.00_02 is waiting for a mount request
24 Full BackupCatalog.2010-09-03_23.00.00_03 is waiting execution
*cancel JobId=23
(pour annuler le job en question)
*quit
```

Glossaire

.REG

Un fichier portant l'extension .REG est un fichier contenant des instructions permettant d'apporter des modifications locales à la base de registre.

AAF

L'annuaire fédérateur est un dispositif technique qui sert à alimenter l'annuaire LDAP d'un rectorat avec les autres annuaires académiques qui existent au sein de l'Éducation nationale et qui sont directement utilisés par les applications du ministère et des collectivités.

ACL

ACL pour Access Control List (ACL) désigne deux choses en sécurité informatique :

- un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX.
- en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.

ACL

ACL pour Access Control List (ACL) désigne deux choses en sécurité informatique :

- un système permettant de faire une gestion plus fine des droits d'accès aux fichiers que ne le permet la méthode employée par les systèmes UNIX.
- en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.

AGRIATES

De responsabilité partagée entre les collectivités locales et les académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements.

RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement.

L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE.

http://www.igc.educatio n.fr/agriates/agriates.ht m scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'intranet académique.

C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements.

RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes.

RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement.

RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements

Anti-spoofing

L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.

ARV

ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan.

http://www.strongswan.org/

Bacula

Bacula est un ensemble de programmes qui permet de gérer les sauvegardes, les restaurations ou la vérifications de données d'un ordinateur sur un réseau hétérogène.

En termes techniques, il s'agit d'un programme de sauvegarde client/serveur. Il est relativement facile d'utilisation et efficace. Il offre de nombreuses fonctions avancées de gestion de stockage qui facilitent la recherche et la restauration de fichiers perdus ou endommagés.

CAS

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.

Conteneur

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.

Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.

Contrôleur de domaine NT

Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire.

Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "ADMINISTRATIF" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service administratif, et les comptes utilisateur qui sont autorisés à s'y connecter.

Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.

Cette base de données est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003), appelés Contrôleurs de Domaine.

Corosync

Corosync est un moteur de cluster. Un cluster est un groupe de deux ou plusieurs machines.

Creole

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

Il a été conçu pour être facilement personnalisable pour l'utilisateur final. Un ensemble d'outils est proposé pour modifier ou étendre les fonctionnalités offerte par EOLE.

CreoleService

`CreoleService` est un nouvel outil qui vient remplacer avantageusement la fonction *Service()* de `FonctionsEoleNg`.

Pour l'utiliser : *`CreoleService apache2 reload`*

S'il existe le même service dans plusieurs conteneurs il est possible de spécifier le conteneur.

Exemple : *`CreoleService -c fichier smbd restart`*

CSV

Le CSV est un format informatique ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules. Il est souvent utilisé pour l'interopérabilité entre applications.

CUPS

CUPS est un système modulaire d'impression informatique qui permet à l'ordinateur sur lequel il est installé de fonctionner en tant que serveur d'impression. Un serveur d'impression est capable d'accepter des tâches d'impression d'autres ordinateurs (les clients) et de les répartir sur les imprimantes qui sont paramétrées.

CUPS met à disposition une interface de gestion accessible avec un navigateur web.

DHCP

Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.

Dictionnaire

Fichier, au format XML, décrivant l'ensemble de variable, des fichiers, des services et des paquets personnalisés en vue de configurer un serveur.

Distribution

Une distribution GNU/Linux est un ensemble cohérent de logiciels rassemblant un système d'exploitation composé d'un noyau Linux et d'applications, la plupart étant des logiciels libres.

DNS

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.

Durée de rétention

La durée de rétention désigne le temps de conservation des sauvegardes avant leur effacement.

ELF

ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé

EPLE

En France, un établissement public local d'enseignement (EPLE) est un établissement scolaire d'enseignement secondaire (ou, exceptionnellement, primaire) :

- collège
- lycée d'enseignement général et technologique (LGT)
- lycée professionnel (LP)
- établissement régional d'enseignement adapté (EREA)
- école régionale du premier degré (ERPD)

Era

Era est une application graphique de génération de règles de sécurité adaptée au module pare-feu Amon. À partir du fichier XML de description du pare-feu, un script de règles iptables pour Netfilter est généré de manière à implémenter ces règles sur

le module pare-feu Amon. La génération directe de règles iptables est également possible, permettant d'utiliser Era pour d'autres types de serveurs sous GNU/Linux.

Erlang

Erlang est un langage de programmation, supportant plusieurs paradigmes : concurrent, temps réel, distribué. Son cœur séquentiel est un langage fonctionnel à évaluation stricte, affectation unique, au typage dynamique fort. Sa couche concurrente est fondée sur le modèle d'acteur. Il possède des fonctionnalités de tolérance aux pannes et de mise à jour du code à chaud, permettant le développement d'applications à très haute disponibilité.

http://fr.wikipedia.org/wiki/Erlang_(langage)

ESU

Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques.

ESU propose de nombreuses fonctions :

- limitation des accès aux paramètres de Windows (panneau de configuration...) ;
- définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ;
- configuration des imprimantes partagées sur les postes ;
- configuration des navigateurs (internet Explorer et Mozilla Firefox) ;
- éditeur de règles permettant de rajouter autant de règles que vous le souhaitez.

FAI

Le FAI est un organisme (une entreprise ou une association) qui met à disposition une connexion au réseau informatique nommé Internet.

FTP

File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du

réseau, ou encore de supprimer ou modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS.

FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).

FTP, qui appartient à la couche application du modèle OSI et du modèle ARPA, deutilise une connexion TCP.

Par convention, deux ports sont attribués (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990.

Ce protocole peut fonctionner avec IPv4 et IPv6.

(Source : http://fr.wikipedia.org/wiki/File_Transfer_Protocol)

GNU

GNU est l'acronyme récursif de GNU is Not Unix. Projet fondé en 1984, il vise à produire un OS complet de type Unix.

Le noyau propre au projet n'étant pas fini, GNU est le plus souvent utilisé avec Linux. On parle alors de système GNU/Linux.

Haute Disponibilité

La haute disponibilité c'est garantir la disponibilité d'un service et son bon fonctionnement.

ICMP

Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

Image ISO

Une image ISO est une archive proposant la copie conforme d'un disque optique ou magnétique. L'opération de gravure de l'image ISO consiste à recopier cette structure sur un disque optique.

IMAP

IMAP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Mais contrairement au protocole POP, il permet de laisser les messages sur le serveur, ce qui présente un gros avantage pour consulter sa messagerie depuis plusieurs postes équipés de clients lourds.

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).

IPv6

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

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.

Licence CeCILL

Acronyme pour CEa Cnrs Inria Logiciel Libre.

C'est une licence libre de droit français compatible avec la licence GNU GPL.

Linux

Le noyau Linux est un noyau de système d'exploitation de type Unix. Le noyau Linux est un logiciel libre développé initialement par Linus Torvalds. Il a officiellement vu le jour en 1991.

Formellement, « Linux » est le nom du seul noyau, mais dans les faits, on appelle souvent « Linux » l'ensemble du système d'exploitation, aussi appelé « GNU/Linux », voire l'ensemble d'une distribution Linux.

LVM

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.

Mise à jour complète

La mise à jour complète prend en compte la mise à jour minimum ainsi que toutes les nouvelles fonctionnalités des paquets EOLE.

Mode promiscuité

Mode promiscuité se réfère à une configuration de la carte réseau qui lui permet d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.

MSS

MSS ou longueur maximum de segment en français désigne la quantité de données en octets qu'un ordinateur ou tout équipement de communication peut contenir dans un paquet seul et non fragmenté. Pour obtenir le meilleur rendement possible, la taille du segment de données et de l'en-tête doivent être inférieures au MTU.

Source : http://fr.wikipedia.org/wiki/Maximum_Segment_Size

MTU

La MTU définit la taille maximum du paquet (en octet) pouvant être transmis sur le réseau sans fragmentation.

Pour plus d'information : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit

NAS

NAS pour Network Attached Storage est un serveur relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

NetBIOS

NetBIOS est une architecture réseau et non un protocole réseau. C'est un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau. Ce service sert à associer un nom d'ordinateur à une adresse IP. NetBIOS tant à disparaître au profit des noms DNS.

Nginx

Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse.

Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions.

Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.

NTP

NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.

NUT

NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments :

- le démon `nut` lancé au démarrage du système ;
- le démon `upsd` qui permet d'interroger l'onduleur, il est lancé sur le PC relié à l'onduleur ;
- le démon `upsmon` qui permet de monitorer et lancer les commandes

nécessaires sur le réseau ondulé (arrêt de machines ...) ;

- différents programmes pour envoyer des commandes manuellement à l'onduleur.

upsd peut communiquer avec plusieurs onduleurs si nécessaire.

upsmon interroge à intervalle régulier la machine du réseau sur laquelle est lancée **upsd**.

OpenID

OpenID est un système d'authentification décentralisé qui permet l'authentification unique, ainsi que le partage d'attributs. Il permet à un utilisateur de s'authentifier auprès de plusieurs sites sans avoir à retenir un identifiant pour chacun d'eux mais en utilisant à chaque fois un unique identifiant OpenID. Le modèle se base sur des liens de confiance préalablement établis entre les fournisseurs de services et les fournisseurs d'identité (OpenID providers). Il permet aussi d'éviter de remplir à chaque fois un nouveau formulaire en réutilisant les informations déjà disponibles. Ce système permet à un utilisateur d'utiliser un mécanisme d'authentification forte.

OSCAR

OSCAR est un logiciel comparable de clonage. Il permet de réaliser des images des partitions et de les restaurer en cas de plantage ou de cloner des ordinateurs strictement identiques qui peuvent contenir aussi bien un système Windows qu'un système GNU/Linux. Il est particulièrement utilisé dans certains établissements scolaires.

Ce logiciel est en réalité un Live CD (basé sur la distribution GNU/Linux Gentoo) ce qui permet d'effectuer la maintenance de manière nomade, mais il peut également être installé en parallèle (dual boot) avec le système d'exploitation principal.

http://oscar.crdp-lyon.fr

Patch EOLE

#fixme

Path MTU Discovery

Lors d'une transmission de données informatiques, le Maximum Transmission Unit (MTU) est la taille maximale d'un paquet pouvant être transmis en une seule fois (sans fragmentation) sur une interface.

On parle de Path MTU pour désigner la taille maximale entre une machine source et une machine destination. Il correspond au plus petit MTU des interfaces où le paquet est transmis.

Pour plus d'informations : http://fr.wikipedia.org/wiki/Path_MTU_discovery

PDC

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.

PKI

Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.

Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs.

En résumé, ces services sont les suivants :

- enregistrement des utilisateurs (ou équipement informatique) ;
- génération de certificats ;
- renouvellement de certificats ;
- révocation de certificats ;
- publication de certificats ;
- publication des listes de révocation (comprenant la liste des certificats révoqués) ;
- identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'ICP) ;

- archivage, séquestre et recouvrement des certificats (option).

Source de la définition : http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques

POP

POP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. C'est cette dernière qui a cours actuellement.

POSIX

POSIX est le nom d'une famille de standards définie depuis 1988 par l'Institute of Electrical and Electronics Engineers. Ces standards ont émergé d'un projet de standardisation des API des logiciels destinés à fonctionner sur des variantes du système d'exploitation UNIX.

PPPoE

PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP et du contrôle de la connexion (débit, etc.), sur un réseau 802.3.

Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers, bien qu'une connexion utilisant un pont Ethernet-Ethernet soit souvent plus stable et plus performante. Il pose également des problèmes de MTU.

Projet LTSP

Linux Terminal Server Project (LTSP) est un ensemble de programmes permettant à plusieurs personnes d'utiliser le même ordinateur. Cela est réalisé par la mise en place d'un réseau informatique composé d'un serveur sous GNU/Linux et de clients légers.

http://www.ltsp.org/

PUA

Applications potentiellement indésirables.

RADIUS

RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification.

Réseau virtuel Privé

Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.

Samba

Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du protocole SMB, protocole standard de Microsoft.

À partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Windows Server, soit en tant que contrôleur de domaine principal (PDC) ou en tant que membre d'un domaine. Il peut également faire partie d'un domaine Active Directory.

SAML

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.

SIECLE anciennement Sconet

SIECLE est une application informatique de gestion des élèves, mise à disposition des établissements scolaires du second degré en France et accessible depuis leurs locaux par un simple navigateur via un réseau sécurisé (appelé réseau AGRIATES). Il remplace depuis janvier 2012 l'application Sconet (Scolarité sur le Net).

SMB

Le protocole SMB permet le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC équipé d'un système d'exploitation Windows.

SMTP

SMTP ou Simple Mail Transfer Protocol, est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.

SSH

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

SSO est une méthode permettant de centraliser l'authentification afin de permettre à l'utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques.

Les objectifs sont :

- simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent ;
- simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ;
- simplifier la définition et la mise en œuvre de politiques de sécurité.

strongSwan

strongSwan est une implémentation libre et complète de VPN IPsec pour les noyaux Linux 2.6 et 3.x. L'objectif de ce projet est de proposer des mécanismes d'authentification forts.

TCP Wrapper

TCP Wrapper est une technique, propre à Unix, permettant de contrôler les accès à un service (ou démon) suivant la source.

Il se configure grâce au deux fichiers /etc/hosts.allow et /etc/hosts.deny.

Tous les démons ne supportent pas la technique TCP Wrapper.

Telnet

Telnet est une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation.

Telnet est un protocole réseau utilisé sur tout réseau prenant en charge le protocole TCP/IP. Le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.

Telnet

Telnet est une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation.

Telnet est un protocole réseau utilisé sur tout réseau prenant en charge le protocole TCP/IP. Le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.

Template

Un template est un fichier contenant des variables Creole, qui sera instancié pour générer un fichier cible (typiquement un fichier de configuration serveur).

UAC

UAC, contrôle du compte de l'utilisateur en français est un mécanisme de protection des données introduit dans les systèmes d'exploitations Windows Vista et 7.

UAC est aussi connu sous ses dénominations précédentes durant le développement de Windows Vista, à savoir UAP (User Account Protection) et LUP (Least User Privilege).

Ce mécanisme permet d'exécuter par défaut les programmes avec des droits restreints, évitant ainsi que des applications puissent tourner avec des droits administratifs, qui permettraient de modifier la sécurité du système d'exploitation.

WINS

WINS est un serveur de noms et services pour les ordinateurs utilisant NetBIOS.

XMPP

XMPP peut être traduit par « Protocole extensible de présence et de messagerie »), et est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données.

XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la Voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.

XMPP est constitué d'un protocole TCP/IP basé sur une architecture client-serveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML).

XMPP est en développement constant et ouvert au sein de l'IETF.

Annexe

1 Configuration de l'anti-virus

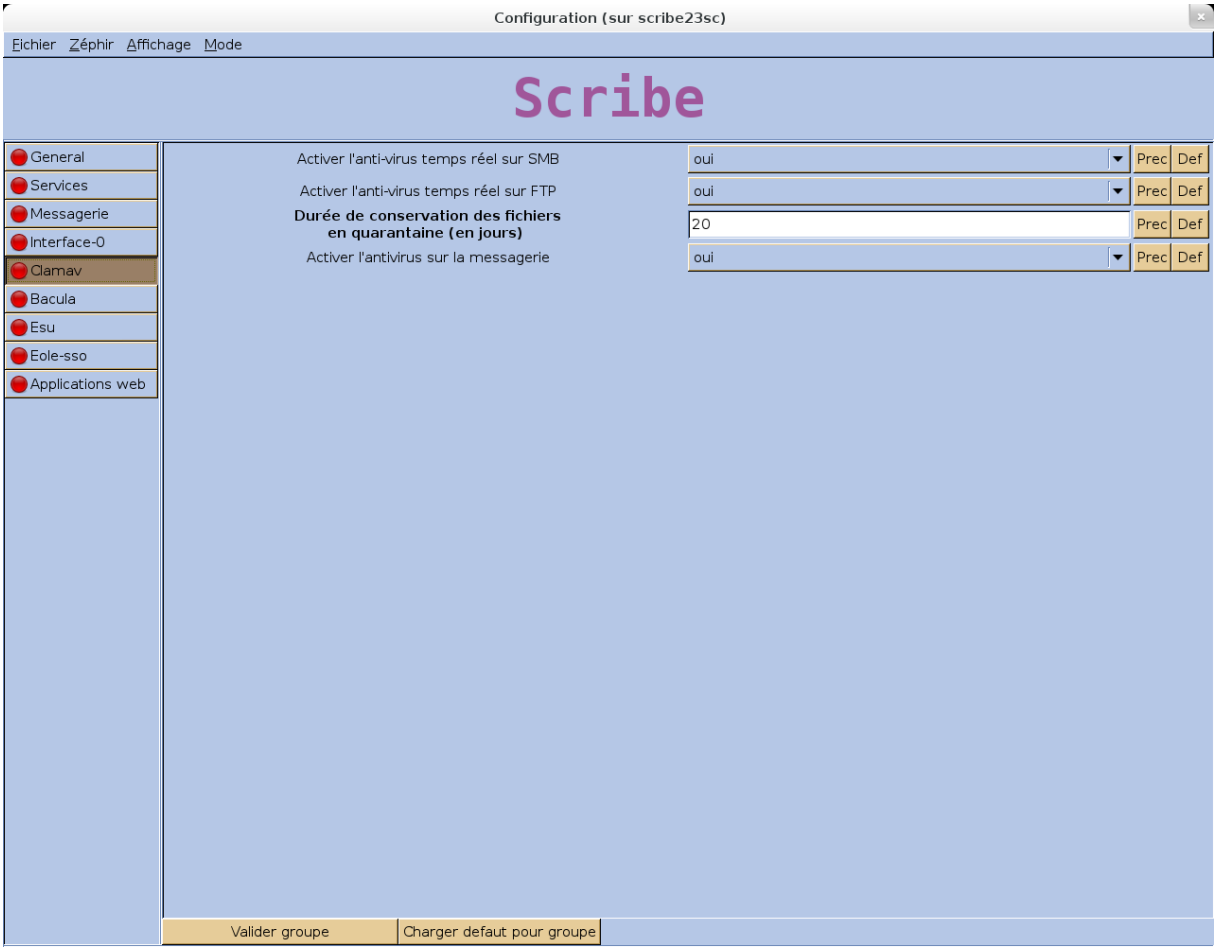
EOLE propose un service anti-virus réalisé à partir du logiciel Clamav.

Activation de l'anti-virus

Par défaut le service est activé sur le module et l'anti-virus est actif sur tous les services.

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

- le service SMB ;
- le service FTP ;
- la messagerie.

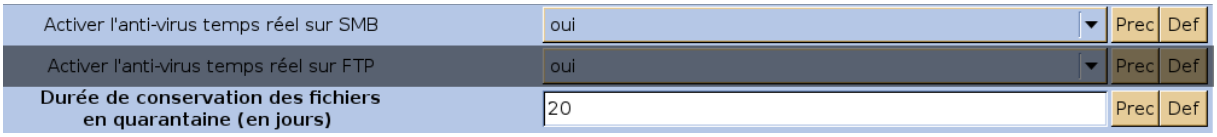


Truc & astuce

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

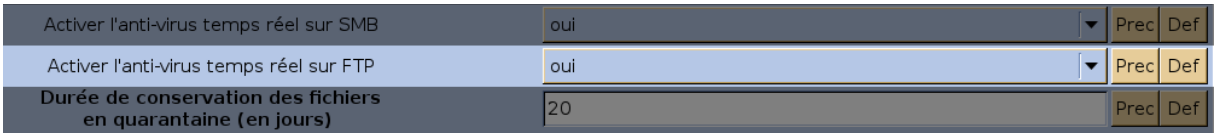
Le service est activé par défaut il est possible de le désactiver en passant la variable **Activer l'anti-virus temps réel sur SMB** à **non** dans l'onglet *Clamav*.



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.

Activation de l'anti-virus sur FTP

Pour activer 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 SMB`** à **`oui`** dans l'onglet *`Clamav`*.



Activation de l'anti-virus sur la messagerie

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

Contribuer

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 soutien à la base de données de virus examinera votre demande et mettre 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.

Attention

Il ne faut pas signaler des PUA* comme étant des faux positifs.

2 Configuration du mode multi-établissement

Attention

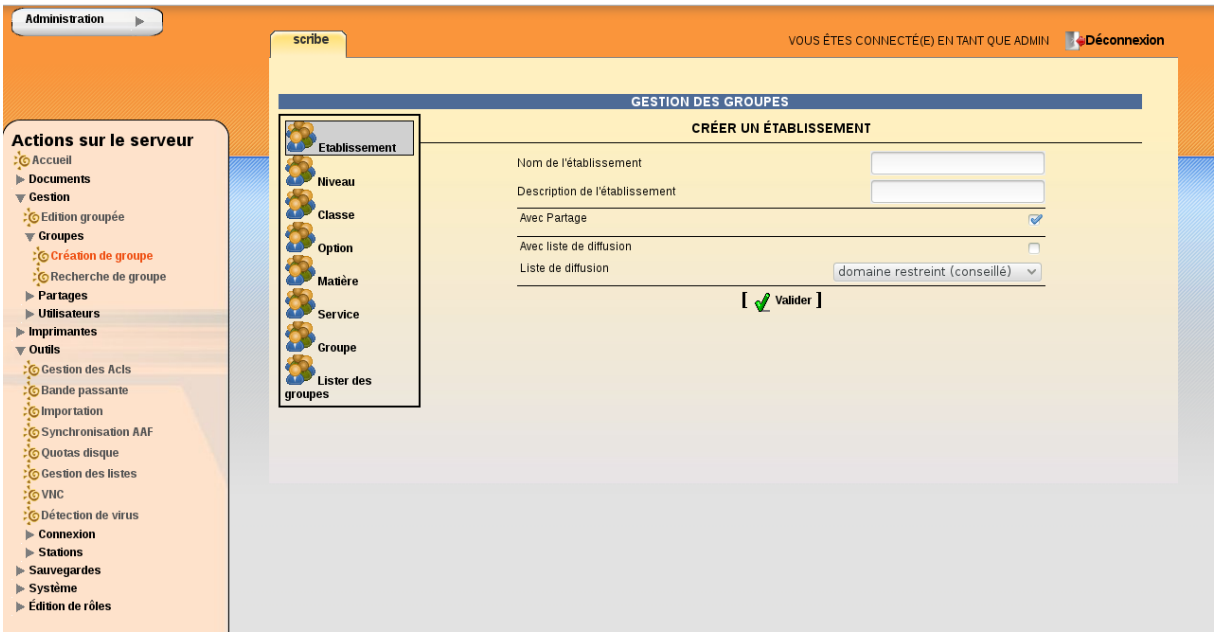
Passer d'un mode à l'autre sur un serveur en production n'est pas supporté.

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

Pour activer le mode multi-établissement il faut se rendre dans l'interface de configuration du module en mode expert, et dans l'onglet *Samba* passer à **oui** l'option **Support du multi-établissement**.

L'établissement par défaut est celui déjà déclaré dans la variable **Identifiant de l'établissement (exemple UAI)** de l'onglet *General*.

Le reste des réglages, la création d'un nouvel établissement et l'ajout des utilisateurs se fait dans l'EAD une fois le module instancié ou reconfiguré.



Il est possible d'ajouter un ou plusieurs établissements dans le menu principal de l'EAD. Il faut se rendre dans *Gestion* → *Groupes* → *Création de groupe* → *Etablissement*.

Les champs à remplir sont :

- le **Nom de l'établissement** ;
- un **Descriptif de l'établissement** ;
- **Avec partage** ;
- **Avec liste de diffusion** ;
- le type de liste de diffusion.

Le bouton Valider permet d'enregistrer la configuration du nouvel établissement.

Le peuplement de l'établissement se fait via l'outil d'importation de l'EAD : menu de l'EAD → *Outils* → *Importation*.

Consultez la rubrique Importation de l'EAD

3 Définition de filtres d'attributs

Toutes les données connues de l'utilisateur peuvent être propagées vers les applications lorsque celles-ci valident l'authentification de l'utilisateur auprès du serveur EoleSSO.

Pour décider quelles informations seront renvoyées aux différentes applications, un système d'application de filtres a été mis en place. Le principe est de définir dans un fichier un ensemble d'attributs à renvoyer à une(des) application(s), ainsi que le nom à leur donner dans le cadre de ce filtre.

Ces fichiers sont à placer dans le répertoire **/usr/share/sso/app_filters** et doivent avoir le format suivant :

```
[section1]
libelle=variable
libelle2=variable2
....
[section2]
....
```

- **section** sert à la mise en forme de la réponse (pour CAS, un nœud dans le XML retourné lors de la validation du ticket)
- **variable** correspond à l'identifiant LDAP de la donnée utilisateur à récupérer
- **libelle** est le nom qui sera utilisé pour présenter cette donnée dans la réponse du serveur

Le choix d'un filtre d'attribut est conditionné par l'adresse du service à atteindre (voir chapitre précédent). Il est également possible de créer dans le répertoire **app_filters** des **fichiers de filtres globaux** dont les attributs seront ajoutés à tous les filtres.

Le format est le même, mais ces fichiers doivent avoir l'extension **.global**.

Dans le cas ou un attribut défini dans un filtre global existe également dans le filtre d'une application, c'est la définition spécifique à l'application qui sera prise en compte lors de l'envoi des attributs à celle-ci.

Attention

Si vous souhaitez appeler la méthode statique `getUser(…)` dans votre application il est impératif d'utiliser au minimum la correspondance `user=uid` dans votre filtre. Sinon l'authentification ne peut pas aboutir : `CAS Authentification failed !`

Exemple

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
```

Complément

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`*

4 Gestion fine des groupes et des utilisateurs : ACL

Des ACLs* sont utilisées sur le système de fichiers pour permettre un réglage fin des droits d'accès aux partages et à leur contenu.

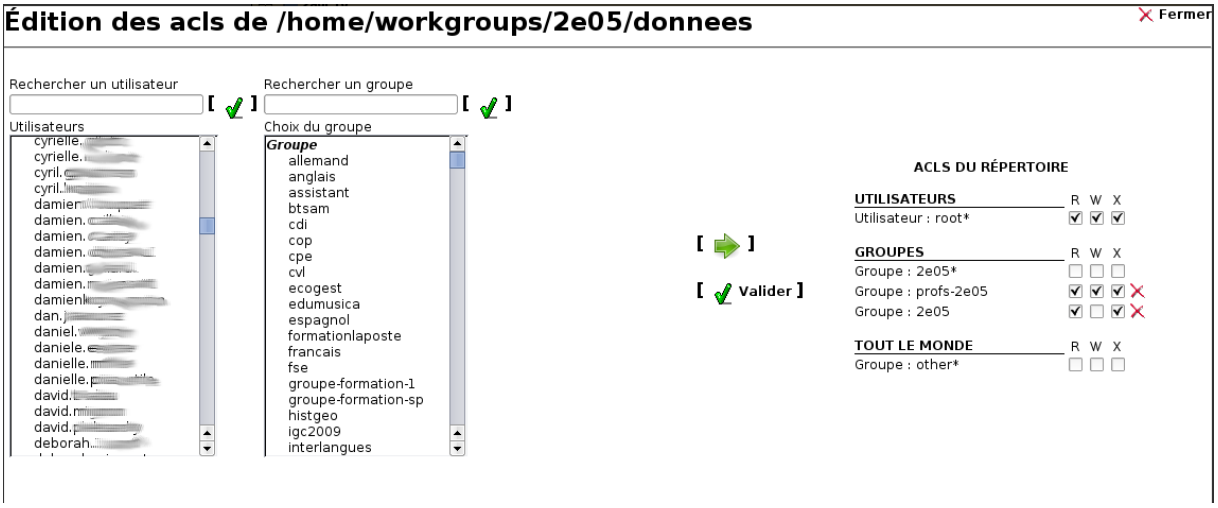
Modification des ACL sous Windows

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* (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.



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.

5 Importation

Se référer au document 'Importation'