

# Panorama des modules

EOLE 2.5



## EOLE 2.5

Version : révision : Avril 2018

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

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

Licence : Cette documentation, rédigée par le Pôle national de compétences Logiciels Libres, est mise à disposition selon les termes de la licence :

**Creative Commons Attribution - Partage dans les Mêmes Conditions 3.0 France (CC BY-SA 3.0 FR)** : <http://creativecommons.org/licenses/by-sa/3.0/fr/>.

### **Vous êtes libres :**

- de **reproduire, distribuer et communiquer** cette création au public ;
- de **modifier** cette création.

### **Selon les conditions suivantes :**

- **Attribution** : vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre) ;
- **Partage des Conditions Initiales à l'Identique** : si vous modifiez, transformez ou adaptez cette création, vous n'avez le droit de distribuer la création qui en résulte que sous un contrat identique à celui-ci.

À chaque réutilisation ou distribution de cette création, vous devez faire apparaître clairement au public les conditions contractuelles de sa mise à disposition. La meilleure manière de les indiquer est un lien vers cette page web.

Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits sur cette œuvre.

Rien dans ce contrat ne diminue ou ne restreint le droit moral de l'auteur ou des auteurs.

Cette documentation est basée sur une réalisation du Pôle national de compétences Logiciels Libres. Les documents d'origines sont disponibles sur le site.

EOLE est un projet libre (Licence GPL).

Il est développé par le Pôle national de compétences Logiciels Libres du ministère de l'Éducation nationale, rattaché à la Direction des Systèmes d'Information de l'académie de Dijon (DSI).

Pour toute information concernant ce projet vous pouvez nous joindre :

- Par courrier électronique : [eole@ac-dijon.fr](mailto:eole@ac-dijon.fr)
- Par FAX : 03-80-44-88-10
- Par courrier : EOLE-DSI - 2G, rue du Général Delaborde - 21000 DIJON
- Le site du Pôle national de compétences Logiciels Libres : <http://eole.orion.education.fr>

# Table des matières

|  |    |
|--|----|
| <b>Chapitre 1 - Introduction</b> .....           | 5  |
| 1. EOLE et le logiciel libre                     | 5  |
| 2. EOLE 2.5                                      | 5  |
| 3. Modules supportés disponibles                 | 8  |
| 4. Eolebase                                      | 10 |
| 5. Les outils EOLE                               | 12 |
| 6. Les dépôts EOLE                               | 13 |
| <b>Chapitre 2 - Module eCDL 2.5</b> .....        | 15 |
| 1. Qu'est ce que le module eCDL ?                | 15 |
| 2. À qui s'adresse ce module ?                   | 15 |
| 3. Les services eCDL                             | 15 |
| 4. Structure des conteneurs                      | 16 |
| 5. Les différences entre les versions 2.4 et 2.5 | 17 |
| <b>Chapitre 3 - Module eSBL 2.5</b> .....        | 20 |
| 1. Qu'est ce que le module eSBL ?                | 20 |
| 2. À qui s'adresse ce module ?                   | 20 |
| 3. Les services eSBL                             | 21 |
| 4. Structure des conteneurs                      | 22 |
| 5. Les différences entre les versions 2.4 et 2.5 | 22 |
| <b>Chapitre 4 - Module Amon 2.5</b> .....        | 25 |
| 1. Qu'est ce que le module Amon ?                | 25 |
| 2. À qui s'adresse ce module ?                   | 26 |
| 3. Les services Amon                             | 27 |
| 4. Structure des conteneurs                      | 27 |
| 5. Pré-requis                                    | 28 |
| 6. Les différences entre les versions 2.4 et 2.5 | 29 |
| <b>Chapitre 5 - Module Horus 2.5</b> .....       | 33 |
| 1. Qu'est ce que le module Horus ?               | 33 |
| 2. À qui s'adresse ce module ?                   | 35 |
| 3. Les services Horus                            | 35 |
| 4. Structure des conteneurs                      | 36 |
| 5. Pré-requis                                    | 36 |
| 6. Les différences entre les versions 2.4 et 2.5 | 37 |
| <b>Chapitre 6 - Module Scribe 2.5</b> .....      | 41 |
| 1. Qu'est ce que le module Scribe ?              | 41 |
| 2. À qui s'adresse ce module ?                   | 43 |
| 3. Les services Scribe                           | 43 |
| 4. Pré-requis                                    | 44 |
| 5. Les différences entre les versions 2.4 et 2.5 | 44 |
| <b>Chapitre 7 - Module Seshat 2.5</b> .....      | 49 |
| 1. Qu'est ce que le module Seshat ?              | 49 |

|  |           |
|--|-----------|
| 2. À qui s'adresse ce module ?                   | 49        |
| 3. Les services Seshat                           | 49        |
| 4. Structure des conteneurs                      | 50        |
| 5. Pré-requis                                    | 50        |
| 6. Les différences entre les versions 2.3 et 2.5 | 51        |
| <b>Chapitre 8 - Module Sphynx 2.5</b> .....      | <b>54</b> |
| 1. Qu'est ce que Sphynx ?                        | 55        |
| 2. À qui s'adresse ce module ?                   | 55        |
| 3. Les services Sphynx                           | 56        |
| 4. Pré-requis                                    | 56        |
| 5. Structure des conteneurs                      | 57        |
| 6. Les différences entre les versions 2.4 et 2.5 | 57        |
| <b>Chapitre 9 - Module Thot 2.7</b> .....        | <b>61</b> |
| 1. Qu'est ce que le module Thot ?                | 61        |
| 2. À qui s'adresse ce module ?                   | 61        |
| 3. Les services Thot                             | 62        |
| 4. Pré-requis                                    | 62        |
| 5. Les différences entre les versions 2.4 et 2.5 | 62        |
| <b>Chapitre 10 - Module Zéphir 2.5</b> .....     | <b>66</b> |
| 1. Qu'est ce que le module Zéphir ?              | 66        |
| 2. À qui s'adresse ce module ?                   | 67        |
| 3. Les services Zéphir                           | 68        |
| 4. Structure des conteneurs                      | 68        |
| 5. Pré-requis                                    | 69        |
| 6. Les différences entre les versions 2.3 et 2.5 | 70        |
| <b>Chapitre 11 - Module AmonEcole 2.5</b> .....  | <b>73</b> |
| 1. Qu'est ce que le module AmonEcole ?           | 73        |
| 2. À qui s'adresse ce module ?                   | 75        |
| 3. Les services AmonEcole                        | 75        |
| 4. Les conteneurs du module AmonEcole            | 76        |
| 5. Pré-requis                                    | 77        |
| 6. Les différences entre les versions 2.4 et 2.5 | 77        |
| Glossaire .....                                  | 82        |

# Chapitre 1

## Introduction



EOLE c'est : des logiciels libres, une version 2.5 et des outils...

## 1. EOLE et le logiciel libre



Le pôle de compétences EOLE du ministère de l'Éducation nationale est l'éditeur de distributions GNU/Linux EOLE basées sur Ubuntu. Il propose des modules serveurs faciles à déployer avec des outils de configuration et d'administration à distance.

Ces réalisations s'insèrent dans le cadre de réflexions et de recommandations d'un certain nombre de structures et d'organismes ministériels favorables à l'usage des logiciels libres dans l'administration.

À voir en particulier la note de la Direction interministérielle des systèmes d'information et de communication, la DISIC, parue en septembre 2012 : "Usage du logiciel libre dans l'administration".

Télécharger la circulaire sur le site de Legifrance :  
[http://circulaire.legifrance.gouv.fr/pdf/2012/09/cir\\_35837.pdf](http://circulaire.legifrance.gouv.fr/pdf/2012/09/cir_35837.pdf)

## 2. EOLE 2.5

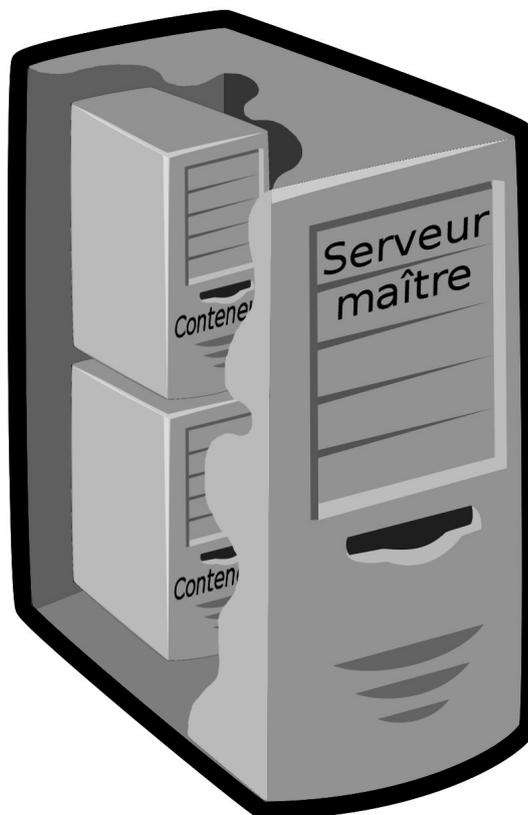


Les modules de la version EOLE 2.5 s'appuient sur la distribution GNU/Linux Ubuntu 14.04 LTS nommée également Trusty Tahr.

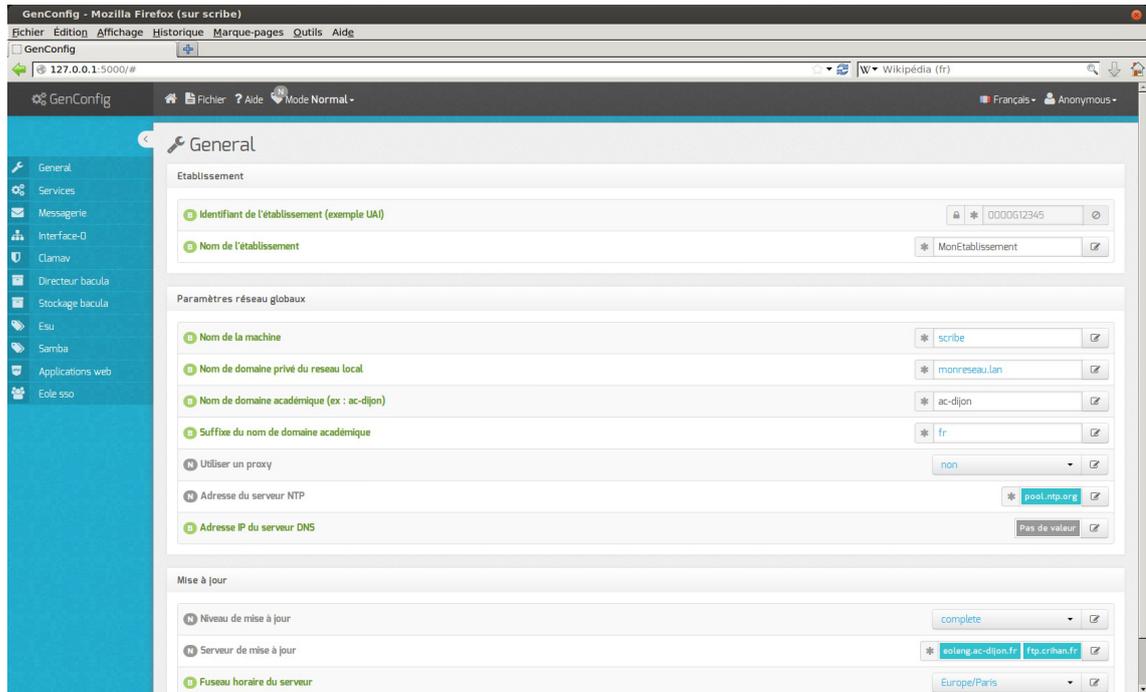
Ubuntu 14.04 LTS est disponible depuis le 17 avril 2014. Portant le label LTS<sup>[p.87]</sup>, cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2019. Le Pôle

de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2019.

# Module

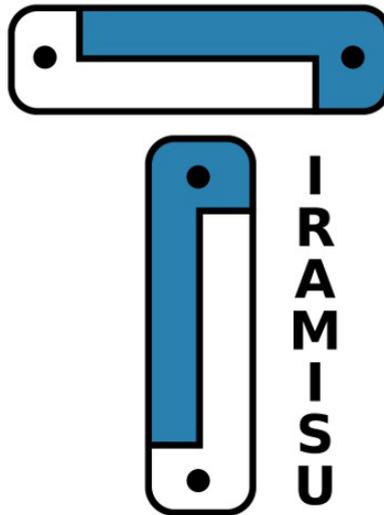


La version 2.5 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule instance du noyau présente sur le maître utilisée par l'ensemble des conteneurs. Cela permet, entre autre, une économie des ressources de la machine physique.



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

L'interface de configuration du module utilise la bibliothèque de gestion de configuration nommée Tiramisu<sup>[p.90]</sup>.



Logo du logiciel Tiramisu

## 3. Modules supportés disponibles

|                | <b>2.6.0</b>  | <b>2.6.1</b>  | <b>2.6.2</b>   | <b>2.7.0</b>  | <b>2.7.1</b>  |
|----------------|---|---|--|---|---|
| Fin du support | Juin 2021   | Juin 2021   | Juin 2021  | Juin 2023   | Juin 2023   |
| eCDL           |   |    |    |   |   |
| eSBL           |    |    |    |    |   |
| Amon           |   |    |    |    |    |
| Eclair         |    |    |    |   |    |
| Hâpy           |    |    |    |    |    |
| Hâpy Node      |    |    |    |    |    |
| Horus (NT)     |   |   |   |   |   |
| Horus (AD)     |   |   |  |   |  |
| Scribe (NT)    |  |  |  |   |   |
| Scribe (AD)    |   |   |  |   |  |
| Seshat         |   |  |  |  |  |
| Seth           |  |  |  |  |  |
| Sphynx         |  |  |  |  |  |
| Thot           |   |  |  |  |  |
| AmonEcole      |   |  |  |   |   |

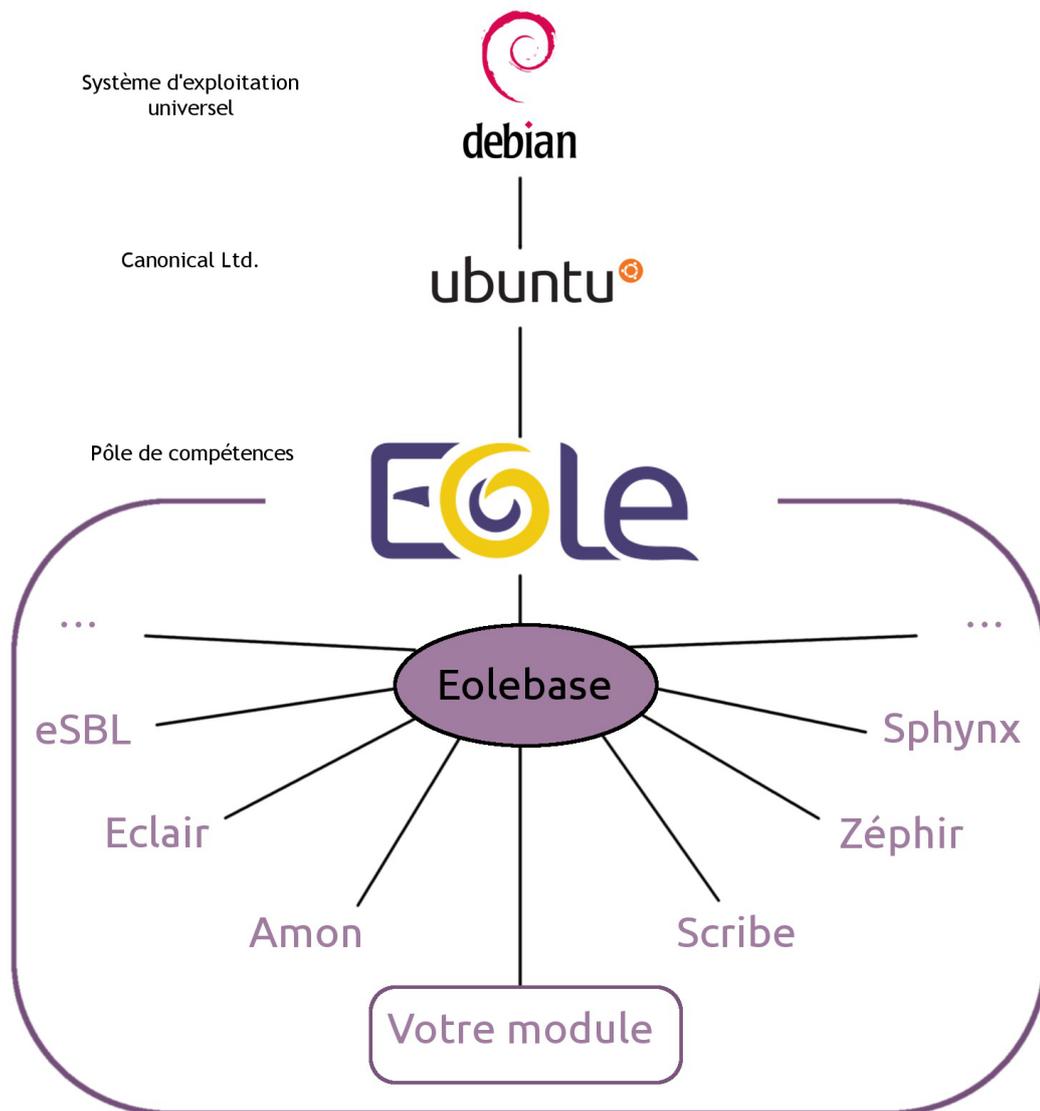
|                 |   |   |   |   |   |
|-----------------|---|---|---|---|---|
| AmonEcoleEclair |   |   |  |   |   |
| Zéphir          |  |  |  |  |  |
| Envole          |   |  |  |   |  |

Tableau des modules par versions d'EOLE

## 4. Eolebase

Comme son nom l'indique, Eolebase est à la base des différents modules EOLE.

Tout en s'appuyant sur la stabilité et les mises à jour de sécurité de la distribution Ubuntu LTS, Eolebase contient les mécanismes techniques qui permettent de réaliser un module EOLE.



Eolebase met à disposition les technologies EOLE pour la création d'un nouveau module personnalisé :

- **l'Installeur** met à disposition une interface simple pour l'installation d'Eolebase ;
- **Creole** est un ensemble d'outils permettant de mettre en œuvre un serveur suivant une configuration définie ;
- **l'Interface de configuration du module** permettra de paramétrer le serveur; les services se configureront avec cette unique interface.

Creole est le cœur de la technologie EOLE.

C'est un ensemble d'outils qui permettent de modifier et/ou d'étendre les fonctionnalités offertes par un module EOLE sans risquer de créer une incohérence avec la configuration par défaut et les futures mises à jour.

Il gère entre autres :

- la personnalisation des options de configuration des modules ;
- le redémarrage des services ;
- l'installation de paquets additionnels ;
- la mise à jour du système.

Pour personnaliser un module, les outils suivants sont à disposition :

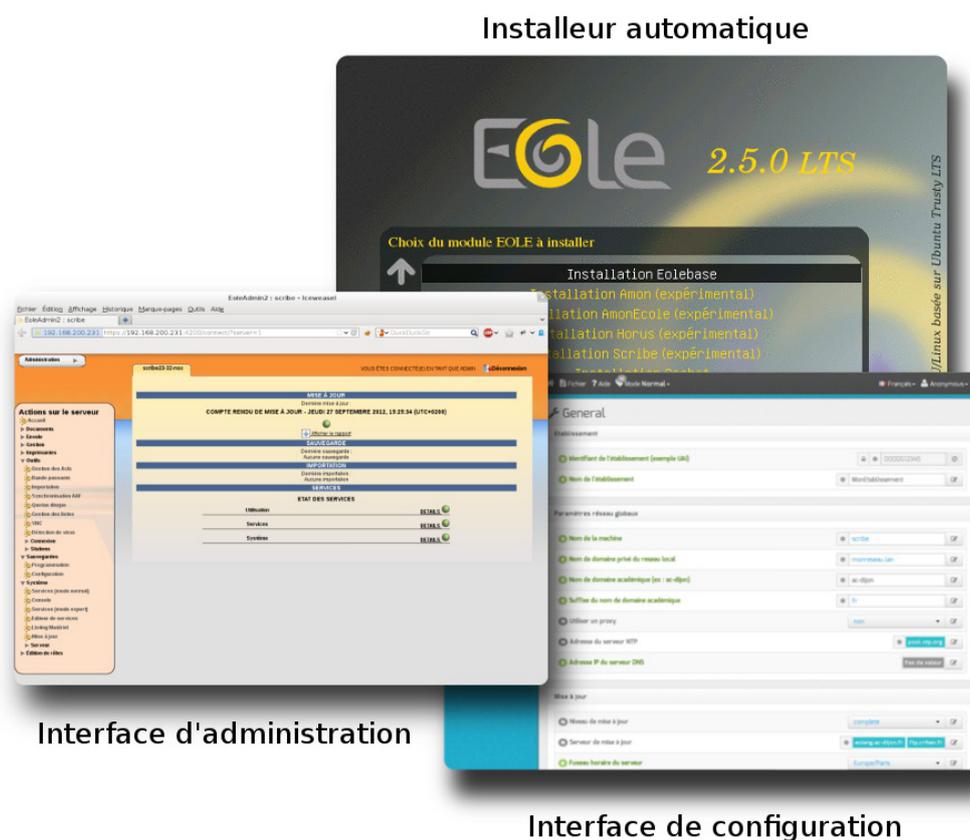
- le **patch** : permettant de modifier les modèles (templates) fournis par EOLE ;
- le **dictionnaire** : permet d'ajouter des options à l'interface de configuration, d'installer de nouveaux paquets ou de gérer de nouveaux services ;
- le **template** : modèle de fichier de configuration qui suivant des choix de configuration sera complété et appliqué au module.

C'est cette technologie qui permet également de construire, à partir d'Eolebase, un nouveau module entièrement personnalisé.

## 5. Les outils EOLE

Tous les modules EOLE mettent à disposition des outils pour faciliter le déploiement, la configuration et l'administration :

- l'**Installeur** met à disposition une interface simple pour choisir le module à installer. Une fois choisi, l'installation du module se déroule sans intervention ;
- l'**Interface de configuration du module** permet de paramétrer le serveur; tous les services se configurent avec cette unique interface ;
- l'**EAD** permet d'administrer le serveur tout au long de son fonctionnement en production.



D'autres outils EOLE spécifiques aux modules sont à disposition : ERA<sup>[p.85]</sup>, Frontend Horus, ARV<sup>[p.83]</sup>, l'application Zéphir.

D'autres interfaces non développées par EOLE sont fournies pour la gestion de certaines données :

PhpMyAdmin, CUPS, etc.

## 6. Les dépôts EOLE

### Architecture des dépôts EOLE

Un miroir des dépôts Ubuntu est disponible à l'adresse suivante :

<http://eole.ac-dijon.fr/ubuntu>

Le miroir propose pour chaque version de la distribution Ubuntu plusieurs catégories de paquets (les fichiers \*.deb) :

- **<version>-backports** : paquets contenant les évolutions fonctionnelles d'une version supérieure d'Ubuntu portées sur une version inférieure ;
- **<version>-proposed** : paquets candidats qui sont éligibles pour passer en version stable après validation totale (dysfonctionnement, régression, etc.) ;
- **<version>-updates** : paquets contenant des mises à jour correctives non critiques ;
- **<version>-security** : paquets contenant des mises à jour de sécurité ;
- **<version>** : paquets de la distribution Ubuntu tels que livrés sur la première image ISO de la version majeure, aucun paquet n'y est ajouté après la publication.

La synchronisation s'effectue chaque nuit.

Les dépôts EOLE 2.5 sont disponibles à l'adresse suivante :

<http://eole.ac-dijon.fr/eole> [<http://eole.ac-dijon.fr/eole>]

Le dépôt propose pour chaque version d'EOLE plusieurs catégories de paquets (les fichiers \*.deb) :

- **eole-2.5-unstable** : paquets de développement pouvant contenir des évolutions fonctionnelles, des corrections de sécurité ou de dysfonctionnement ;
- **eole-2.5-testing** : paquets candidats (correspondant aux images ISO candidates de la distribution) sont éligibles pour passer en version stable après validation totale ;
- **eole-2.5.x-proposed-updates** : paquets candidats qui sont éligibles pour passer en version stable après validation totale (dysfonctionnement, régression, etc.) ;
- **eole-2.5.x-updates** : paquets contenant des mises à jour correctives non critiques ;
- **eole-2.5.x-security** : paquets contenant des mises à jour de sécurité ;
- **eole-2.5.x** : paquets EOLE tels que livrés sur la première image ISO de la version majeure, aucun paquet n'y est ajouté après la publication.

### Politique de publication des paquets

Les mises à jour sont composées de paquets dépendants les uns des autres. Avant toute publication sur le site de référence <http://eole.ac-dijon.fr/eole> et sur les miroirs académiques (ex. : <ftp://ftp.crihan.fr>), les paquets sont copiés sur le dépôt <http://test-eole.ac-dijon.fr>. Ce dépôt est réservé aux développeurs et aux contributeurs. Il permet d'avoir les paquets à disposition tels qu'ils le seront lors de la publication officielle.

Le délai de synchronisation des paquets entre les 2 dépôts varie en fonction du type de paquet :

- **eole-2.5-unstable** : dépôt synchronisé toutes les 15 minutes ;
- **eole-2.5-testing** : dépôt synchronisé toutes les 6 heures ;
- **eole-2.5.x-proposed-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.5.x-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.5.x-security** : synchronisation manuelle avec annonce préalable ;
- **eole-2.5.x** : aucune modification sur ce dépôt.

Les miroirs académiques sont en principe synchronisés toutes les nuits.

## Architectures supportées

Seules les architectures 32 (x86) et 64 bits (x86\_64) sont supportées par Ubuntu et par EOLE. Pour un paquet spécifique à une architecture le nom de celle-ci apparaît dans le nom du paquet :

- **all** : paquets compatibles avec toutes les architectures ;
- **i386** : paquets compilés spécifiquement pour l'architecture i386 ;
- **amd64** : paquets compilés spécifiquement pour l'architecture 64 bits.

## Signature des paquets EOLE

La clé GPG<sup>[p.86]</sup> publique de la clé signant les paquets EOLE est disponible à l'adresse : <http://eole.ac-dijon.fr/eole/project/eole-2.5-repository.key>

# Chapitre 2

## Module eCDL 2.5

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.

### 1. Qu'est ce que le module eCDL ?

Le module eCDL est un contrôleur de domaine de compte Samba 3<sup>[p.89]</sup>.

Il peut être interfacé avec un annuaire LDAP<sup>[p.87]</sup>, 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

### 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.

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

### Services spécifiques au module 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. Structure des conteneurs

Le module eCDL s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Les différences entre les versions 2.4 et 2.5

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

### Noyau

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

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

### Commandes

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

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

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

### Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

`instance` .

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## La sauvegarde

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

## 2.5.1

## Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### 2.5.2.1

#### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 3

## Module eSBL 2.5

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).

### 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

### 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.

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

### Services spécifiques au module 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 base de données ;
- *Bareos* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller le courrier, les partages du serveur et les échanges FTP ;
- *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. Structure des conteneurs

Le module eSBL s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Les différences entre les versions 2.4 et 2.5

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

### Noyau

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

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

### Changement dans le PATH des commandes

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

### Répertoire d'installation du logiciel Nginx

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

### Suppression de la base matériels

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

### Logiciel de sauvegarde

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

### La sauvegarde

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

## 2.5.1

### Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### Gestion des ACLs depuis l'EAD

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

### 2.5.2.1

#### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 4

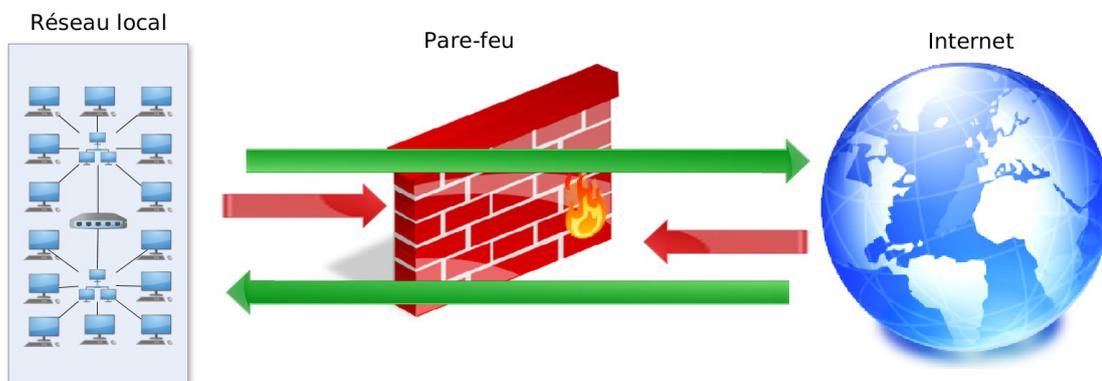
## Module Amon 2.5

Le module Amon est un pare-feu facile à installer et à utiliser. Il permet de faire respecter la politique de sécurité du réseau et 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).

## 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<sup>[p.85]</sup>, est à votre disposition pour effectuer ce travail.

Il est également possible de créer un réseau virtuel privé (RVP<sup>[p.89]</sup>, 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<sup>[p.82]</sup>.



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.

## 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.

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

### Services spécifiques au module Amon

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

## 4. Structure des conteneurs

Le module Amon s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Pré-requis

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

Dans le cadre de la mise en œuvre d'un réseau virtuel privé<sup>[p.89]</sup> entre le serveur Amon et un concentrateur académique (par exemple le module Sphynx), il faut au préalable s'assurer de la compatibilité des logiciels.

### **La compatibilité est assurée par strongSwan**

Actuellement toutes les versions maintenues du module Sphynx fonctionnent avec toutes les versions maintenues du module Amon et inversement.

La compatibilité du module Sphynx avec les versions du module Amon est dépendante de la compatibilité des versions de strongSwan<sup>[p.90]</sup> entre elles. Pour le moment, les versions divergent peu.

Pour vérifier cette compatibilité, il est possible de relever les différentes versions de strongSwan intégrées sur les serveurs concernés et de se rendre sur le site du projet strongSwan : <https://strongswan.org/>.

Ce module fonctionne relativement bien sur de petits serveurs mais l'espace disque, la mémoire et la vitesse du CPU doivent être adaptés au nombre de connexions simultanées.

Les CPU doivent être de préférence en 64 bits.

Le modèle de filtrage est déterminé par le nombre de carte lui-même dépendant de l'utilisation que vous

faites du serveur.

Dans la plupart des cas le module Amon est équipé de 4 cartes réseau :

- réseau extérieur ;
- réseau interne pédagogique ;
- réseau interne administratif ;
- une DMZ<sup>[p.84]</sup>.

L'espace disque et la mémoire RAM sont les ressources les plus critiques, lors d'un partitionnement manuel il faut privilégier la partition `/var` qui contient le plus de données.



Exemple d'usage du module Amon dans un collège. Il y a environ 200 comptes utilisateurs, 140 postes clients et 50 connectés en moyenne. Cette machine est un Intel(R) Xeon(R) CPU X3430 @ 2.40GHz avec 2Go de RAM et 30Go d'espace disque (dont 20 Go sont réservés au `/var` et utilisé à 50%).

## 6. Les différences entre les versions 2.4 et 2.5

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

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

### Noyau

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

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## 2.5.1

### Filtrage avec e2guardian

Le module Amon intègre le logiciel libre e2guardian<sup>[p.84]</sup>. Le logiciel DansGuardian a été complètement abandonné sur le module. Le nombre maximum de processus disponibles pour traiter les nouvelles connexions peut être modifié jusqu'à 8192.

### WPAD

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

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

### Paquet dédié pour le service WPAD d'EOLE

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

### Mode VPN

Le mode VPN database n'est plus supporté et n'est plus disponible sur le module Amon.

### Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### Liste des domaines de destination à ne pas authentifier

La gestion de la liste des domaines de destination à ne pas authentifier est prise en charge dans

l'interface de configuration du module.

## 2.5.2.1

### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 5

## Module Horus 2.5

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

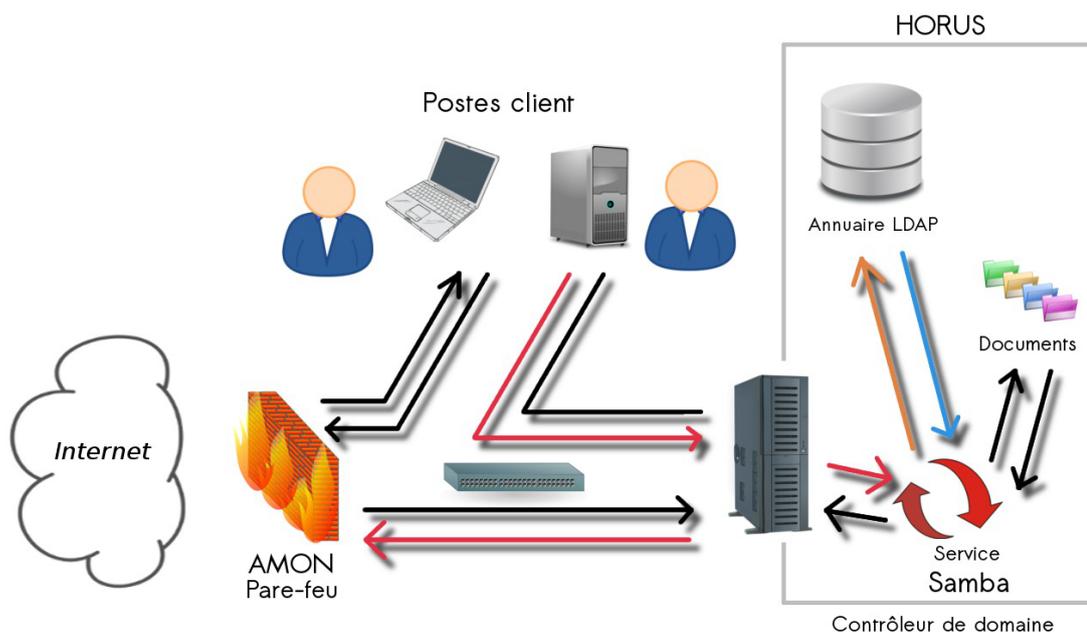
Il est également utilisable dans n'importe quelle autre structure nécessitant un contrôleur de domaine.

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

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

Le contrôleur de domaine permet donc :

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



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

## 1. Qu'est ce que le module Horus ?

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

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

Il peut également se substituer à un contrôleur de domaine NT<sup>[p.83]</sup>, 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<sup>[p.86]</sup>. Il est aussi chargé de la gestion des impressions, et éventuellement d'un service DHCP<sup>[p.84]</sup> pour l'attribution dynamique d'adresse IP.

Depuis plusieurs années, les applications nationales utilisées en Établissement Public Local d'Enseignement<sup>[p.85]</sup> (EPLÉ) sont qualifiées pour fonctionner sur le module Horus :

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



Les applications nationales sont décrites à l'adresse suivante :

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

## Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL<sup>[p.82]</sup> ;
- 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<sup>[p.82]</sup>, CSV<sup>[p.84]</sup>, ...) ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau ;
- un service de messagerie instantanée (standard XMPP<sup>[p.91]</sup>) ;

Serveur web :

- une authentification centralisée ;
- des applications.

Gestion avancée des utilisateurs et des postes clients :

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

## 2. À qui s'adresse ce module ?

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

## 3. Les services Horus

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

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

### Services communs à tous les modules

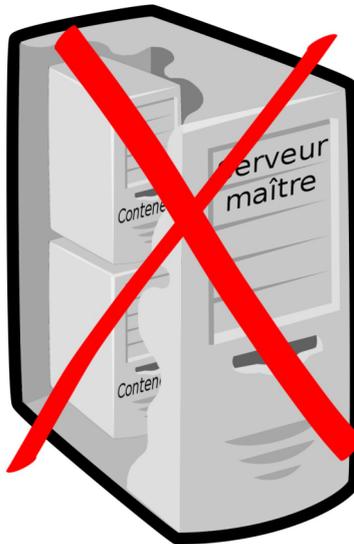
- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;
- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO*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

### Services spécifiques au module Horus

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseau ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL<sup>[p.82]</sup> ;
- *CUPS* : serveur d'impression ;
- *InterBase* : système de gestion de base de données utilisé pour les anciennes applications nationales ;
- *MySQL* : système de gestion de base de données utilisé pour les nouvelles applications nationales ;
- *Bareos* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP.

## 4. Structure des conteneurs

Le module Horus s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Pré-requis

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

Les CPU doivent être de préférence en 64 bits.

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

Le module fonctionne avec une seule carte réseau.

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

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



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

## 6. Les différences entre les versions 2.4 et 2.5

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

### Noyau

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

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

### Commandes

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

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

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

### Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## La sauvegarde

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

## 2.5.1

## ClamAV

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

## Gestion des ACLs depuis l'EAD

L'EAD permet depuis cette version d'appliquer :

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

## Activation du proxy ESU dans les modèles par défaut

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

## Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### Gestion des ACLs depuis l'EAD

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

### Liste des machines

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

### JoinEOLE

JoinEOLE est un utilitaire de jonction au domaine Samba.

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

### Samba

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

### Gestion des bases de données EoleDB

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

## **EoleSSO cluster**

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

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

### **2.5.2.1**

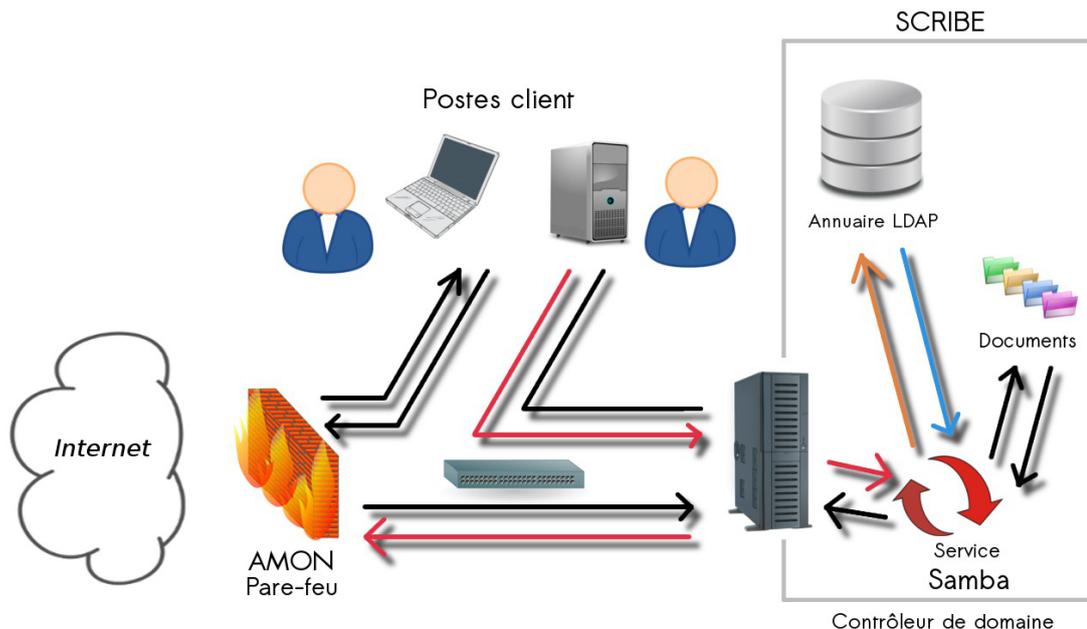
#### **Installation UEFI**

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 6

## Module Scribe 2.5

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.

## 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 toutes les services seront installées sur une seule machine mais séparées grâce à l'usage de conteneurs.

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

système hôte.

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

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

### Principales fonctionnalités

Serveur de fichiers et d'impression :

- contrôleur de domaine ;
- partage de fichiers et de répertoires ;
- support des ACL<sup>[p.82]</sup> ;
- 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<sup>[p.90]</sup>, ONDE<sup>[p.83]</sup>, AAF<sup>[p.82]</sup>, CSV<sup>[p.84]</sup>,... ) ;
- 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<sup>[p.86]</sup> et POP<sup>[p.89]</sup>) ;
- un service de listes de diffusion ;
- un service de messagerie instantanée (standard XMPP<sup>[p.91]</sup>) ;
- une sécurité anti-spam, un anti-virus, une gestion de quotas (taille des boîtes 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).

## 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.

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

### Services spécifiques au module 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<sup>[p.82]</sup> ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de base de données ;
- *Bareos* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;

- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

## 4. Pré-requis

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

Les CPU doivent être de préférence en 64 bits.

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

Le module fonctionne avec une seule carte réseau.

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

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



Exemple d'usage du module Scribe dans une cité scolaire (collège/lycée/BTS). Il y a 2332 comptes utilisateurs, 602 postes clients et 130 connectés en moyenne. Cette machine est un Intel Xeon CPU 3.20GHz avec 8Go de RAM et 1To de disque dur.

## 5. Les différences entre les versions 2.4 et 2.5

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

### Noyau

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

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## La sauvegarde

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

## 2.5.1

### ClamAV

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

### Optimisation du client Scribe

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

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

### Gestion des ACLs depuis l'EAD

L'EAD permet depuis cette version d'appliquer :

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

### Activation du proxy ESU dans les modèles par défaut

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

### Choix du type de partitionnement à l'installation

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

## Montée de version de l'application ecoStations

L'application ecoStations qui permet de gérer l'extinction et l'allumage des postes à des horaires donnés passe en version 2.4.8.

L'ajout d'un script permet notamment d'annuler le re-démarrage d'une station.

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### Gestion des ACLs depuis l'EAD

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

### Liste des machines

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

### JoinEOLE

JoinEOLE est un utilitaire de jonction au domaine Samba.

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

### EOP

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

### AAF

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

### Samba

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

### Gestion des bases de données EoleDB

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

## Envole 5

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

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

## EoleSSO cluster

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

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

## 2.5.2.1

### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 7

## Module Seshat 2.5

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 ou Horus d'une même académie.

### 1. Qu'est ce que le module Seshat ?

Le module Seshat permet la centralisation de la réplication des annuaires des modules Scribe ou Horus d'une académie. Cette réplication des comptes utilisateur et des groupes peut être partielle ou complète.

Le module Seshat permet également la mise en place d'un point d'entrée vers un ENT centralisé et peut être un relai de messagerie.

La fédération des identités et l'authentification unique peuvent se faire entre des modules Scribe/Horus et Seshat mais aussi entre le module Seshat et des services tiers (ARENA<sup>[p.82]</sup>, téléservices, éditeurs, ...).

### 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).

### 3. Les services Seshat

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

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

#### Services communs à tous les modules

- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;

- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO* : gestion de l'authentification centralisée ;
- *Exim4* : serveur de messagerie ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps.

### Services spécifiques au module 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 base de données ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller le courrier électronique ;
- *Apache* : serveur web ;
- *Spamassassin* : anti-spam.

## 4. Structure des conteneurs

Le module Seshat s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Pré-requis

Ce module fonctionne relativement bien sur des petits serveurs.

Les CPU doivent être de préférence en 64 bits.

Le module ne nécessite qu'une carte réseau.

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

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



Pas d'exemple de configuration pour ce module

## 6. Les différences entre les versions 2.3 et 2.5

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.

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

### Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

### 2.5.1

#### Choix du type de partitionnement à l'installation

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

### 2.5.2

#### Mot de passe au 1er redémarrage après installation

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

#### Gestion des bases de données EoleDB

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

#### EoleSSO cluster

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

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

### 2.5.2.1

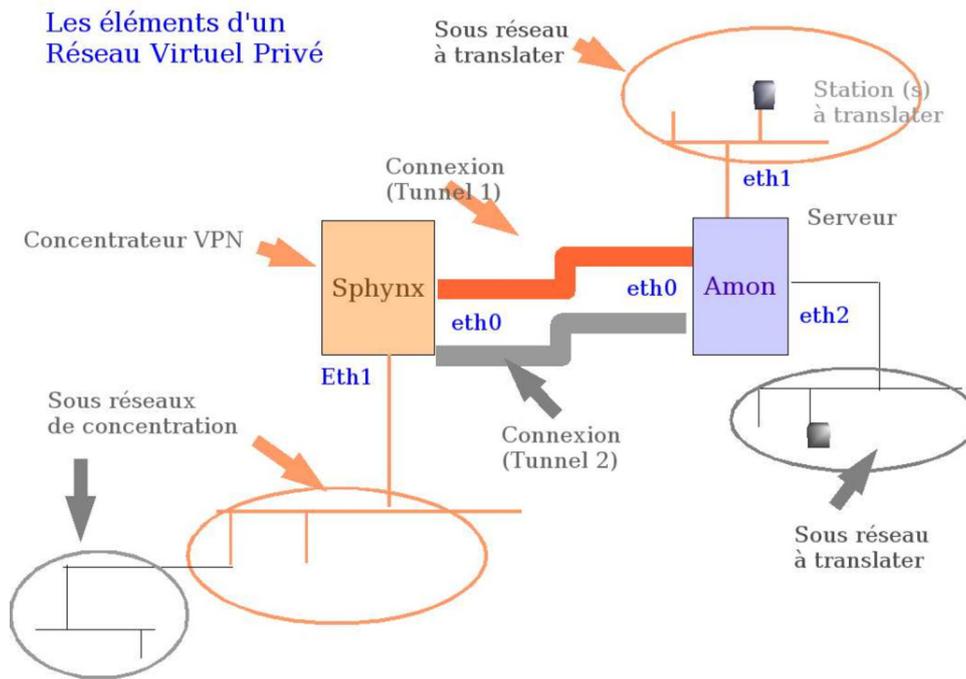
#### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

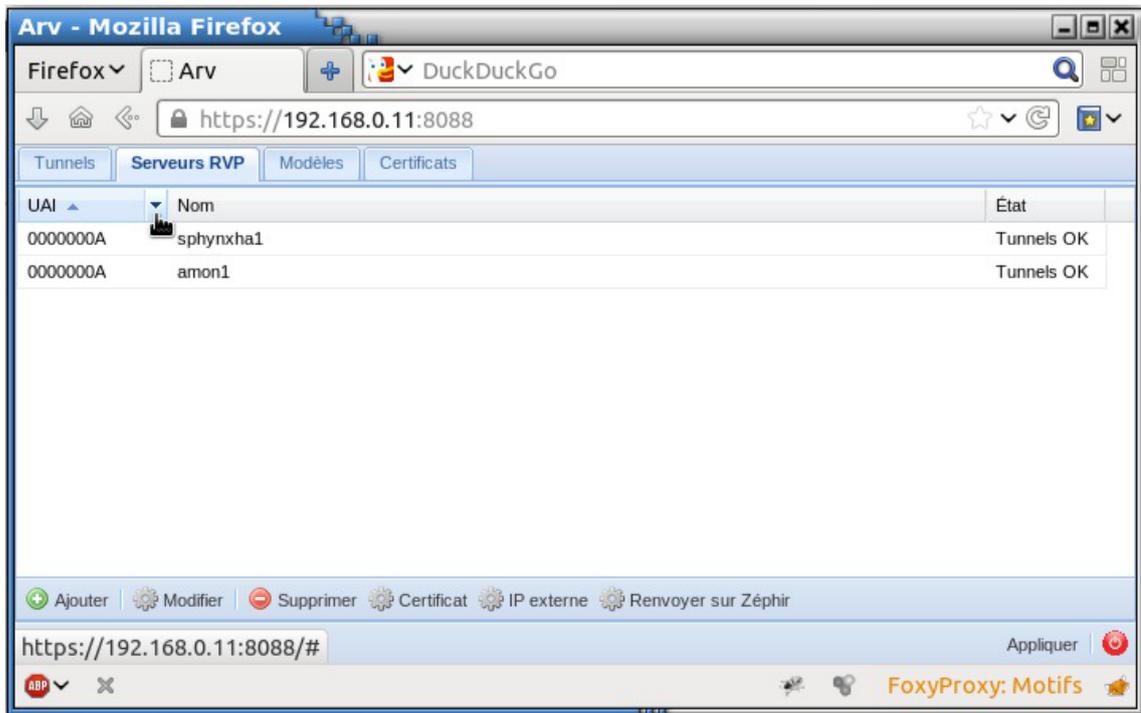
# Chapitre 8

## Module Sphynx 2.5

Le serveur Sphynx est un concentrateur de Réseaux Virtuels Privés (RVP<sup>[p.89]</sup> 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<sup>[p.82]</sup>.



L'outil ARV<sup>[p.83]</sup>, pré-configuré dans le module Sphynx, permet de construire un modèle de configuration RVP. Il permet de générer des configurations RVP pour strongSwan<sup>[p.90]</sup>.



## 1. Qu'est ce que Sphynx ?

Sphynx est un concentrateur de Réseau Virtuel Privé (RVP<sup>[p.89]</sup>). 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<sup>[p.89]</sup> 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<sup>[p.89]</sup> ;
- mise à jour opérée sur le serveur Sphynx au moyen des outils livrés dans la distribution.

## 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. Le RVP pourra alors être monté entre :

- deux modules Sphynx ;
- un module Sphynx et un module Amon ;
- entre un module Sphynx et un serveur gérant IPsec<sup>[p.86]</sup>.

## 3. Les services Sphynx

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

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

### Services communs à tous les modules

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

### Services spécifiques au module 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. Pré-requis

Le module Sphynx nécessite une machine pourvue de 2 cartes réseau.

Une troisième carte est obligatoire pour l'activation de la haute disponibilité<sup>[p.86]</sup>.

Le module n'utilise que très peu de ressources.

### 💡 La compatibilité est assurée par strongSwan

Actuellement toutes les versions maintenues du module Sphynx fonctionnent avec toutes les versions maintenues du module Amon et inversement.

La compatibilité du module Sphynx avec les versions du module Amon est dépendante de la compatibilité des versions de strongSwan<sup>[p.90]</sup> entre elles. Pour le moment, les versions divergent peu.

Pour vérifier cette compatibilité, il est possible de relever les différentes versions de

strongSwan intégrées sur les serveurs concernés et de se rendre sur le site du projet strongSwan : <https://strongswan.org/>.

## 5. Structure des conteneurs

Le module Sphynx s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 6. Les différences entre les versions 2.4 et 2.5

Le module Sphynx n'est disponible qu'à partir de la version 2.5.2 d'EOLE.

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

### Noyau

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

### Mise à jour

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

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

## Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## La sauvegarde

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

## 2.5.1

### Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

## Haute disponibilité

La configuration de la haute disponibilité a été simplifiée, des variables spécifiques à ce module ont été ajoutées pour permettre un calcul automatique des variables Pacemaker.

## Mode VPN

Le mode VPN database n'est plus supporté et n'est plus disponible sur le module Sphynx. Un serveur Sphynx en mode fichier plat continuera à communiquer avec des serveurs distants configurés en mode database. La transition pourra se faire progressivement.

## 2.5.2.1

### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 9

## Module Thot 2.7

Le module Thot est un module expérimental<sup>[p.85]</sup>, il peut rester des dysfonctionnements, les contours du module ne sont pas complètement établis.

Le module Thot permet de mettre en place un annuaire centralisé.

### 1. Qu'est ce que le module Thot ?

Le module Thot permet de mettre en place un annuaire centralisé respectant les préconisations du Schéma Directeur des Espaces numériques de Travail, dans sa version 4.1 (SDET 4.1<sup>[p.89]</sup>), défini par le ministère de l'Éducation nationale.

Il est principalement alimenté par les fichiers XML<sup>[p.90]</sup> exportés de l'annuaire académique fédérateur (AAF<sup>[p.82]</sup>).

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

La procédure d'alimentation actuelle fonctionne de la façon suivante :

1. lecture de fichiers XML<sup>[p.90]</sup> exportés depuis AAF<sup>[p.82]</sup> complets ou delta
2. stockage des informations dans la base de données MySQL du module
3. initialisation et/ou mise à jour de l'annuaire OpenLDAP local

#### Principales fonctionnalités

Annuaire :

- l'annuaire est initialisé à partir d'importation de comptes AAF<sup>[p.82]</sup> ;
- l'annuaire peut servir de base d'authentification pour d'autres services réseau.

### 2. À qui s'adresse ce module ?

Le module Thot répond au besoin de centraliser l'alimentation et la gestion des annuaires des établissements scolaires.

De ce fait il s'adresse principalement aux services académiques mais peut également intéresser les collectivités pour la mise en place d'un annuaire de type ENT<sup>[p.85]</sup>.

## 3. Les services Thot

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

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

### Services communs à tous les modules

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

### Services spécifiques au module Thot

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

## 4. Pré-requis

Il n'y a pas de pré-requis matériel particulier pour ce module.

Un serveur standard avec une carte réseau suffit. Il faut malgré tout privilégier la mémoire vive plutôt que les cœurs. En effet l'importation et les mises à jour nécessitent beaucoup de mémoire.

Dans le cas d'un partitionnement manuel il faut privilégier plus d'espace pour le répertoire `/var` qui accueille les bases de données et l'annuaire.

## 5. Les différences entre les versions 2.4 et 2.5

Le module Thot est expérimental<sup>[p.85]</sup> et n'est disponible qu'à partir de la version 2.4 d'EOLE.

## Mise à jour

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

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

## Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

### Mode conteneur

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

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

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

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

### Changement dans le PATH des commandes

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

### Répertoire d'installation du logiciel Nginx

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

### Suppression de la base matériels

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

### Logiciel de sauvegarde

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

### La sauvegarde

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

## 2.5.1

### Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### 2.5.2.1

## Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 10

## Module Zéphir 2.5

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.

Parmi d'autres fonctionnalités le module Zéphir permet :

- Gestion centralisée des configurations
  - Adaptations sous forme de variantes
  - Gestion par groupes
  - Préparation de la migration
- Surveillance des serveurs inscrits
  - État du système et des services
  - Alertes par courrier électronique
- Envoi de fichiers et exécution d'actions à distance.
- Fonctions spécifiques à certains modules : ARV, Seshat,...

### 1. Qu'est ce que le module Zéphir ?

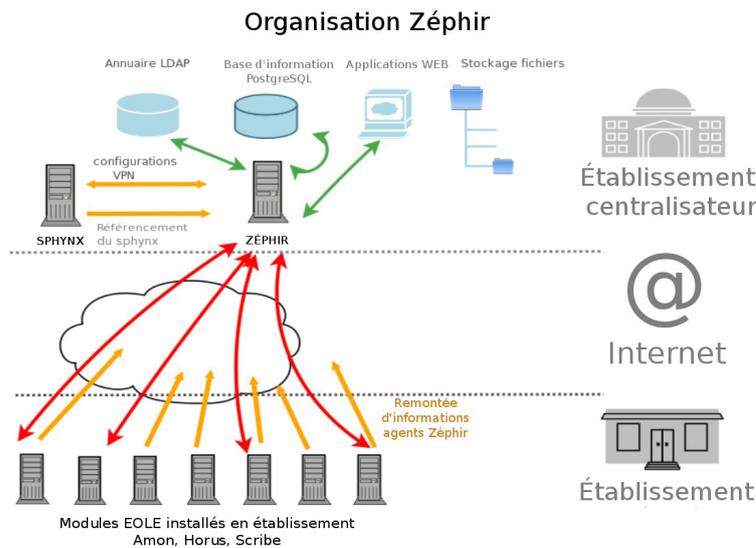
Le module Zéphir permet de déployer et gérer un parc de serveurs. Il héberge une base de données des établissements et des serveurs installés dans ces établissements. Cette base de données peut être pré-initialisée à partir du fichier national des établissements. L'ensemble constitue un inventaire de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



Organisation du module Zéphir

### 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.

## 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.

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

### Services spécifiques au module 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. Structure des conteneurs

Le module Zéphir s'installe par défaut en mode non conteneur<sup>[p.83]</sup>.



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

## 5. Pré-requis

Le module sert à la surveillance et à la gestion à distance des modules EOLE.

La puissance de la machine est dépendante du nombre de serveurs à gérer.

Le cache des configurations étant activé par défaut, la mémoire RAM doit être privilégiée, elle dépend du nombre de serveurs à administrer. Il est recommandé d'avoir 4 Go pour environ 400/500 serveurs et au moins 8 Go au delà.

Les fonctionnalités du module demandent une bonne bande passante.

Le module héberge une base de donnée, il est souhaitable de favoriser une machine physique si le nombre de clients est important.

L'espace disque n'est pas la ressource la plus critique, par contre lors d'un partitionnement manuel il faut privilégier la partition `/var` qui contient le plus de données :

- les configurations et les fichiers personnalisés des serveurs ;
- la base de données ;
- les statistiques des serveurs ;
- les logs.



Un module Zéphir qui gère 600 serveurs utilise 20 Go d'espace disque dont une partition `/var` de plus de 7 Go. 8 Go de mémoire RAM sont nécessaires.

Le module Zéphir doit être accessible par les clients en SSH<sup>[p.90]</sup>.

## 6. Les différences entre les versions 2.3 et 2.5

Le module Zéphir est un portage fonctionnel du module Zéphir 2.3.

Dans cette version, Zéphir prend en charge les modules EOLE dans les versions 2.3, 2.4 et 2.5.

Le module comporte quelques évolutions mineures :

- la gestion des thèmes a été améliorée ;
- ajout d'un délai pour lancer certaines actions (le délai est pris en compte après la prochaine connexion du client).

Pour la gestion des modules 2.4 et 2.5 :

- nouveau mode de gestion des dictionnaires ;
- l'édition de la configuration d'un module dans l'application web Zéphir se fait maintenant au travers de la nouvelle interface de configuration du module (intégration de la version gen\_config 2.4/2.5).



Les versions 2.5 du module Zéphir ne prennent pas en charge les modules 2.6. D'une manière générale le serveur Zéphir ne gère pas de versions supérieures à lui-même. Si cette fonctionnalité existait dans la version 2.3 elle n'est pas possible à implémenter dans Zéphir 2.5 car des changements dans Creole et un changement de version de Tiramisu sur les versions EOLE 2.6 ne le permettent pas.

### Mise à jour

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

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

### Passage à une nouvelle version

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

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

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

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

### Commandes

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

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

Un fichier `config.eol.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de

la reconfiguration du serveur. Celui-ci permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## Paquet dédié pour le service PostgreSQL d'EOLE

Un paquet nommé `eole-postgresql` est nouvellement dédié pour gérer PostgreSQL.

### 2.5.1

#### Choix du type de partitionnement à l'installation

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

### 2.5.2

#### Mot de passe au 1er redémarrage après installation

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

#### 2.5.2.1

##### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Chapitre 11

## Module AmonEcole 2.5

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.

### 1. Qu'est ce que le module AmonEcole ?

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

Grâce à LXC toutes les services seront installées sur une seule machine mais séparées grâce à l'usage de conteneurs.

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

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

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

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

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

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

Vous pouvez les utiliser tels quels ou bien les modifier à votre convenance. Un outil spécifique, ERA<sup>[p.85]</sup>, 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<sup>[p.82]</sup>.

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<sup>[p.82]</sup> ;
- 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<sup>[p.90]</sup>, ONDE<sup>[p.83]</sup>, AAF<sup>[p.82]</sup>, CSV<sup>[p.84]</sup>,... ) ;
- 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<sup>[p.91]</sup>) ;
- 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).



Ce module est fourni exclusivement en mode conteneur.

## 2. À qui s'adresse ce module ?

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

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

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

## 3. Les services AmonEcole

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

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

### Services communs à tous les modules

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

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

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

### Services spécifiques au module Amon

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

### Services spécifiques au module Scribe

- *OpenLDAP* : service d'annuaire centralisant les utilisateurs et pouvant servir de base pour l'authentification d'autres services réseaux ;
- *Samba* : serveur de fichiers permettant le partage de fichiers et répertoires, d'imprimantes, la gestion des droits utilisateur, des comptes ainsi que des accès, des quotas disque et des ACL<sup>[p.82]</sup> ;
- *CUPS* : serveur d'impression ;
- *MySQL* : système de gestion de base de données ;
- *Bareos* : logiciel de sauvegarde ;
- *ProFTPD* : serveur FTP, il permet aux utilisateurs d'accéder à leurs fichiers via ce protocole ;
- *ClamAV* : anti-virus, il peut être activé pour surveiller le courrier, les partages du serveur et les échanges FTP ;
- *dhcp3-server* : serveur DHCP ;
- *tftpd-hpa* : serveur TFTP ;
- *Apache* : serveur web ;
- *Courier* : gestion du courrier électronique ;
- *Sympa* : gestionnaire de listes de diffusion ;
- *Jabber* : serveur de messagerie instantanée
- *Spamassassin* : anti-spam.

## 4. Les conteneurs du module AmonEcole

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

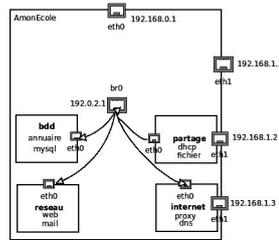


Schéma des conteneurs du module AmonEcole, exemple d'adresses IP proposées par défaut

Deux conteneurs ont une adresse IP sur le réseau eth1 :

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

## 5. Pré-requis

Ce module fonctionne relativement bien sur des petits serveurs.

Les CPU doivent être de préférence en 64 bits.

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

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

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

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



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

## 6. Les différences entre les versions 2.4 et 2.5

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

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

### Noyau

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

### Mise à jour

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

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

## Passage à une nouvelle version

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

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

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

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

## Commandes

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

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

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

## Interface de configuration du module

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

- Flask<sup>[p.85]</sup> ;
- Backbone.js<sup>[p.83]</sup> et Marionette<sup>[p.88]</sup> ;
- Tiramisu<sup>[p.90]</sup>.

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

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

## Règles pare-feu

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

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

## Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu<sup>[p.90]</sup>.

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML<sup>[p.90]</sup> Creole extra. Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet associé ce qui est à la fois plus simple et plus sûr.

## Mode conteneur

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

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

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

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

## Changement dans le PATH des commandes

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

## Répertoire d'installation du logiciel Nginx

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

## Suppression de la base matériels

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

## Logiciel de sauvegarde

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

## La sauvegarde

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

## 2.5.1

### Filtrage avec e2guardian

Le module Amon intègre le logiciel libre e2guardian<sup>[p.84]</sup>. Le logiciel DansGuardian a été complètement abandonné sur le module. Le nombre maximum de processus disponibles pour traiter les nouvelles connexions peut être modifié jusqu'à 8192.

### WPAD

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

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

### Paquet dédié pour le service WPAD d'EOLE

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

### ClamAV

À partir de la version 2.5.1, l'antivirus temps réel ClamAV est activé par défaut et utilisé pour le FTP et la

messagerie mais est désactivé sur les partages Samba.

### Optimisation du client Scribe

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

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

### Gestion des ACLs depuis l'EAD

L'EAD permet depuis cette version d'appliquer :

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

### Activation du proxy ESU dans les modèles par défaut

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

### Choix du type de partitionnement à l'installation

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

## 2.5.2

### Mot de passe au 1er redémarrage après installation

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

### Gestion des ACLs depuis l'EAD

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

### Liste des machines

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

### JoinEOLE

JoinEOLE est un utilitaire de jonction au domaine Samba.

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

### EOP

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

## AAF

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

## Samba

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

## Gestion des bases de données EoleDB

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

## Envole 5

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

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

### 2.5.2.1

#### Installation UEFI

L'image ISO EOLE 2.5.2.1 intègre le support de l'UEFI<sup>[p.90]</sup>.

# Glossaire

|   |   |
|---|---|
| <p><b>AAF</b><br/>= <i>Annuaire Académique Fédérateur</i></p>   | <p>L'annuaire fédérateur est un dispositif technique qui sert à alimenter l'annuaire LDAP d'un rectorat avec les autres annuaires académiques qui existent au sein de l'Éducation nationale et qui sont directement utilisés par les applications du ministère et des collectivités.</p>  |
| <p><b>ACL</b><br/>= <i>Access Control List</i></p>  | <p>Le terme ACL désigne deux choses en sécurité informatique :</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.</li> </ul>   |
| <p><b>AGRIATES</b><br/>= <i>Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires</i></p> | <p>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.</p> <p>RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissements et leur rectorat de rattachement.</p> <p>L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE.</p> <p><a href="http://www.igc.education.fr/agriates/agriates.htm">http://www.igc.education.fr/agriates/agriates.htm</a></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.</p> |

|  |  |
|--|--|
| <p><b>ARENA</b><br/>= Accès aux Ressources de l'Éducation Nationale et Académiques</p> | <p>Les portails d'applications ARENA vous donnent accès aux applications en ligne du ministère de l'Éducation nationale et de l'Académie.</p>  |
| <p><b>ARV</b><br/>= Administration de Réseaux Virtuels</p>                             | <p>ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan.<br/><a href="http://www.strongswan.org/">http://www.strongswan.org/</a></p>  |
| <p><b>Backbone.js</b></p>  | <p>Backbone est une bibliothèque JavaScript avec une interface RESTful JSON et est basée sur le modèle-vue-contrôleur (MVC). Cette bibliothèque est connue pour être légère, comme sa seule dépendance avec la bibliothèque JavaScript Underscore.js. Elle est conçue pour développer des applications web d'une seule page et permet de maintenir les différentes parties d'applications Web (par exemple, les clients multiples et le serveur) synchronisée. Backbone a été créé par Jeremy Ashkenas, qui est également connu pour CoffeeScript.<br/><a href="http://backbonejs.org/">http://backbonejs.org/</a></p>   |
| <p><b>BE1D</b><br/>= Base Élèves 1er Degré</p>   | <p>L'application informatique "Base élèves premier degré" permet la gestion administrative et pédagogique des élèves de la maternelle au C.M.2 dans les écoles publiques ou privées. Elle facilite la répartition des élèves dans les classes et le suivi des parcours scolaires et améliore le pilotage académique et national.<br/><a href="http://www.education.gouv.fr/cid24413/base-eleves-premier-degre.html">http://www.education.gouv.fr/cid24413/base-eleves-premier-degre.html</a><br/>En 2017 l'application BE1D fait l'objet d'une refonte complète et devient ONDE (Outil Numérique pour la Direction d'École).<br/><a href="http://eduscol.education.fr/cid113087/refonte-de-l-application-base-elev">http://eduscol.education.fr/cid113087/refonte-de-l-application-base-elev</a></p> |
| <p><b>Conteneur</b><br/>= LXC</p>  | <p>Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés.<br/>Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.</p>   |

|   |   |
|---|---|
| <p><b>Contrôleur de domaine NT</b></p>                              | <p>Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire.</p> <p>Chez Microsoft, un domaine est une entité logique vue comme une enveloppe étiquetée. Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "ADMINISTRATIF" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service administratif, et les comptes utilisateur qui sont autorisés à s'y connecter.</p> <p>Le domaine permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données.</p> <p>Cette base de données est stockée sur des serveurs particuliers (Windows Server NT4, 2000, 2003), appelés Contrôleurs de Domaine.</p> |
| <p><b>CSV</b><br/>= <i>Comma-separated values</i></p>               | <p>Le CSV est un format informatique ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules. Il est souvent utilisé pour l'interopérabilité entre applications.</p>   |
| <p><b>DHCP</b><br/>= <i>Dynamic Host Configuration Protocol</i></p> | <p>Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.</p>   |
| <p><b>DMZ</b><br/>= <i>Demilitarized Zone</i></p>                   | <p>En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.</p> <p>Source Wikipédia : <a href="http://fr.wikipedia.org/wiki/Zone_démilitarisée">http://fr.wikipedia.org/wiki/Zone démilitarisée</a> (informatique)</p>  |

|   |  |
|---|--|
| <p><b>e2guardian</b></p>  | <p>e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie.</p> <p>Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian.</p> <p><a href="http://e2guardian.org">http://e2guardian.org</a></p> |
| <p><b>ENT</b><br/>= <i>Espace Numérique de Travail</i></p>                | <p>L'ENT est un ensemble intégré de services numériques, choisi, organisé et mis à disposition de la communauté éducative par l'établissement scolaire. Techniquement parlant c'est un ensemble de services en ligne, personnalisés et sécurisés.</p> <p><a href="http://eduscol.education.fr/cid55726/qu-est-ent.html">http://eduscol.education.fr/cid55726/qu-est-ent.html</a></p>   |
| <p><b>EPLE</b><br/>= <i>Établissement Public Local d'Enseignement</i></p> | <p>En France, un établissement public local d'enseignement (EPL) est un établissement scolaire d'enseignement secondaire (ou, exceptionnellement, primaire) :</p> <ul style="list-style-type: none"> <li>• collège</li> <li>• lycée d'enseignement général et technologique (LGT)</li> <li>• lycée professionnel (LP)</li> <li>• établissement régional d'enseignement adapté (EREA)</li> <li>• école régionale du premier degré (ERPD)</li> </ul>   |
| <p><b>ERA</b><br/>= <i>Éditeur de Règles pour le module Amon</i></p>      | <p>ERA est une application graphique de génération et de gestion de règles de sécurité adaptée au module pare-feu Amon. À partir du fichier XML de description du pare-feu, un script de règles iptables pour Netfilter est généré de manière à implémenter ces règles sur le module pare-feu Amon. La génération directe de règles iptables est également possible, permettant d'utiliser ERA pour d'autres types de serveurs sous GNU/Linux.</p>   |
| <p><b>Expérimental</b><br/>= <i>Test, preuve de concept,</i><br/>...</p>  | <p>Expérimental signifie que le périmètre du développement n'est pas clairement défini et qu'il relève plutôt de la preuve de concept. Son comportement n'est pas forcément le comportement définitif, d'ailleurs il peut très bien ne pas aboutir.</p>  |

|  |  |
|--|--|
| <p><b>Flask</b></p>  | <p>Flask est un framework d'application web léger écrit en Python et basé sur le toolkit Werkzeug (une librairie Python WSGI) et sur le moteur de template Jinja2.</p> <p>Flask est appelé microframework parce qu'il garde un cœur simple, mais extensible. Il n'y a aucune couche d'abstraction de données, pas de formulaire de validation ou tout autre composant que des bibliothèques tierces ne traitent déjà. Cependant, Flask supporte les extensions, ce qui permet d'ajouter des fonctionnalités si elles sont mises en œuvre dans Flask lui-même.</p> <p>Il existe des extensions pour utiliser les objets relationnels, valider des formulaires, le téléchargement, diverses technologies d'authentification ouvertes, et plus encore.</p> <p>Flask est sous licence BSD.</p> <p><a href="http://flask.pocoo.org/">http://flask.pocoo.org/</a></p>  |
| <p><b>GPG</b><br/>= <i>GnuPG</i></p>                                   | <p>GPG est l'implémentation GNU du standard OpenPGP.</p> <p>OpenPGP est un format pour l'échange sécurisé de données.</p> <p><a href="http://fr.wikipedia.org/wiki/GNU_Privacy_Guard">http://fr.wikipedia.org/wiki/GNU_Privacy_Guard</a></p>   |
| <p><b>Haute Disponibilité</b><br/>= <i>High Availability ou HA</i></p> | <p>La haute disponibilité c'est garantir la disponibilité et le bon fonctionnement d'un service ou d'une architecture informatique.</p> <p>Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité :</p> <ul style="list-style-type: none"> <li>• la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle. Est alors créé un cluster de haute-disponibilité (par opposition à un cluster de calcul) : une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités ;</li> <li>• la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur. ITIL contient de nombreux processus de ce type.</li> </ul> <p>Source Wikipédia : <a href="http://fr.wikipedia.org/wiki/Haute_disponibilité">http://fr.wikipedia.org/wiki/Haute_disponibilité</a></p> |
| <p><b>IMAP</b><br/>= <i>Internet Message Access Protocol</i></p>       | <p>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.</p>  |
| <p><b>InterBase</b></p>  | <p>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).</p> <p>Source Wikipédia : <a href="http://fr.wikipedia.org/wiki/InterBase">http://fr.wikipedia.org/wiki/InterBase</a></p>   |

|   |   |
|---|---|
| <b>IPsec</b><br><i>= Internet Protocol Security</i>           | IPsec est un standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques. IPsec offre des services d'authentification, de contrôle d'intégrité et de confidentialité en s'appuyant sur un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.<br>Source Wikipédia : <a href="http://fr.wikipedia.org/wiki/Internet_Protocol_Security">http://fr.wikipedia.org/wiki/Internet Protocol Security</a> |
| <b>LDAP</b><br><i>= Lightweight Directory Access Protocol</i> | À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.   |

**LTS**

= *Long Term Support*

Certaines versions d'Ubuntu sont estampillées LTS. Ces versions, publiées tous les deux ans au mois d'avril, sont soutenues pour une durée prolongée de 60 mois (5 ans).

Le label LTS :

- la récupération des paquets de Debian se fait de manière plus conservatrice, synchronisée depuis Debian testing plutôt que Debian unstable ;
- la stabilisation de la distribution commence tôt dans le cycle de développement en limitant le nombre de nouveautés. L'équipe d'Ubuntu fait une sélection entre les paquets qui doivent être inclus dans une distribution maintenue sur une durée d'au plus 5 ans et ceux qui pourront être optionnellement installés par les utilisateurs ;
- les changements structurels majeurs sont le plus possible évités, comme le changement des applications incluses par défaut dans la distribution, la transition vers d'autres bibliothèques ou les changements des couches basses du système.

Une version LTS est :

- tournée vers les entreprises : ces versions sont pensées pour le déploiement dans des parcs de serveurs et de postes de travail dont la durée de vie est longue et où les changements sont peu fréquents ;
- compatible avec les nouveaux matériels : des révisions sont publiées à intervalles réguliers (une point release) pour ajouter la prise en charge de nouveaux matériels pour serveurs et postes de travail ;
- davantage testée : la phase de développement alpha est réduite, afin d'étendre davantage la période de stabilisation bêta pour récolter le plus de retours d'expérience et de rapports de bogues et pour stabiliser l'ensemble de la distribution.

Clairement, une version LTS n'est pas :

- une version incluant de nombreuses nouveautés : l'effort est surtout tourné vers la stabilisation et le renforcement des fonctionnalités existantes. Si des exceptions sont accordées à certains projets, elles sont documentées et leur intégration dans une version LTS doit être complétée pour la version bêta 1 du cycle de développement ;
- une version d'avant-garde : plutôt que d'importer les paquets de Debian depuis sa version unstable, ceux-ci sont tirés depuis la version testing de Debian. Même si certaines nouveautés ne sont pas incluses dans ces paquets, il y a plus de bénéfices à importer des paquets testés qui introduisent moins de bogues et moins de régressions.

|   |  |
|---|--|
| <b>Marionette</b>   | <p>Marionette simplifie le code applicatif Backbone grâce à des vues robustes et des solutions d'architecture.</p> <p><a href="http://marionettejs.com/">http://marionettejs.com/</a></p>  |
| <b>PKI</b><br><i>= Public Key Infrastructure</i>  | <p>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.</p> <p>En résumé, ces services sont les suivants :</p> <ul style="list-style-type: none"> <li>• enregistrement des utilisateurs (ou équipement informatique) ;</li> <li>• génération de certificats ;</li> <li>• renouvellement de certificats ;</li> <li>• révocation de certificats ;</li> <li>• publication de certificats ;</li> <li>• publication des listes de révocation (comprenant la liste des certificats révoqués) ;</li> <li>• identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'ICP) ;</li> <li>• archivage, séquestre et recouvrement des certificats (option).</li> </ul> <p>Source de la définition :<br/> <a href="http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_public">http://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_public</a></p> |
| <b>POP</b><br><i>= Post Office Protocol</i>   | <p>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.</p>  |
| <b>Réseau virtuel Privé</b><br><i>= RVP ou VPN (Virtual Private Network) en anglais</i> | <p>Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.</p>  |
| <b>Samba</b><br><i>= SaMBa : Server Message Block</i>                                   | <p>Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du protocole SMB, protocole standard de Microsoft.</p> <p>À partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Windows Server, soit en tant que contrôleur de domaine principal (PDC) ou en tant que membre d'un domaine. Il peut également faire partie d'un domaine Active Directory.</p>  |

|   |  |
|---|--|
| <p><b>SDET</b><br/>= <i>Schéma Directeur des Espaces Numériques de Travail</i></p>  | <p>Le Schéma Directeur des Espaces Numériques de Travail (SDET) regroupe les grandes orientations de l'éducation nationale pour ses espaces numériques de travail. Il permet de définir les services attendus et leurs préconisations techniques.<br/>Pour plus d'informations consultez la page :<br/><a href="http://eduscol.education.fr/pid25719/schema-directeur-des-ent-sdet.htm">http://eduscol.education.fr/pid25719/schema-directeur-des-ent-sdet.htm</a></p>   |
| <p><b>SIECLE anciennement Sconet</b><br/>= <i>Système d'information pour les élèves en collèges et lycée et pour les établissements</i></p> | <p>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).</p>   |
| <p><b>SSH</b><br/>= <i>Secure Shell</i></p>   | <p>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.</p>  |
| <p><b>strongSwan</b></p>  | <p>strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x).<br/>L'objectif de ce projet est de proposer des mécanismes d'authentification forts.<br/><a href="http://www.strongswan.org/">http://www.strongswan.org/</a></p>   |
| <p><b>Tiramisu</b><br/>= <i>Outil de gestion de configuration</i></p>   | <p>À cause de l'afflux de plus en plus grand des options de configuration des serveurs EOLE (plus de 1600 au dernier recensement), il était devenu de plus en plus difficile de correctement récupérer les options et de les utiliser là où elles devaient effectivement être employées.<br/>Pour remédier à ces difficultés, l'outil Tiramisu a été développé, il est utilisé comme moteur du générateur de configuration de la version EOLE 2.4.<br/>La documentation technique du projet :<br/><a href="http://tiramisu.labs.libre-entreprise.org">http://tiramisu.labs.libre-entreprise.org</a><br/>Les sources du projet Tiramisu :<br/><a href="http://labs.libre-entreprise.org/projects/tiramisu/">http://labs.libre-entreprise.org/projects/tiramisu/</a></p> |
| <p><b>UEFI</b><br/>= <i>Unified Extensible Firmware Interface</i></p>   | <p>Le standard UEFI définit un logiciel intermédiaire entre le micrologiciel (firmware) et le système d'exploitation (OS) d'un ordinateur. Cette interface succède sur certaines cartes-mères au BIOS. Elle fait suite à EFI (Extensible Firmware Interface), conçue par Intel pour les processeurs Itanium.<br/>Source Wikipédia :<br/><a href="https://fr.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface">https://fr.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface</a></p>  |

|  |   |
|--|---|
| <p><b>XML</b><br/>= <i>Extensible Markup Language</i></p>                  | <p>L'Extensible Markup Language ( « langage de balisage extensible » en français) est un langage informatique de balisage générique qui dérive du SGML. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG... Elle est reconnaissable par son usage des chevrons (&lt; &gt;) encadrant les balises. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche...) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés une application XML respecte généralement certains principes :</p> <ul style="list-style-type: none"> <li>• la structure d'un document XML est définie et validable par un schéma,</li> <li>• un document XML est entièrement transformable dans un autre document XML.</li> </ul> <p>Source : <a href="http://fr.wikipedia.org/wiki/XML">http://fr.wikipedia.org/wiki/XML</a></p> |
| <p><b>XMPP</b><br/>= <i>Extensible Messaging and Presence Protocol</i></p> | <p>XMPP peut être traduit par « Protocole extensible de présence et de messagerie »), et est un ensemble de protocoles standards ouverts de l'Internet Engineering Task Force (IETF) pour la messagerie instantanée, et plus généralement une architecture décentralisée d'échange de données.</p> <p>XMPP est également un système de collaboration en quasi-temps-réel et d'échange multimédia via le protocole Jingle, dont la Voix sur réseau IP (téléphonie sur Internet), la visioconférence et l'échange de fichiers sont des exemples d'applications.</p> <p>XMPP est constitué d'un protocole TCP/IP basé sur une architecture client-serveur permettant les échanges décentralisés de messages instantanés ou non, entre clients, au format Extensible Markup Language (XML).</p> <p>XMPP est en développement constant et ouvert au sein de l'IETF.</p>  |