

Installation et mise en œuvre du module Amon

EOLE 2.5.2



EOLE 2.5.2

Version : révision : Avril 2018

Date : création : Mai 2015

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

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

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

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

Vous êtes libres :

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

Selon les conditions suivantes :

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

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

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

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

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

EOLE est un projet libre (Licence GPL).

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

Pour toute information concernant ce projet vous pouvez nous joindre :

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

Table des matières

Chapitre 1 - Présentation et historique du projet EOLE	9
1. Les objectifs d'EOLE	9
2. Historique du projet EOLE	9
3. Logiciel Libre	14
4. Méta-distribution EOLE	15
5. EOLE 2.5	17
6. Modules supportés disponibles	19
7. Eolebase	21
8. Quelques références	23
Chapitre 2 - Introduction au module Amon	24
1. Qu'est ce que le module Amon ?	24
2. À qui s'adresse ce module ?	25
3. Les services Amon	26
4. Structure des conteneurs	26
5. Pré-requis	27
6. Les différences entre les versions 2.4 et 2.5	28
7. Errata 2.5.n	31
Chapitre 3 - Fonctionnement du module Amon	32
Chapitre 4 - Mise en œuvre du module	36
Chapitre 5 - Installation du module	38
1. Pré-requis	38
2. Médias d'installation	39
3. Déroulement de l'installation	43
4. Partitionnement personnalisé	45
5. Choisir le mode du module	58
Chapitre 6 - Configuration du module Amon	62
1. Configuration généralités	62
1.1. Configuration en mode autonome	63
1.1.1. Accès distant	65
1.1.2. La zone Menu	66
1.1.3. La zone Onglet	69
1.1.4. La zone Formulaire	70
1.1.5. La zone Validation	73
1.1.6. Enregistrer la configuration	74
1.1.7. Le mode Debug	75
1.1.8. FAQ	77
1.2. Configuration en mode Zéphir	79
2. Configuration en mode basique	86
2.1. Onglet Général	87
2.2. Onglet Firewall	89
2.3. Onglet Interface-0	90
2.4. Onglet Interface-1	92
2.5. Onglet Interface-n	94
2.6. Onglet Messagerie	96

2.7. Onglet Proxy authentifié : 5 méthodes d'authentification	98
3. Configuration en mode normal	101
3.1. Onglet Général	102
3.2. Onglet Services	105
3.3. Onglet Firewall	105
3.4. Onglet Interface-0	107
3.5. Onglet Interface-1	110
3.6. Onglet Interface-n	115
3.7. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité	119
3.8. Onglet Clamav : Configuration de l'anti-virus	123
3.9. Onglet Relai DHCP	125
3.10. Onglet Onduleur	126
3.11. Onglet Rvp : Mettre en place le réseau virtuel privé	131
3.12. Onglet Eole sso : Configuration du service SSO pour l'authentification unique	133
3.13. Onglet Messagerie	138
3.14. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS	140
3.15. Onglet Proxy authentifié : 5 méthodes d'authentification	142
3.16. Onglets Proxy authentifié 2 : Double authentification	147
3.17. Onglet Wpad : découverte automatique du proxy	147
3.18. Onglet Exceptions proxy	148
3.19. Onglet Reverse proxy : Configuration du proxy inverse	150
3.20. Onglet Freeradius : Configuration de l'authentification Radius	153
4. Configuration en mode expert	157
4.1. Onglet Général	159
4.2. Onglet Services	162
4.3. Onglet Firewall	162
4.4. Onglet Système	164
4.5. Onglet Sshd : Gestion SSH avancée	166
4.6. Onglet Logs : Gestion des logs centralisés	167
4.7. Onglet Interface-0	169
4.8. Onglet Interface-1	174
4.9. Onglet Interface-n	180
4.10. Onglet Réseau avancé	186
4.11. Onglet Certificats ssl : gestion des certificats SSL	190
4.12. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité	192
4.13. Onglet Clamav : Configuration de l'anti-virus	196
4.14. Onglet Relai DHCP	198
4.15. Onglet Onduleur	199
4.16. Onglet Eole sso : Configuration du service SSO pour l'authentification unique	205
4.17. Onglet Rvp : Mettre en place le réseau virtuel privé	213
4.18. Onglet Zones-dns : Configuration du DNS	218
4.19. Onglet Ead-web : EAD et proxy inverse	220
4.20. Onglet Messagerie	220
4.21. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS	225
4.22. Onglet Filtrage web : Configuration du filtrage web	226
4.23. Onglet Squid : Configuration du proxy	231
4.24. Onglet Proxy authentifié : 5 méthodes d'authentification	236
4.25. Onglets Squid2 et Proxy authentifié 2 : Double authentification	241
4.26. Onglet Wpad : découverte automatique du proxy	242
4.27. Onglet Exceptions proxy	243
4.28. Onglet Proxy parent : Chaînage du proxy	245
4.29. Onglet Reverse proxy : Configuration du proxy inverse	247
4.30. Onglet Freeradius : Configuration de l'authentification Radius	251
4.31. Onglet Eoleflask	255

5. Configuration du module Amon avec le module Scribe en DMZ	256
6. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur	259
7. Configurer le module Amon pour Envole	260
8. Configuration DNS pour chaque interface	264
9. Configurer la découverte automatique du proxy avec WPAD	267
Chapitre 7 - Instanciation du module	272
1. Principes de l'instanciation	272
2. Lancement de l'instanciation	273
2.1. Les mots de passe	273
2.2. Activation automatique de la mise à jour hebdomadaire	274
2.3. Le redémarrage	274
Chapitre 8 - Administration du module Amon	276
1. Administration généralités	276
1.1. Principes de l'administration	276
1.2. Découverte de GNU/Linux	277
1.2.1. Les Bases	277
1.2.2. Quelques Commandes	283
1.2.3. Les conteneurs	284
1.2.4. La gestion des onduleurs	284
1.2.5. Les manuels	285
1.2.6. L'éditeur de texte Vim	286
1.2.7. Les commandes à distance avec SSH	291
1.2.8. Quelques références	296
1.3. Reconfiguration	297
1.4. L'interface d'administration EAD	298
1.4.1. Principe général	299
1.4.2. Premier pas dans l'administration d'un serveur	299
1.4.3. Ajout/suppression de serveurs	301
1.4.4. Surveillance de l'état du serveur	304
1.4.5. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur	306
1.4.6. Authentification locale et SSO	307
1.4.7. Redémarrer, arrêter et reconfigurer	309
1.4.8. Mise à jour depuis l'EAD	309
1.4.9. Arrêt et redémarrage de services	310
1.4.10. Rôles et association de rôles	312
1.4.11. La console	332
1.4.12. Listing matériel	334
1.4.13. Bande passante	334
1.4.14. Résoudre des dysfonctionnements liés à l'EAD	335
1.5. L'interface d'administration semi-graphique	335
1.6. Les mises à jour	336
1.6.1. Les différents types de mises à jour	337
1.6.2. Les procédures de mise à jour	340
1.6.3. Ajout de dépôts supplémentaires	344
1.7. Installation manuelle de paquets	345
1.8. Passage d'une version d'EOLE à une autre	346
1.9. Passage d'une version RC à une version stable	347
2. Fonctionnalités de l'EAD propres au module Amon	347
2.1. Rôles et association de rôles	348
2.1.1. Gestion des rôles	348
2.1.2. Association des rôles	352

2.1.3. Les rôles sur le module Amon	354
2.2. Directives optionnelles ERA depuis l'EAD	355
2.3. Exceptions sur la source ou la destination	355
2.4. Filtrage web	357
2.4.1. Filtrage par utilisateur	358
2.4.2. Filtrage par machine ou par groupe de machine	359
2.4.3. Interdire l'accès à un sous-réseau depuis une interface	364
2.4.4. Interdire ou restreindre l'activité d'un sous-réseau	366
2.4.5. Bases de filtres optionnels	368
2.4.6. Filtrage syntaxique	370
2.4.7. Interdire et autoriser des domaines	371
2.4.8. Interdire des extensions et des types MIME	373
2.4.9. Politique liste blanche	375
2.5. Observatoire des navigations	376
2.6. Outil d'analyse de logs LightSquid	377
3. ERA, éditeur de règles pour le module Amon	380
3.1. Introduction	380
3.1.1. Présentation	380
3.1.2. Les fichiers XML de modèles	381
3.1.3. Les variables Creole	382
3.2. Utilisation	383
3.2.1. Les zones de sécurité	383
3.2.2. Les flux	389
3.2.3. Les directives	391
3.2.4. La qualité de service	399
3.2.5. Les options du modèle	400
3.2.6. L'inclusion statique	400
3.2.7. Imbriquer des modèles :l'héritage	401
3.2.8. Communication avec Zéphir	402
3.3. Directives optionnelles ERA depuis l'EAD	403
3.4. Compléments techniques	403
3.4.1. Le format XML interne	403
3.4.2. Comportement du Backend	405
3.4.3. Intégration avec Creole	405
3.4.4. Le compilateur	406
3.5. Quelques références	407
4. Gestion des tunnels : RVP	407
5. Résoudre des dysfonctionnements liés au MTU	408
Chapitre 9 - Personnalisation du module	410
1. Panorama des services	410
1.1. Services liés aux bases de données	410
1.1.1. eole-annuaire	410
1.1.2. eole-client-annuaire	411
1.1.3. eole-db	411
1.1.4. eole-interbase	411
1.1.5. eole-mysql	412
1.1.6. eole-postgresql	412
1.2. Services liés aux serveurs de fichiers	413
1.2.1. eole-fichier-primaire	413
1.2.2. eole-fichier-membre	413

1.2.3. eole-cups	414
1.2.4. eole-proftpd	415
1.2.5. eole-dhcp	415
1.2.6. eole-nfs	416
1.3. Services web	417
1.3.1. eole-web	417
1.3.2. eole-reverseproxy	417
1.3.3. eole-wpad	418
1.4. Services liés à la messagerie	418
1.4.1. eole-exim	418
1.4.2. eole-spamassassin	419
1.4.3. eole-courier	419
1.4.4. eole-sympa	420
1.5. Proxy et authentification	420
1.5.1. eole-proxy	420
1.5.2. eole-radius	421
1.6. Autres services réseau	422
1.6.1. eole-antivirus	422
1.6.2. eole-apt-cacher-ng	423
1.6.3. eole-bareos	423
1.6.4. eole-dns	424
1.6.5. eole-dhcrelay	424
1.6.6. eole-nut	425
1.6.7. eole-pacemaker	425
1.6.8. eole-snmpd	425
1.6.9. eole-vpn	426
2. Personnalisation du serveur à l'aide de Creole	426
2.1. Répertoires utilisés par EOLE	426
2.2. Création de patch Creole	427
2.3. Les dictionnaires Creole	429
2.3.1. Ajouter un en-tête XML	430
2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu	430
2.3.3. Utiliser des familles, variables et des séparateurs	439
2.3.4. Comportement des variables	443
2.3.5. Mettre en place des contraintes	443
2.3.6. Afficher de l'aide	450
2.4. Le langage de template Creole	451
2.4.1. Déclarations du langage Creole	451
2.4.2. Fonctions prédéfinies	455
2.4.3. Utilisation avancée	459
2.4.4. Exemple	460
2.5. Les scripts Creole	461
2.5.1. CreoleLint et CreoleCat	461
2.5.2. CreoleGet et CreoleSet	463
2.5.3. CreoleRun et CreoleService	465
2.5.4. CreoleLock	466
2.5.5. Indications pour la programmation	468
2.6. Ajout de script exécuté à l'instance ou au reconfigure	471
2.7. Ajout d'un test diagnose	472
2.8. Gestion des noyaux Linux	473
2.9. Gestion des tâches planifiées eole-schedule	474
2.10. Gestion du pare-feu eole-firewall	478

Chapitre 10 - Résolution de problèmes	480
1. Problèmes à la mise en œuvre	480
2. Problèmes à l'exploitation	481
3. Trouver de l'information	486
4. Demander de l'aide / Signaler un problème	489
5. Contribuer au projet EOLE	493
Chapitre 11 - Documentations techniques	494
1. Les dépôts EOLE	494
2. Gestion des journaux systèmes sur EOLE	495
3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation	496
3.1. Contexte juridique	496
3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation	498
Chapitre 12 - Paramétrage des postes client	502
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine	502
2. Configurer la découverte automatique du proxy avec WPAD	503
3. Proxy non configuré dans le navigateur : redirection ou page d'information	508
4. Synthèse des paramètres proxy à utiliser pour les postes client	512
Chapitre 13 - Compléments techniques	514
1. Les services utilisés sur le module Amon	514
1.1. eole-antivirus	514
1.2. eole-dhcrelay	515
1.3. eole-dns	515
1.4. eole-exim	516
1.5. eole-nut	516
1.6. eole-proxy	517
1.7. eole-radius	518
1.8. eole-reverseproxy	518
1.9. eole-vpn	518
1.10. eole-wpad	519
2. Ports utilisés sur le module Amon	519
Chapitre 14 - Questions fréquentes	522
1. Questions fréquentes communes aux modules	522
2. Questions fréquentes propres au module Amon	537
Glossaire	540

Chapitre 1

Présentation et historique du projet EOLE

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



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

1. Les objectifs d'EOLE

Les objectifs du projet EOLE sont les suivants :

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

2. Historique du projet EOLE

Les dates significatives du projet

2000

- projet local à l'académie de Dijon pour répondre à un besoin identifié concernant la protection des élèves et des données administratives ;
- établissements pilotes : Cité scolaire de Montchapet, Lycée Le Castel et Lycée Simone Weil ;
- distribution GNU/Linux utilisée : Mandrake 7.

2001

- projet national à la demande du ministère de l'Éducation nationale ;

- naissance du premier module EOLE 1.0 à partir de la distribution Mandrake 8 : **Amon**, serveur pare-feu.

2002

- études de contenu nationales & développement par le CETIAD^[p.542] ;
- généralisation du module Amon 1.0 dans les collèges et les lycées de plusieurs académies : Clermont-Ferrand, Montpellier, Besançon... ;
- nouveau module 1.0 : **Sphynx**, concentrateur de réseaux privés virtuels et **Horus**, serveur de fichiers administratif

2003

- l'équipe EOLE devient pôle national de compétence EOLE ;
- module Amon 1.5.

2004

- module Sphynx 1.1 ;
- nouveau module 1.0 : **Scribe**, serveur de fichiers pédagogique ;
- écriture d'un éditeur de règles pour le module Amon nommé **ERA**.

2005

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

2006

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

2007

- intégration de @SSR (sécurité routière) sur le module Scribe ;
- EOLE NG 2.0 (en octobre), utilisation de la distribution Ubuntu 7.04 (Feisty Fawn) ;
- démonstrateur d'un module utilisant la technologie Xen^[p.564].

2008

- EOLE NG 2.1 (mai), utilisation de la distribution Ubuntu 7.10 (Gutsy Gibbon) ;
- nouveau module 2.1 : **Eclair**, serveur de clients légers Linux.

2009

- EOLE NG 2.2 LTS (janvier), utilisation de la distribution Ubuntu 8.04 LTS (Hardy Heron) ;
- nouveaux modules :
 - **AmonEcole**, Scribe et Amon sont virtualisés avec la technologie OpenVZ^[p.556] ;
 - **Seshat** le relais de messagerie pour le domaine intra-académique ;
- la console de visualisation de l'IDS Prelude (fonctionnant avec ZéphirLog) ;
- nouveau module 2.2 eSSL par le MEDDE^[p.553] ;

- intégration d'Envole^[p.546] 2.0 sur le module Scribe.

2011

- EOLE NG 2.3 LTS (juin), utilisation de la distribution Ubuntu 10.04 LTS (Lucid Lynx) ;
- introduction du mode conteneur utilisant la technologie LXC^[p.552] pour remplacer OpenVZ ;
- nouveaux modules 2.3 : eSBL et eCDL par le Ministère de l'Écologie, du Développement durable et de l'énergie (MEDDE)^[p.553].

2012

- portage d'Eclair en 2.3 (juillet), repose sur ltsf-cluster, le serveur embarque le logiciel Gaspacho^[p.548] ;
- nouveau module 2.3 : **AmonEcole+**, AmonEcole + Eclair.

2013

- le pôle de compétences EOLE devient pôle de compétences logiciel libre ;
- L'interface de configuration du module est basée sur de nouvelles technologies : Flask, Backbone.js, Marionette et Tiramisu ;
- les solutions EOLE sont inscrites au Socle Interministériel de Logiciel Libre (SILL)^[p.560] 2013 ;
- EOLE 2.4 LTS alpha1 (septembre) ;
- EOLE 2.4 LTS alpha2 (octobre) ;
- nouveau module 2.4 : **Thot**, annuaire centralisé.

2014

- les solutions EOLE sont inscrites au Socle Interministériel de Logiciel Libre (SILL)^[p.560] 2014 ;
- EOLE 2.4 LTS RC (février) ;
- EOLE 2.4 LTS (mai) : portage des modules Amon, Scribe, Horus et Sphynx.

2015

- EOLE 2.4.1 LTS (février), utilisation de la distribution Ubuntu 12.04 LTS (Precise Pangolin)
 - portage d'AmonEcole ;
 - nouveaux modules 2.4 : **Hâpy**, **Hâpy Node**, **Hâpy Market** et **Hâpy Master** sont des solutions de virtualisation basées sur OpenNebula^[p.556].
- EOLE 2.4.1.1 LTS (mai)
- EOLE 2.5 LTS (juillet), utilisation de la distribution Ubuntu 14.04 LTS (Trusty Tahr) ;
 - portage du module Seshat ;
 - portage du module Zéphir ;
 - nouvelle charte graphique.
- EOLE 2.4.2 LTS (juillet)
 - nouvelle version d'Envole : version 4.
- EOLE 2.5.1 LTS (novembre)
 - portage du module Scribe ;
 - portage du module Amon ;
 - portage du module Horus ;
 - portage du module AmonEcole ;

- portage du module eCDL ;
- portage du module eSBL ;
- portage d'Envole 4 sur EOLE 2.5.1 par la mutualisation Envole.

2016

- EOLE 2.5.2 LTS (avril)
 - portage du module Sphynx ;
 - publication d'Envole 5 sur EOLE 2.5.2 par la mutualisation Envole.
- EOLE 2.6 LTS (décembre), utilisation de la distribution Ubuntu 16.04 LTS (Xenial Xerus)
 - portage du module Scribe ;
 - portage du module Horus ;
 - portage des modules Hâpy : **Hâpy** et **Hâpy Node** ;
 - portage du module Sphynx ;
 - portage du module Eclair ;
 - portage du module eSBL ;
 - portage du module Zéphir ;
 - nouveau module 2.6 : **Seth** est une solution de contrôleur de domaine de type Active Directory élaborée conjointement par le Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche (MENSUR) et le Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM^[p.553]).

Cette version d'EOLE marque l'arrêt du support pour l'architecture i386.

2017

- EOLE 2.6.1 LTS (mai)
 - portage des modules : Amon, AmonEcole, Seshat, Thot et eCDL ;
 - publication d'Envole 6 sur EOLE 2.6.1 par la mutualisation Envole.
- EOLE 2.6.2 LTS (décembre)
 - portage du module AmonEcoleEclair.






















































2018

- EOLE 2.7 LTS (décembre), utilisation de la distribution Ubuntu 18.04 LTS (Bionic Beaver)
 - portage du module Amon ;
 - portage du module Seth ;
 - portage du module eSBL ;
 - portage du module Sphynx ;
 - portage du module Seshat ;
 - portage du module Thot ;
 - portage du module Zéphir ;
 - portage des module Hâpy : Hâpy et Hâpy Node ;
 - abandon du module eCDL au profit du module Seth.

2019

- EOLE 2.7.1 LTS (juin)
 - portage du module Eclair ;
 - portage du module Scribe en Scribe AD ;
 - portage du module Horus en Horus AD ;
 - abandon du module eSBL au profit du module Seth en mode membre.

Historiques des versions des modules EOLE

Version	2.0	2.1	2.2	2.3	2.4.0	2.4.1	2.4.2	2.5.0	2.5.1	2.5.2	2.6.0
Date de sortie	2007	2008	2009	2011-1012	2014	2015	2015	2015	2015	2016	2016
Fin du support	HS	HS	HS	HS	HS	HS	HS	HS	HS	HS	Juin 2021
eCDL											
eSBL											
Amon											
Eclair											
Hâpy											
Hâpy Node											
Hâpy Market											
Hâpy Master											
Horus (NT)											
Horus (AD)											
Scribe (NT)											












































Scribe (AD)											
Seshat											
Seth											
Sentinelle											
Sphynx											
Thot											
AmonEcole											
AmonEcole+ AmonEcoleEclair											
AmonHorus											
Zéphir											
ZéphirLog											
Envole											

Tableau des modules par versions d'EOLE

3. Logiciel Libre

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

Le logiciel libre garantit quatre niveaux de libertés :

- utilisation : la liberté d'utiliser/exécuter le logiciel pour quelque usage que ce soit ;
- étude : la liberté d'étudier le fonctionnement du programme, et de l'adapter à vos besoins ;
- redistribution : la liberté de redistribuer des copies ;
- modification : la liberté d'améliorer le programme, et de rendre publiques vos améliorations de telle

sorte que la communauté tout entière en bénéficie.

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

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

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

Licences

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

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

Pour ses développements internes, EOLE a choisi la licence libre CeCILL^[p.551].

Contributions au libre

Contribuer au libre peut prendre plusieurs formes : promotion, amélioration, documentation, traduction, remontée de dysfonctionnement...

Le pôle de compétences Logiciels libres utilise et intègre de nombreux logiciels libres ce qui offre l'opportunité de contribuer à différents projets libres :

- Ubuntu Launchpad : <https://bugs.launchpad.net/~eole-team> ;
- AskUbuntu : <https://askubuntu.com/users/389629/eole-team> ;
- OpenNebula : <http://dev.opennebula.org/users/1416> ;
- GitHub : <https://github.com/eole> ;
- The Samba-Bugzilla : <https://bugzilla.samba.org> ;
- Wikipédia : <https://fr.wikipedia.org/wiki/Spécial:Contributions/EOLE-team> [https://fr.wikipedia.org/wiki/Sp%C3%A9cial:Contributions/EOLE-team] ;
- OpenStreetMap : <https://www.openstreetmap.org/user/EOLE-Team>.

Ces contributions prennent essentiellement la forme de traductions et de remontées de dysfonctionnements avec parfois la soumission de correctifs et de solutions.

Une page wiki sur la forge recense les contributions récentes d'EOLE à différentes communautés du logiciel libre :

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

4. Méta-distribution EOLE

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

La méta-distribution EOLE regroupe l'ensemble des modules développés. Chaque module donne

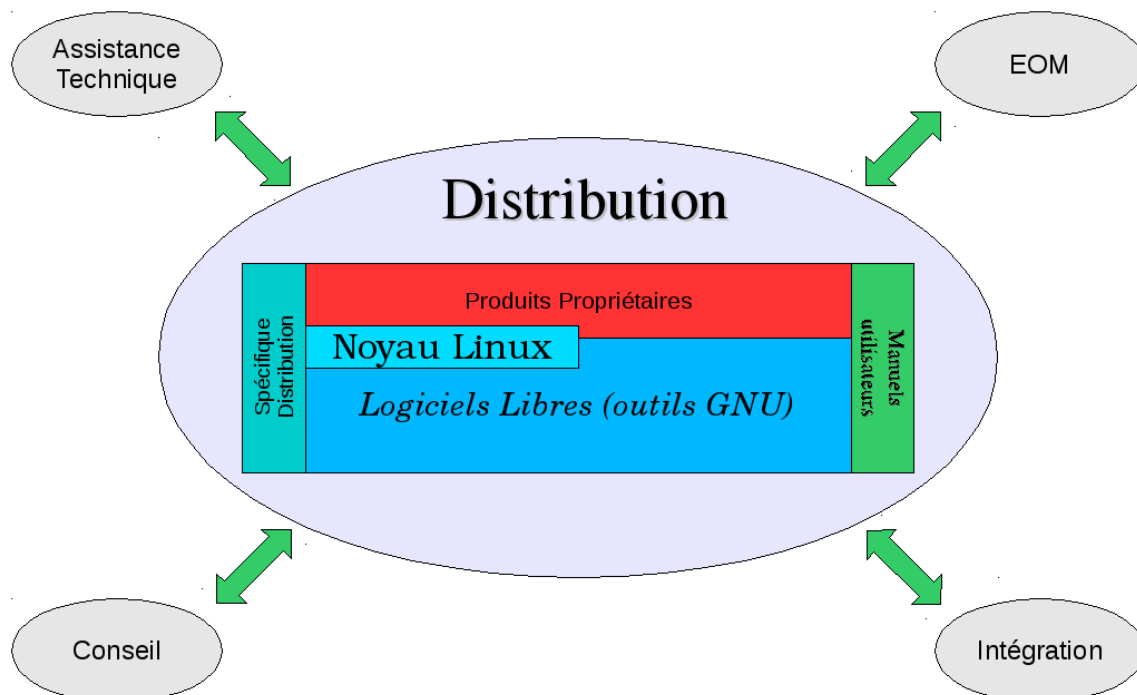
naissance à une distribution GNU/Linux à part entière.

Une distribution GNU/Linux

Une distribution^[p.544] GNU/Linux^[p.551] est un ensemble cohérent de logiciels groupés autour d'un noyau (ou kernel) Linux.

Elle comporte :

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



Les modules EOLE

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

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

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

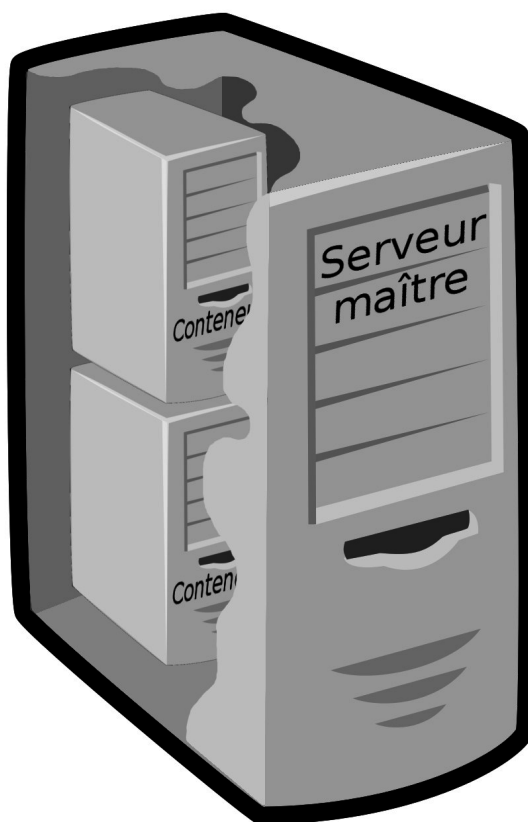
5. EOLE 2.5



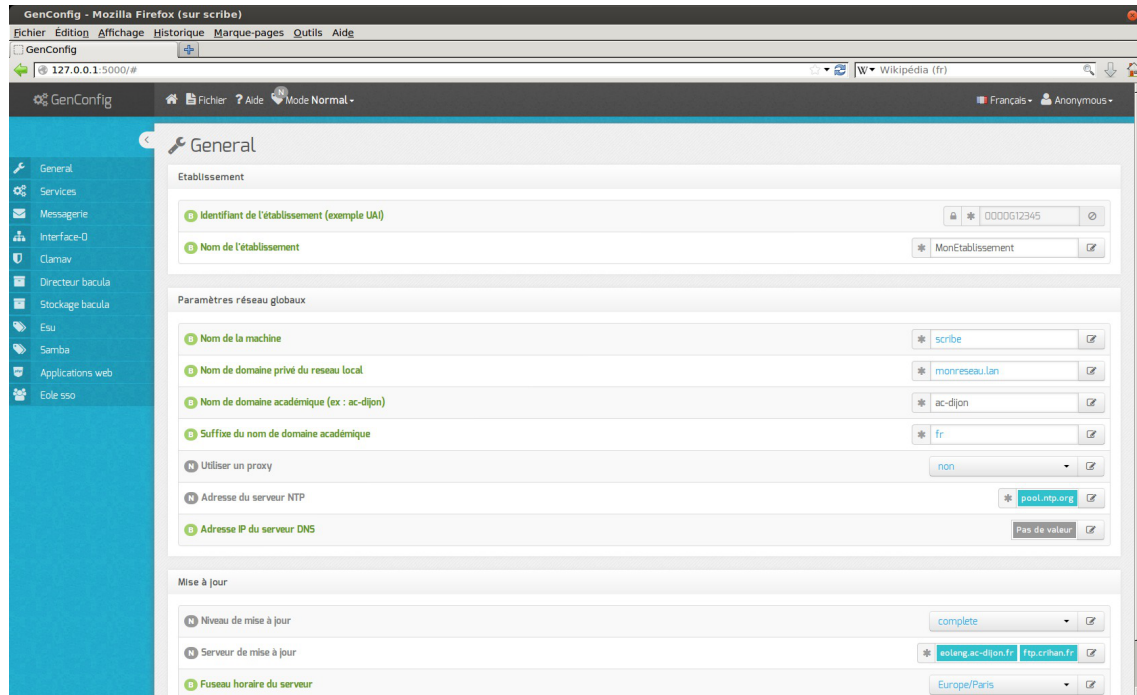
Les modules de la version EOLE 2.5 s'appuient sur la distribution GNU/Linux Ubuntu 14.04 LTS nommée également Trusty Tahr.

Ubuntu 14.04 LTS est disponible depuis le 17 avril 2014. Portant le label LTS^[p.551], 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

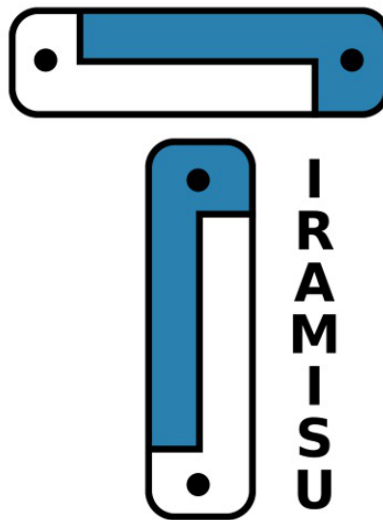


La version 2.5 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule 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^[p.562].



Logo du logiciel Tiramisu

6. Modules supportés disponibles

	2.6.0	2.6.1	2.6.2	2.7.0	2.7.1
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					
Sphinx					
Thot					
AmonEcole					










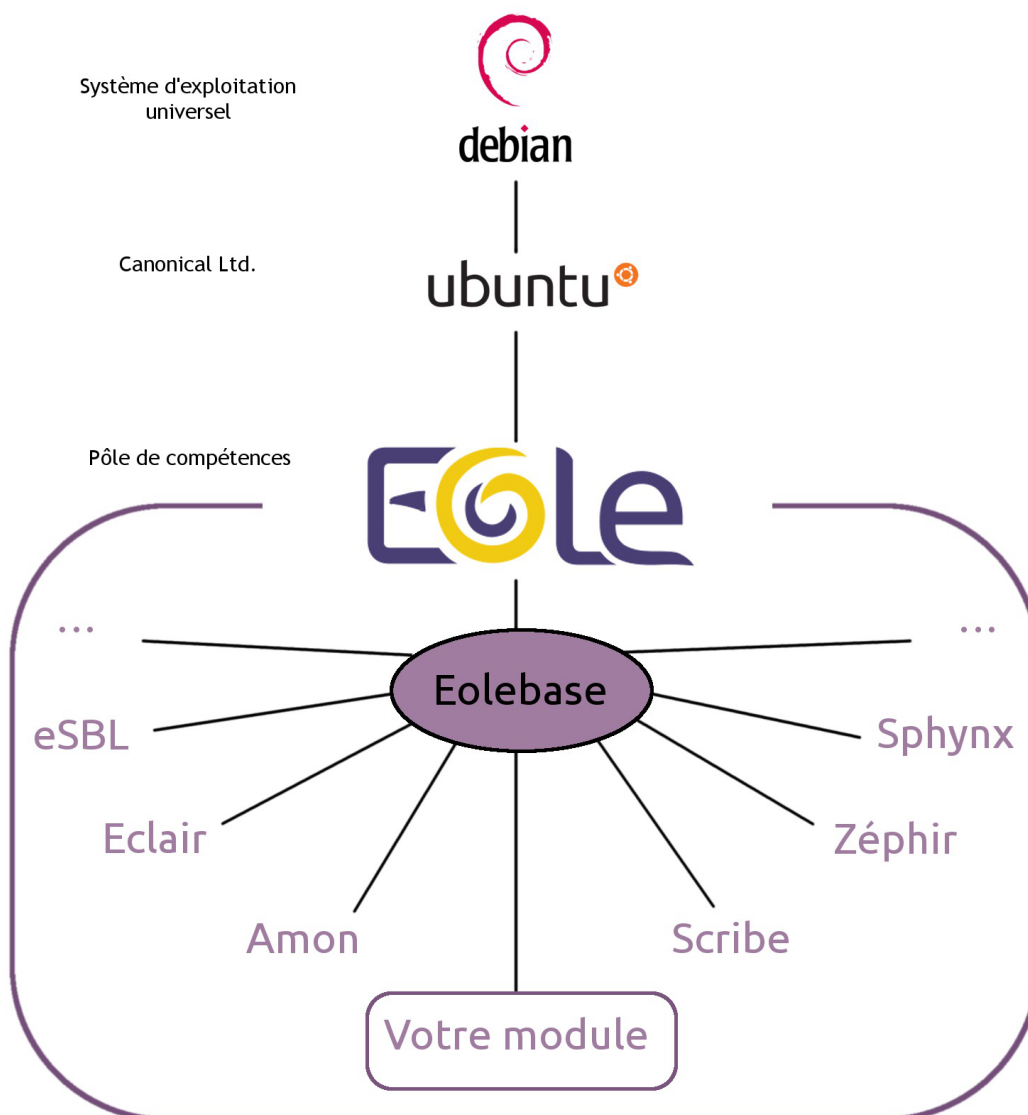
AmonEcoleEclair					
Zéphir					
Envole					

Tableau des modules par versions d'EOLE

7. Eolebase

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

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



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.

8. Quelques références

- Les sites EOLE :
 - Site web Officiel : <https://pcll.ac-dijon.fr/eole/>
 - Listes de diffusion : <https://pcll.ac-dijon.fr/listes>
 - La forge : <http://dev-eole.ac-dijon.fr/>
- Logiciel Libre :
 - <http://www.gnu.org/philosophy/free-sw.fr.html>
- Licence GPL :
 - Gnu.org : <http://www.gnu.org/licenses/licenses.fr.html#GPL>
 - Wikipédia : http://fr.wikipedia.org/wiki/Licence_publique_générale_GNU (http://fr.wikipedia.org/wiki/Licence_publique_g%C3%A9n%C3%A9rale_GNU)
- Licence CeCILL :
 - CeCILL.info : <http://www.cecill.info>
 - Wikipédia : http://fr.wikipedia.org/wiki/Licence_CeCILL

Chapitre 2

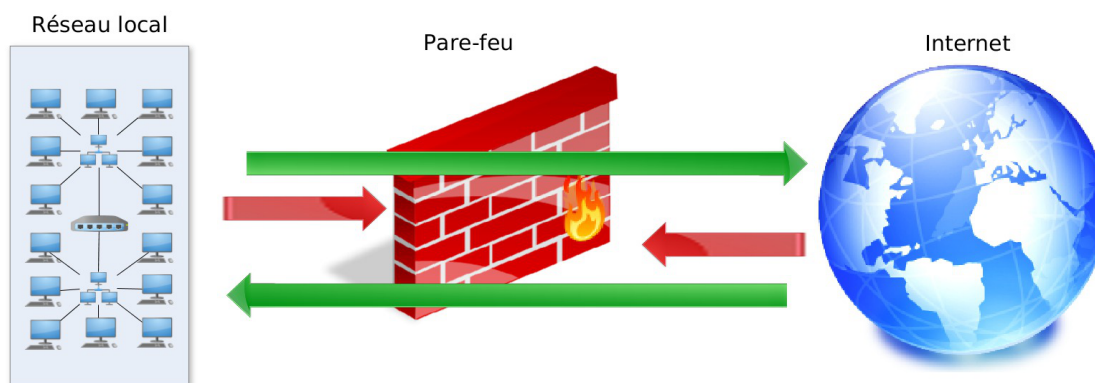
Introduction au module Amon

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.

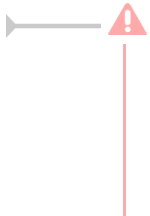
Installé sur un serveur dédié, équipé de deux, trois, quatre ou cinq interfaces réseau, il permet d'organiser au mieux l'architecture réseau d'un établissement.

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^[p.546], est à votre disposition pour effectuer ce travail.

Il est également possible de créer un réseau virtuel privé (RVP^[p.559], VPN) entre l'établissement (une structure administrative) et un concentrateur académique (par exemple le module Sphynx). Ce réseau virtuel privé permet de sécuriser les flux sensibles au travers d'Internet.

Pour l'Éducation nationale, ce réseau est nommé réseau AGRIATES^[p.540].



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

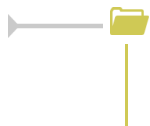
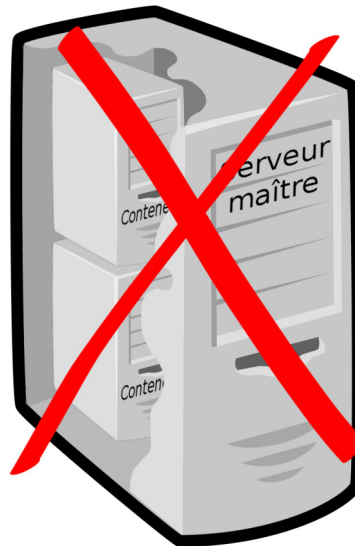
- *Noyau Linux 3.x* : Noyau Linux Ubuntu ;
- *OpenSSH* : prise en main à distance moyennant une demande d'authentification ;
- *Rsyslog* : service de journalisation et de centralisation des logs ;
- *Pam* : gestion des authentifications ;
- *EAD* : outil EOLE pour l'administration du serveur ;
- *EoleSSO* : 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^[p.543].



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^[p.559] 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^[p.562] 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^[p.545].

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^[p.547] ;
- Backbone.js^[p.541] et Marionette^[p.553] ;
- Tiramisu^[p.562].

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

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

Règles pare-feu

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

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

Tâches planifiées

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

En version 2.5, `eole-schedule` est géré depuis Tiramisu^[p.562].

La liste des scripts à activer pour la gestion des tâches est décrite dans des dictionnaires XML^[p.564] 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^[p.545]. 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^[p.563].

7. Errata 2.5.n

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

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



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



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

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

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

Chapitre 3

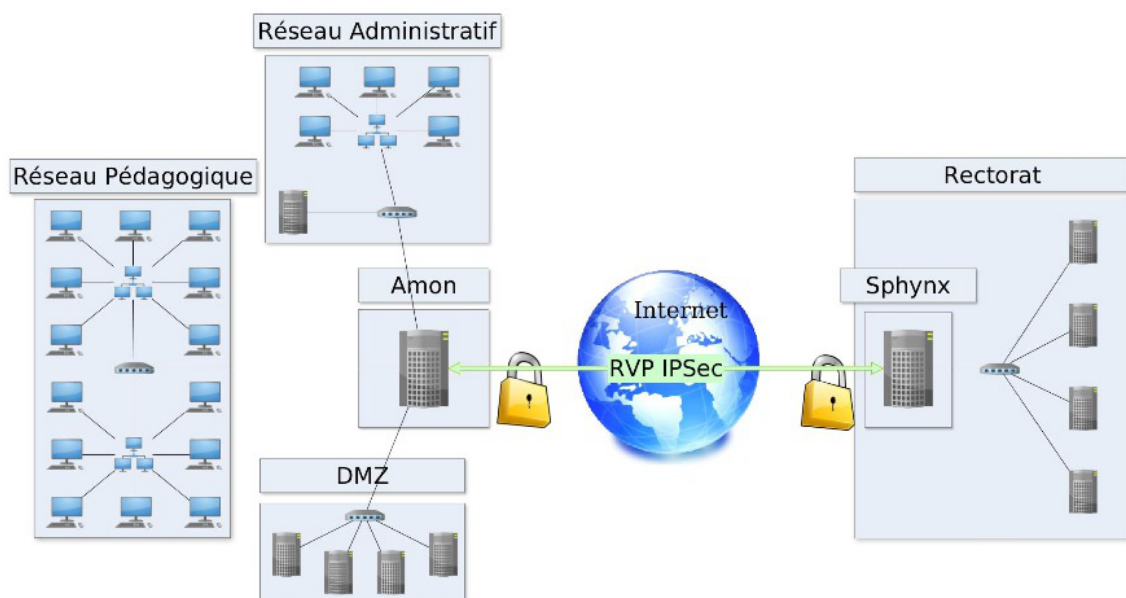
Fonctionnement du module Amon

Pour jouer son rôle, le module Amon repose sur beaucoup de projets libres : iptables, strongSwan, squid, e2guardian, Nginx.

Tous les services sont activables, désactivables, pour construire une passerelle sur mesure.

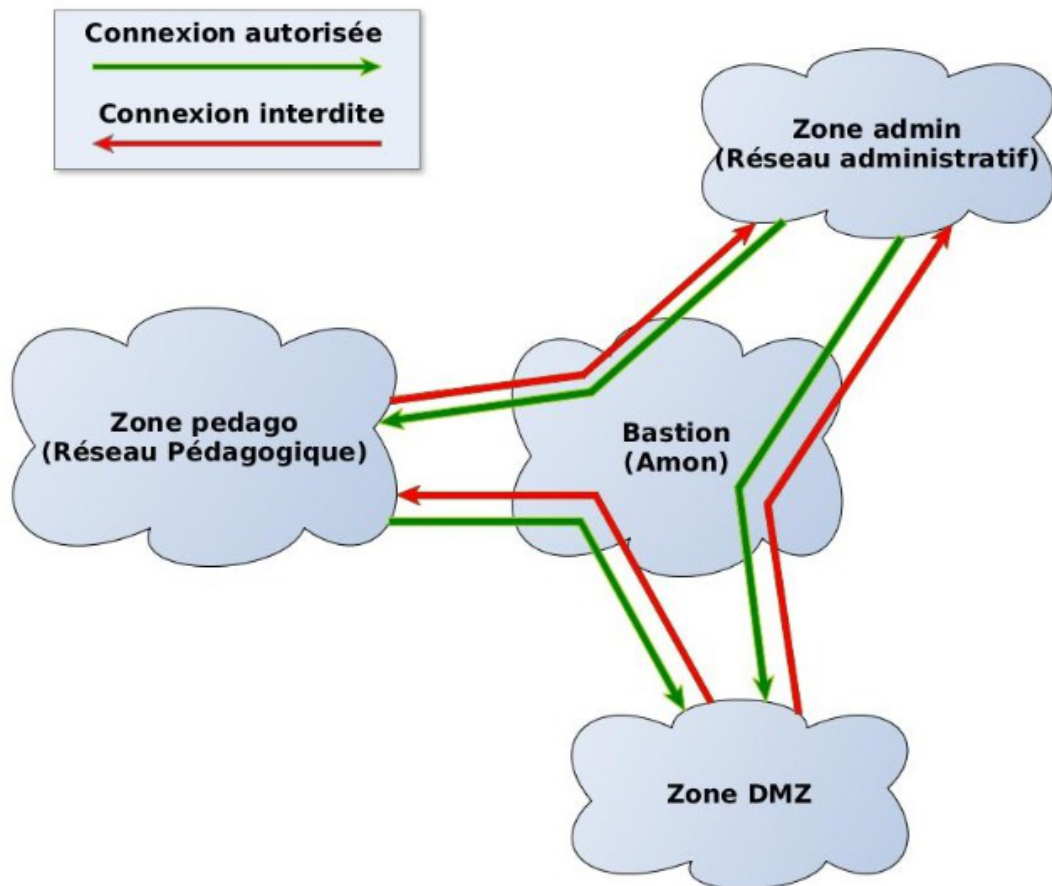
La passerelle permet :

- la mutualisation de l'accès Internet pour les réseaux locaux ;
- la gestion des Réseaux Virtuels Privés (RVP/VPN).



Le module Amon permet de mettre en place rapidement et facilement tous les services nécessaires à la sécurisation d'un réseau et à l'application des règles de communication autorisées. Le pare-feu^[p.557] repose sur le logiciel iptables^[p.550] et l'éditeur de règles ERA^[p.546] permet de générer les règles et de gérer la description de la politique de sécurité d'un pare-feu. Cette politique est sauvegardée intégralement dans un fichier de type XML^[p.564] avec un format spécifique à l'application.

Par un processus de compilation, ERA transforme le fichier XML en un bloc de règles iptables, de manière à instancier ces règles sur un pare-feu cible.



Typiquement, le module Amon devrait être équipé au minimum de 2 cartes réseau :

- l'interface-0, carte affectée pour le trafic réseau extérieur ;
- l'interface-1, carte affectée pour le trafic réseau intérieur ;

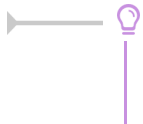
Des cartes supplémentaires interface-n peuvent être ajoutées.

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

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



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



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

Chaque carte réseau devra avoir sa propre adresse IP. Le choix de celles-ci dépend de l'architecture réseau en place.

Le service bastion récupère les règles par défaut des zones ainsi que toutes les règles personnalisées :

- les règles optionnelles de l'EAD ;
- les postes et les groupes de postes interdits ou restreints dans l'EAD ;
- les règles sur les horaires de l'EAD ;
- les règles ipsets (les exceptions sur une directive) ;
- les règles de la QOS ;
- les règles tcpwrapper (host allow et hosts deny).

Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu.

La liste des actions du service se trouve dans le script `/usr/share/era/bastion.sh`.

Le service bastion met en cache les règles mais ne les régénère pas à chaque fois.

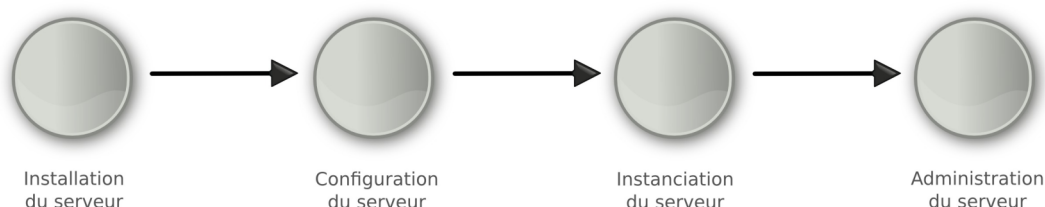
Seules les commandes `CreoleService bastion restart` ou `service bastion restart` vont régénérer les règles.

Le proxy filtrant repose sur l'utilisation de squid et de e2guardian et permet :

- de gérer une liste de sites et d'URL interdits ;
- le filtrage syntaxique ;
- l'interdiction par extension et type MIME ;
- de gérer une liste blanche (« tout interdit sauf ») ;
- d'interdire une plage d'IP et plage horaire ;
- l'économie de bande passante par la mise en cache.

Chapitre 4

Mise en œuvre du module



Fil rouge de la mise en œuvre

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

- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.549] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (<http://eole.orion.education.fr>). Tous les modules installables depuis cette unique image ISO.

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

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

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

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

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

Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid [p.561], e2guardian [p.545], etc.

- La **phase d'instanciation** s'effectue au moyen de la commande `instance`.

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

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

Cette phase doit être complétée par un diagnostic complet du module à l'aide de la commande `diagnose -L`.

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

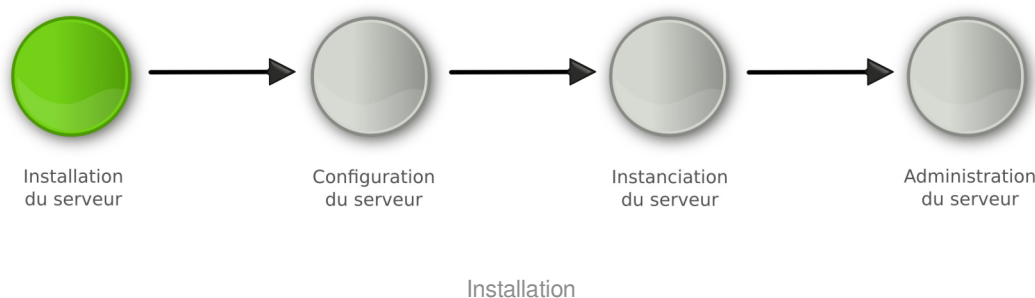
Chaque module possède des fonctionnalités propres, souvent complémentaires.

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

Chapitre 5

Installation du module

La première des quatre phases



- La **phase d'installation** s'effectue au moyen d'un support de type CD-ROM ou clé USB, l'image ISO [p.549] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (<http://eole.orion.education.fr>). Tous les modules installables depuis cette unique image ISO.

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

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

1. Pré-requis

Choix du matériel

Il est recommandé de vérifier la compatibilité matérielle en s'assurant que le serveur est compatible avec Ubuntu server 14.04 LTS (Trusty Tahr).

L'image ISO d'EOLE 2.5.2.1 intègre le support de l'UEFI [p.563].

Choix de l'architecture

Deux architectures sont supportées par EOLE :

- la version 32 bits (x86 [p.564]) ;
- la version 64 bits (AMD64 [p.540]).

2. Médias d'installation

Les images d'installation des modules EOLE (format ISO et MD5SUMS) sont disponibles sur le site du projet EOLE en HTTP^[p.549] :

- <http://eole.ac-dijon.fr/pub/iso>

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

```
$ md5sum -c MD5SUMS
eole-2.5.2-alternate-i386.iso: Réussi
```

Différents types de média sont utilisables pour installer les modules.

CD-ROM

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

Clé USB

Créer une clé USB bootable depuis une distribution GNU/Linux

Pour créer une clé USB bootable avec l'image ISO EOLE depuis une distribution GNU/Linux ;

1. ouvrir un terminal en super utilisateur ;
2. insérer une clé USB, repérer le nom du périphérique (exemple : `/dev/sdx`) et démonter le support (`umount /dev/sdxy`) ;
3. se placer dans le répertoire contenant l'image ISO préalablement téléchargée ;
4. `# dd if=eole-2.5.x-alternate-amd64.iso of=/dev/sdx` (les données seront perdues !) ;
5. démarrer le serveur cible sur la clé USB.

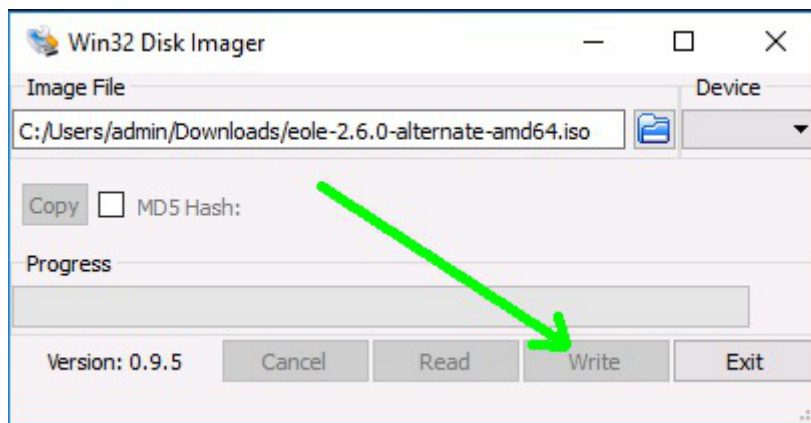
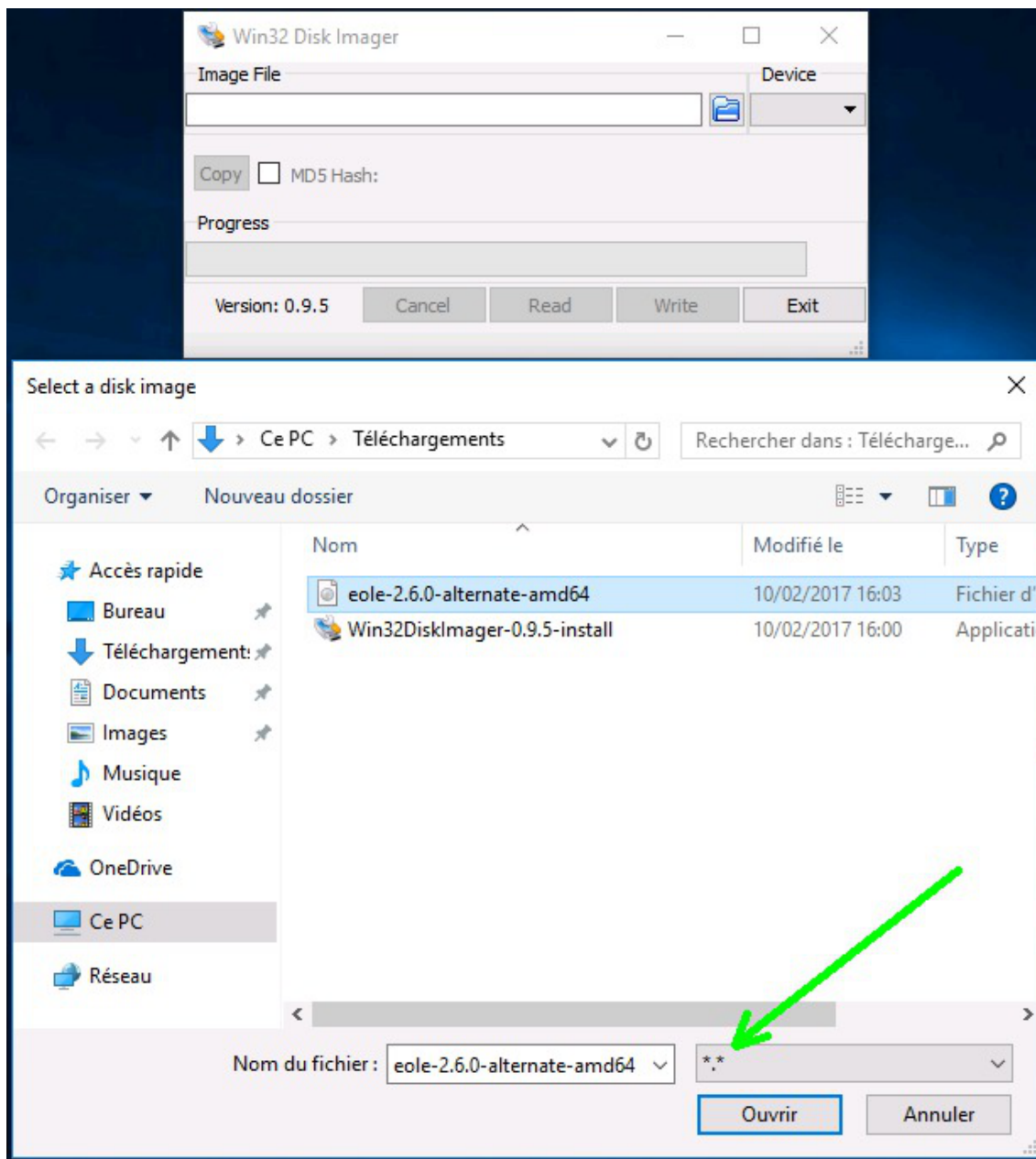


La commande `dd` écrase intégralement le contenu de la clé.

Créer une clé USB bootable depuis un poste Windows

Sur un poste Windows, il est possible de créer une clé USB bootable avec l'image ISO EOLE en utilisant le logiciel Win32 Disc Imager :

<https://sourceforge.net/projects/win32diskimager/>



PXE

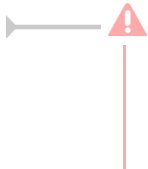
Le document suivant décrit la mise en place d'une configuration PXE^[p.559] pour installer les modules

EOLE :

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

Installer EOLE depuis Ubuntu

Il est possible d'installer EOLE 2.5 sur une version installée de **Ubuntu LTS 14.04 édition serveur** [<http://releases.ubuntu.com/14.04/>].



Il faut avoir à l'esprit que le partitionnement sera celui effectué à l'installation de la version d'Ubuntu et non le partitionnement automatique en LVM^[p.552] proposé par l'installateur de l'image ISO EOLE.

Utiliser les dépôts EOLE

- ajouter les dépôts EOLE

```
# cat > /etc/apt/sources.list.d/eole.list <<EOF
deb http://eole.ac-dijon.fr/eole eole-2.5.2 main cloud
deb http://eole.ac-dijon.fr/eole eole-2.5.2-security main cloud
deb http://eole.ac-dijon.fr/eole eole-2.5.2-updates main cloud
EOF
```

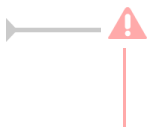
- ajouter la clé GPG publique d'EOLE (clé qui signe les paquets EOLE pour en vérifier l'intégrité)

```
# wget -O - "http://eole.ac-dijon.fr/eole/project/eole-2.5-repository.key" | sudo
apt-key --keyring /etc/apt/trusted.gpg.d/eole-archive-keyring.gpg add -
```

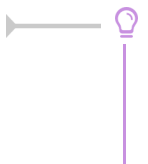
- mettre à jour les dépôts

```
# apt-get update
```

Installer le module désiré



Attention les modules ne sont pas tous qualifiés pour être installés en mode conteneur et inversement certains modules ne sont pas installables en mode non conteneur (AmonEcole).



Les options `-y` et `--force-yes` de la commande `apt-get` indiquent au système de répondre automatiquement à toutes les questions pouvant apparaître lors de la configuration des paquets à installer.

Eolebase non conteneur

Installer la base d'EOLE pour un module non conteneur :

```
# apt-get install -y --force-yes eole-server eole-exim-pkg
```



Nécessite de télécharger environ 150 Mo d'archives.

Module non conteneur

Installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-all`, `eole-amon-all`):

```
# apt-get -y --force-yes install eole-nomDuModule-all
```



Pour installer les modules Scribe ou eSBL de cette manière il faut ajouter le dépôt Envole 5 au fichier `/etc/apt/sources.list.d/eole.list` :

```
# echo "deb http://eole.ac-dijon.fr/envole envole-5 main" >>
/etc/apt/sources.list.d/eole.list && apt-get update
```

Il faut ensuite procéder à l'installation du méta-paquet :

```
# apt-get -y --force-yes install eole-scribe-all
```



Nécessite de télécharger entre 180 Mo et 350 Mo d'archives selon le module à installer.

Eolebase conteneur

Installer la base d'EOLE pour un module conteneur :

```
# apt-get -y --force-yes install eole-lxc-controller
```



Nécessite de télécharger environ 150 Mo d'archives.

Module conteneur

Installer la base d'EOLE pour un module conteneur :

```
# apt-get -y --force-yes install eole-lxc-controller
eole-nomDuModule-module
```

Installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-module`, `eole-amon-module`).



Nécessite de télécharger entre 160 Mo et 200 Mo d'archives selon le module à installer.

Redémarrer le serveur

À la fin de l'installation il faut redémarrer le serveur pour mettre en place les mécanismes EOLE : interface de configuration du module, privilège via sudo...

Le mot de passe à utiliser pour se connecter en `root` est celui affiché dans la console.

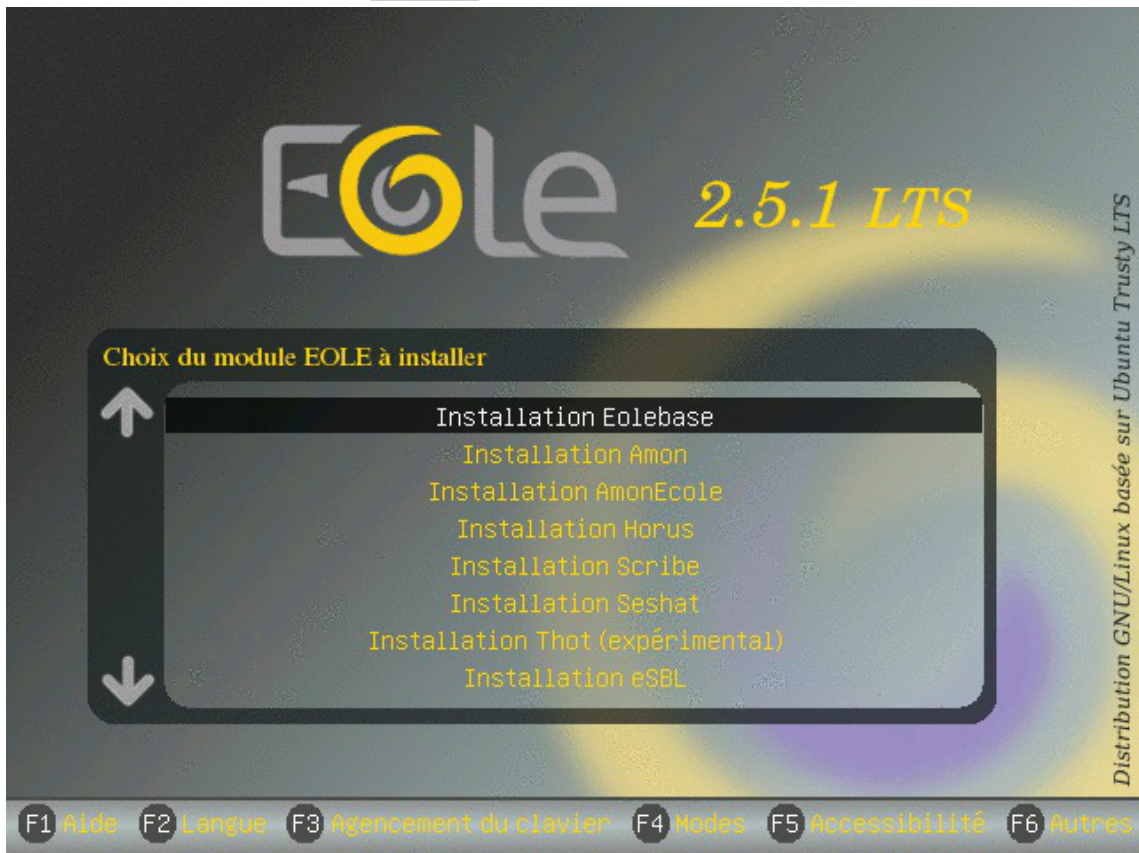
Voir aussi...

Choisir le mode du module [p.58]

3. Déroulement de l'installation

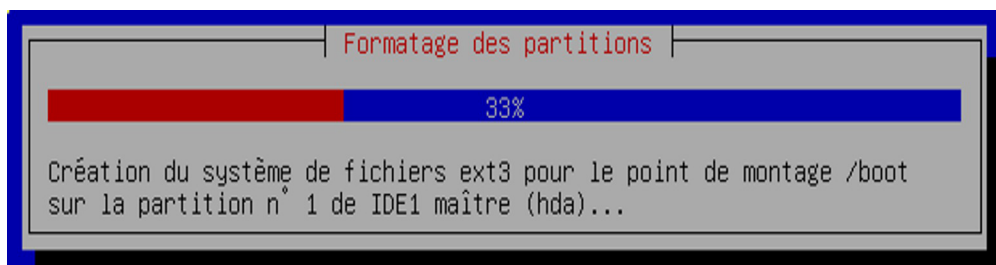
Pour installer un module, il suffit de :

- démarrer le serveur cible avec le média d'installation choisi ;
- sélectionner le module à installer parmi ceux proposés ;
- valider en appuyant sur la touche **Entrée** .



Menu général de l'installateur EOLE 2.5

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



Formatage des partitions du disque

Les différentes phases de l'installation sont :

1. détection du matériel ;
2. charger des composants supplémentaires ;

3. configuration du réseau avec DHCP ;
4. démarrage de l'outil de partitionnement ;
5. partitionnement LVM^[p.552] assisté ou manuel ;

```

[!!!] Conditional Boolean

Voulez-vous forcer un partitionnement manuel ?

Si vous sélectionnez « Oui », vous forcez un partitionnement
manuel comme sur Eolebase sans avoir besoin de brancher un second
disque ou une clef USB.

Si vous sélectionnez « Non », vous forcez un partitionnement
automatique même sur Eolebase.

Si vous sélectionnez « Non » mais que deux disques sont détectés, le
partitionnement manuel sera quand même activé.

<Oui>                                     <Non>

```

Forcer le partitionnement manuel en répondant oui à la question

6. formatage des partitions ;
7. configuration de l'outil de gestion des paquets (Apt^[p.541]) ;
8. choisir et installer des logiciels ;
9. installation du programme de démarrage GNU GRUB^[p.548] ;
10. fin de l'installation.

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

```

[!!!] Terminer l'installation
      Installation terminée

L'installation est terminée et vous allez pouvoir maintenant démarrer
votre nouveau système. Veuillez vérifier que le support
d'installation (CD, disquettes) est bien retiré afin que le nouveau
système puisse démarrer et éviter de relancer la procédure
d'installation.

<Revenir en arrière>                       <Continuer>

```

Fin de l'installation

En validant `Continuer`, le système redémarre automatiquement.



La bonne répartition de l'espace disque résultant d'un partitionnement automatique n'est pas garanti sur un disque inférieur à 30Go.



Une fois le système redémarré, comme indiqué par le prompt, vous pouvez ouvrir une session dans la console, mais aussi au travers de SSH, avec l'utilisateur **root** et le **mot de passe aléatoire** qui est **affiché**. Ce mot de passe sera bien évidemment changé lors de

| l'étape d'instanciation.



Les mots de passe générés aléatoirement suivent les critères suivants :

- 12 caractères ;
- au moins une majuscule ;
- au moins un chiffre ;
- au moins un caractère spécial ;
- pas de caractères ambigus (l ou 1, 0 ou O, ...).

Cas particuliers pour une version inférieure à EOLE 2.5.1



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

Cependant, si l'installateur rencontre au moins deux disques dans l'ordinateur (2 disques durs ou 1 clé USB) il passe en partitionnement manuel quelque soit le module.

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

- lancer une installation `Eolebase` qui vous proposera de partitionner manuellement ;
- installer ensuite le méta-paquet du module souhaité au moyen du programme en ligne de commande : `apt-get install eole-<module>-module`



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

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

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

Voir aussi...

Partitionnement personnalisé ^[p.45]

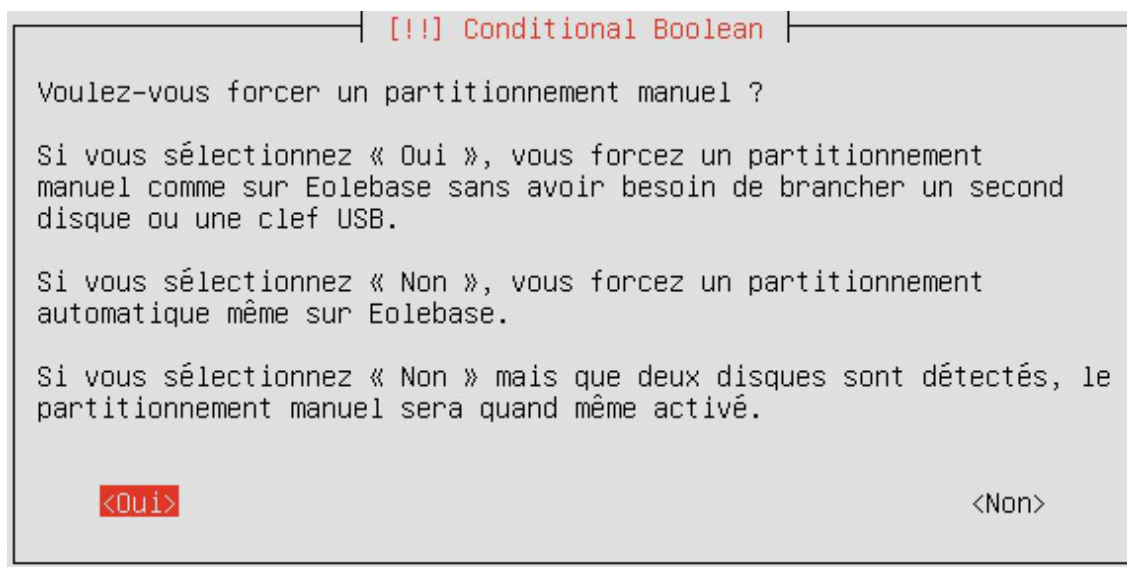
4. Partitionnement personnalisé

Le partitionnement utilise le logiciel LVM^[p.552].

- Sur une version inférieure à 2.5.1 d'EOLE, seule l'installation d'`Eolebase`, aiguille systématiquement vers un partitionnement manuel et nécessite une intervention.

Cependant, si l'installeur rencontre au moins deux disques dans l'ordinateur (2 disques durs ou 1 clé USB) il passe en partitionnement manuel quel que soit le module.

- Sur une version supérieure ou égale à 2.5.1 d'EOLE, une fenêtre propose de choisir un partitionnement manuel, il peut être refusé, le partitionnement sera alors automatique y compris sur un Eolebase.

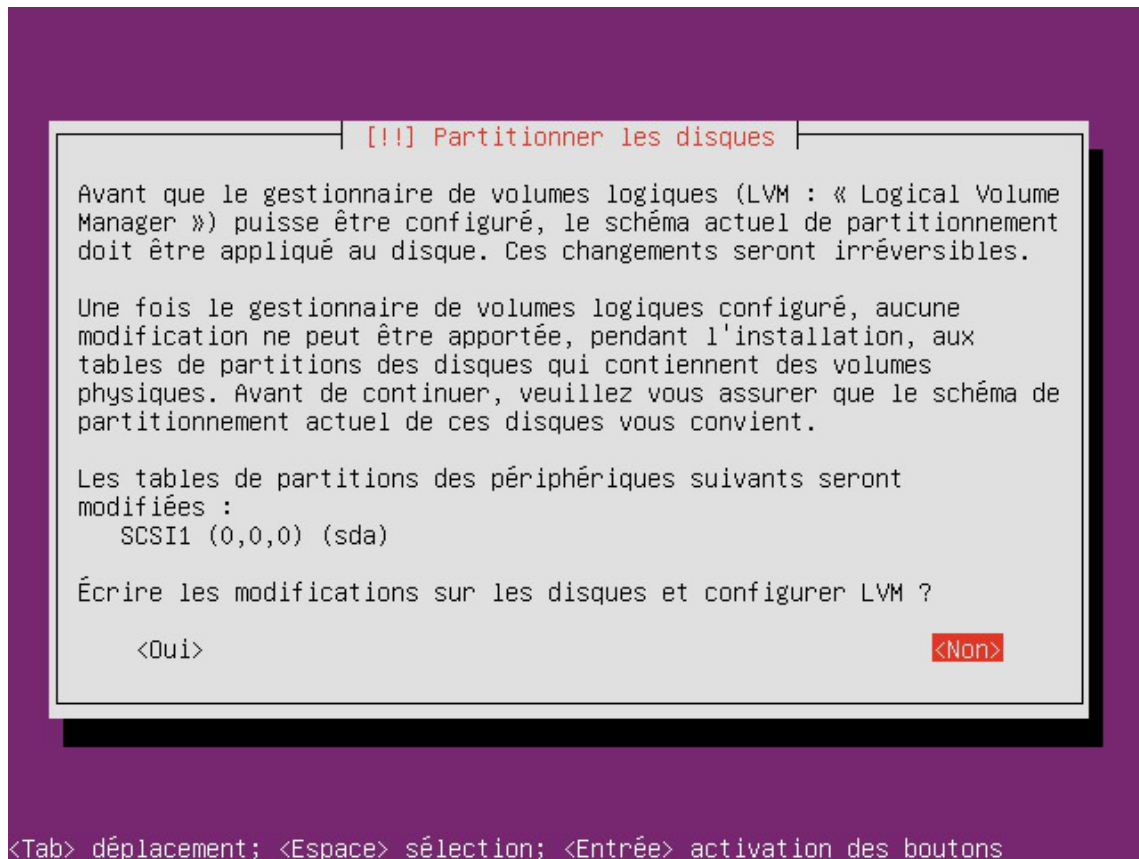


Forcer le partitionnement manuel en répondant oui à la question

- ⚠ La présence d'une partition `/home` avec l'option `usrquota` est requise pour les modules **Horus**, **Scribe** et **AmonEcole**.
- ⚠ Si le mode conteneur est envisagé, le partitionnement doit prendre en compte le fait que les conteneurs sont mis en place dans le répertoire `/opt/lxc`.
- ⚠ La bonne répartition de l'espace disque résultant d'un partitionnement automatique n'est pas garanti sur un disque inférieur à 30Go.

Partitionnement manuel

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



Un volume logique nommé `keep_x` sans point de montage et sans système de fichiers contient l'espace qui n'a pas été attribué lors du calcul des autres volumes.

Sur un Eolebase il n'y a pas de volume proposé pour le point de montage `/home`.

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

```

[!!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés

Groupe de volumes LVM eolebase-vg, volume logique keep_1 - 17.9 G
n° 1 17.9 GB
Groupe de volumes LVM eolebase-vg, volume logique root - 9.5 GB L
n° 1 9.5 GB F ext4 /
Groupe de volumes LVM eolebase-vg, volume logique tmp - 2.0 GB Li
n° 1 2.0 GB F ext4 /tmp
SCSI2 (0,0,0) (sda) - 32.2 GB ATA QEMU HARDDISK
n° 1 primaire 2.0 GB F swap swap
n° 2 primaire 749.7 MB B F ext4 /boot
n° 3 primaire 29.4 GB K lvm

<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

- Sélectionner Supprimer un volume logique

```

[!!!] Partitionner les disques

Synthèse de la configuration du gestionnaire de volumes logiques :

Volumes physiques libres : 0
Volumes physiques utilisés : 1
Groupes de volumes : 1
Volumes logiques : 3

Action de configuration de LVM :

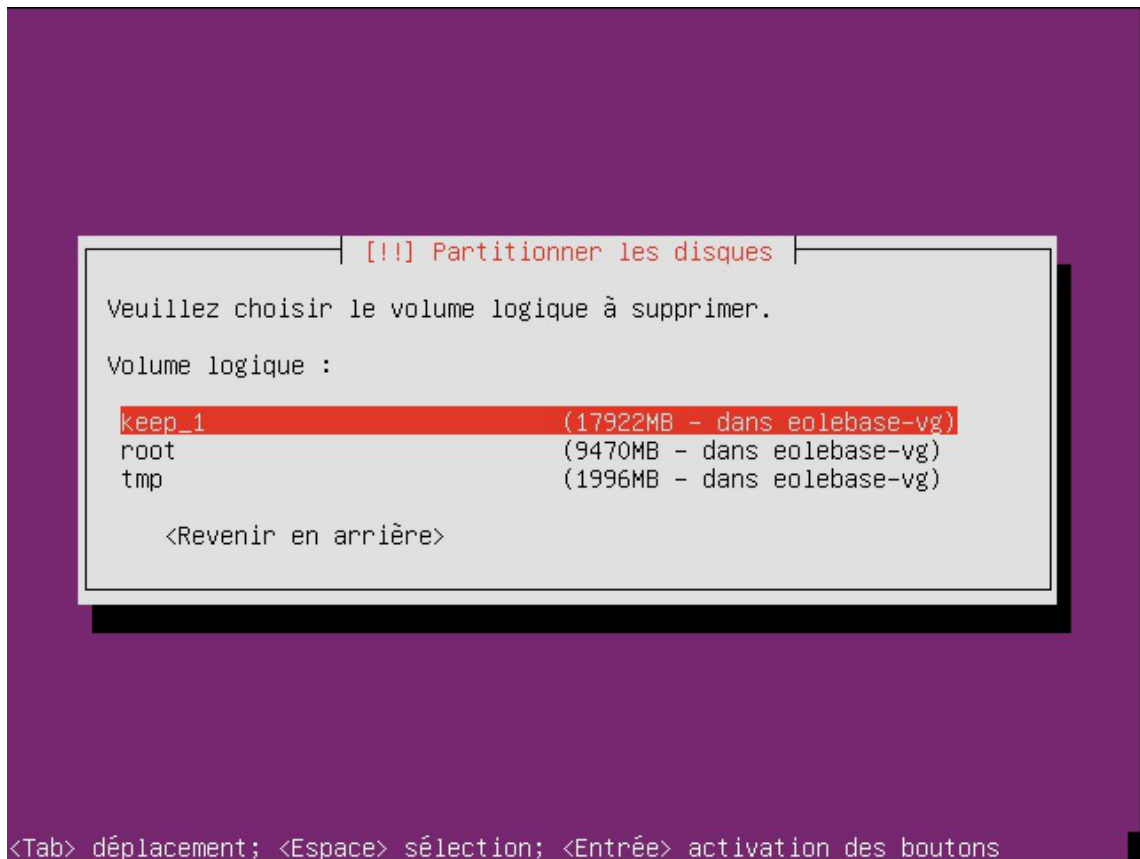
Afficher les détails de configuration
Créer un groupe de volumes
Créer un volume logique
Supprimer un volume logique
Etendre un groupe de volumes
Terminer

<Revenir en arrière>

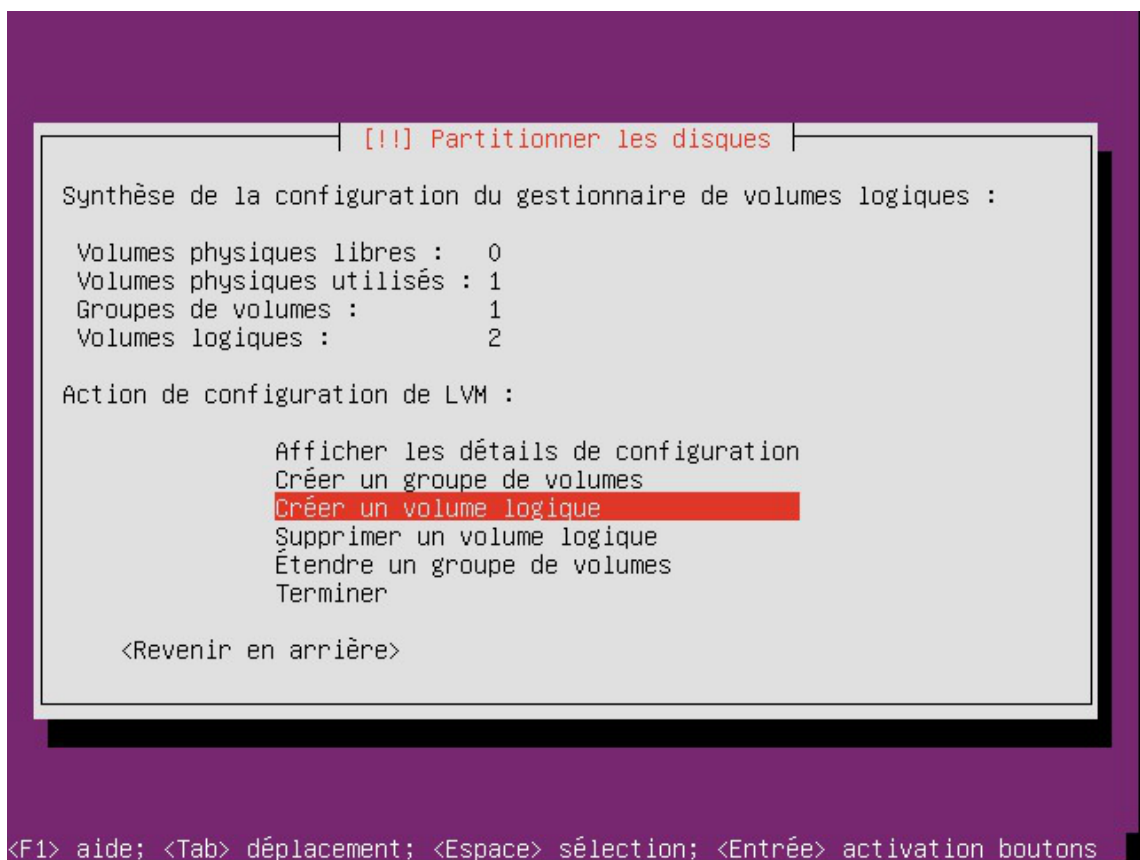
<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

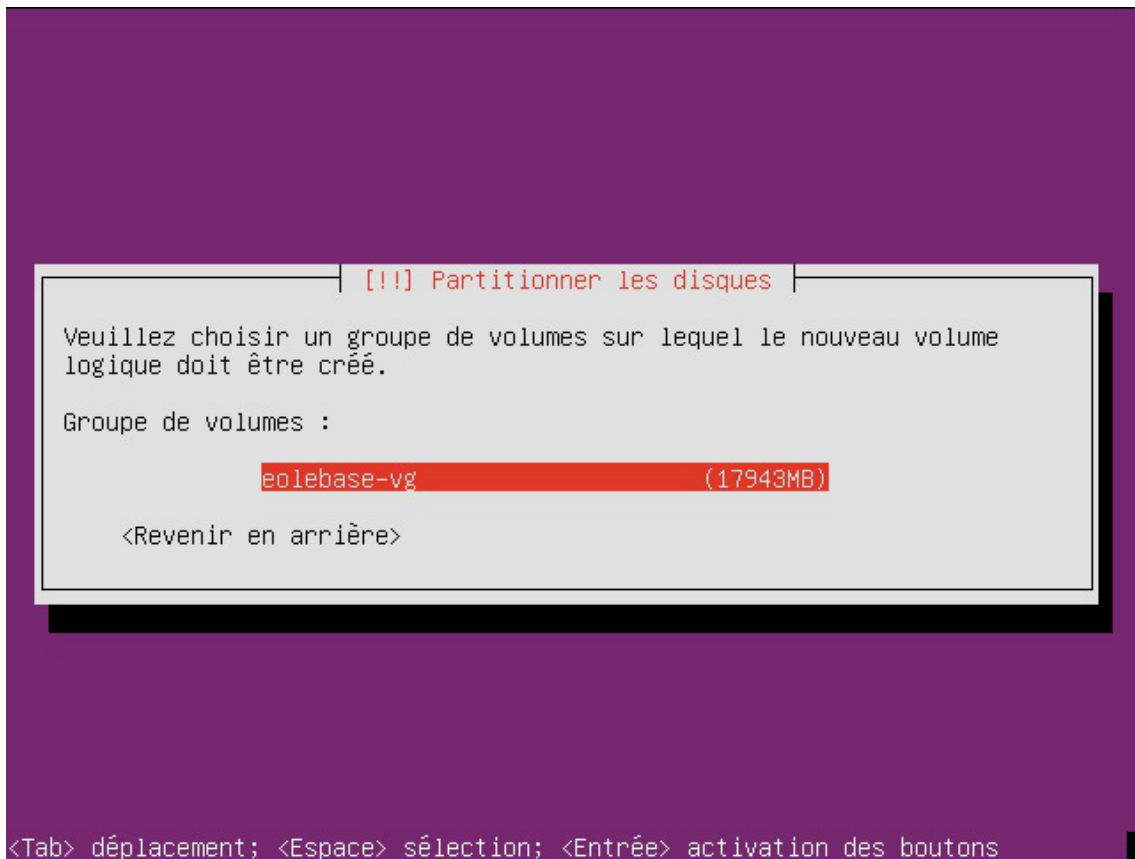
- Sélectionner le volume logique keep_x



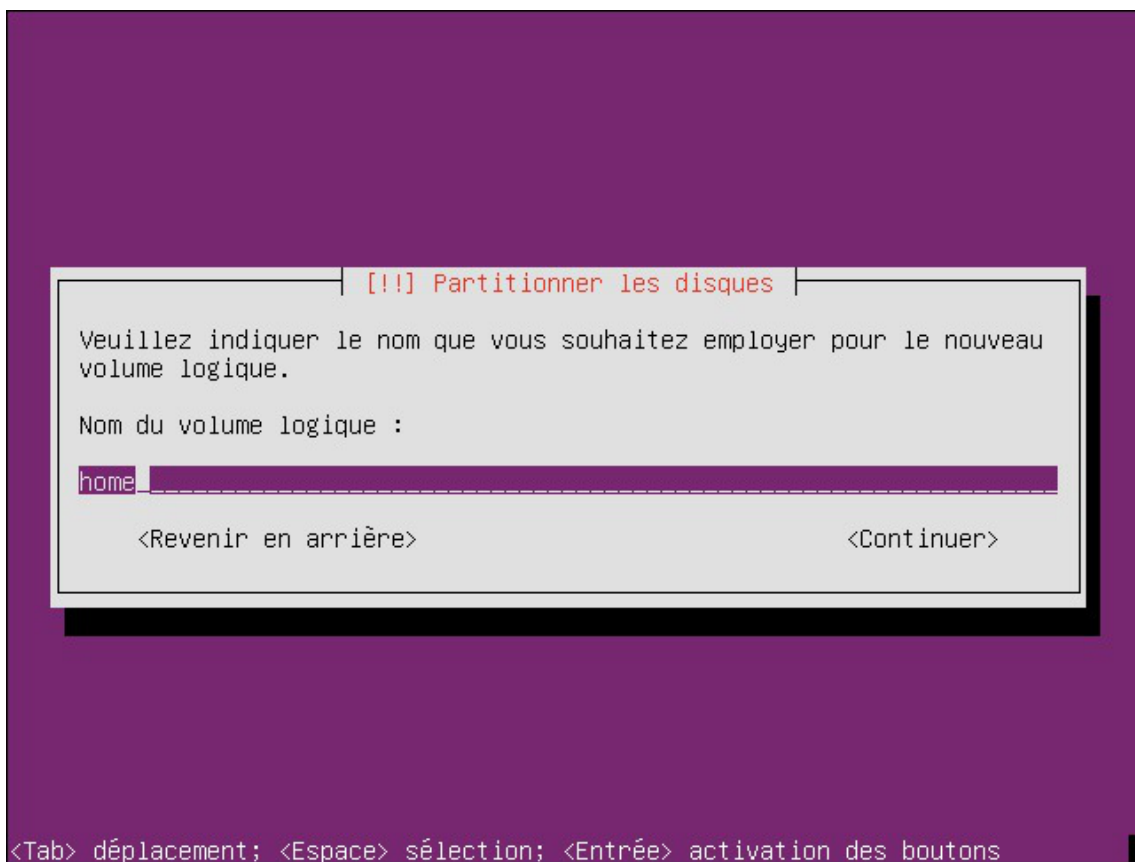
- De retour sur la gestion des volumes logiques, sélectionner **Créer un volume logique**



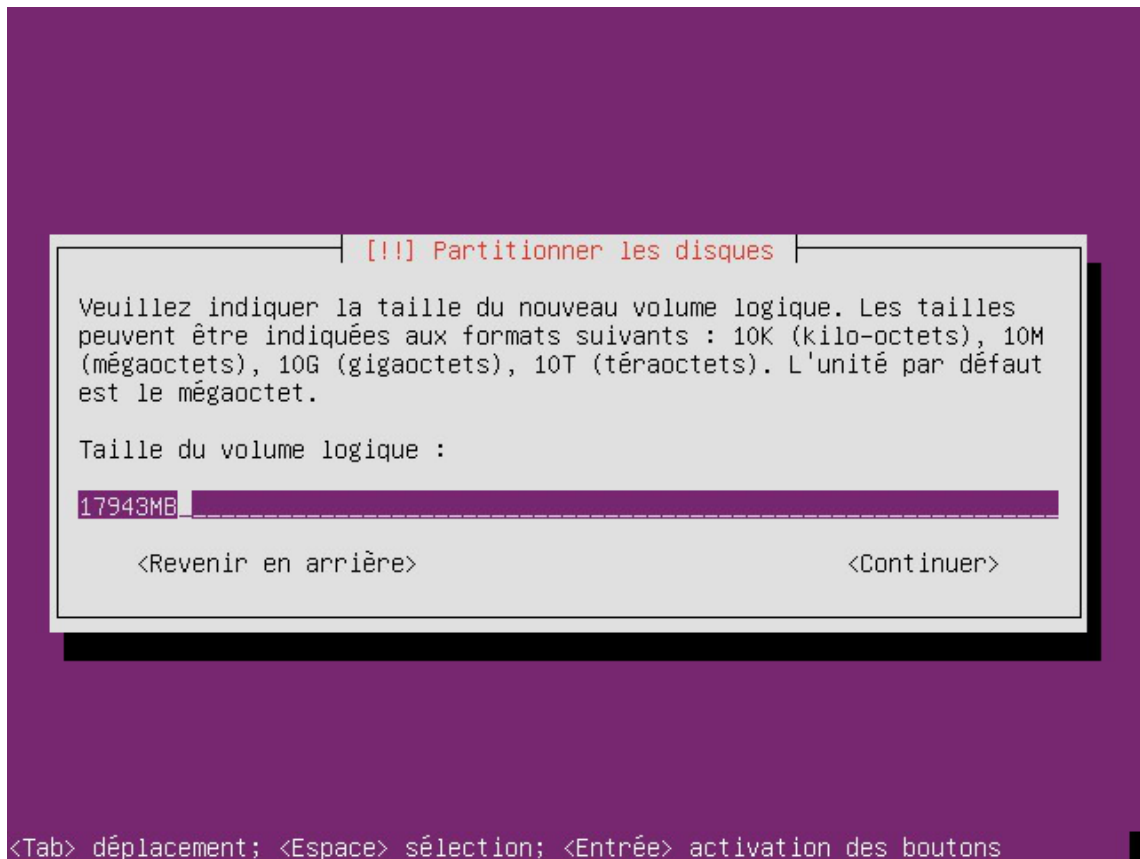
- Valider l'unique **Groupe de volumes** proposé



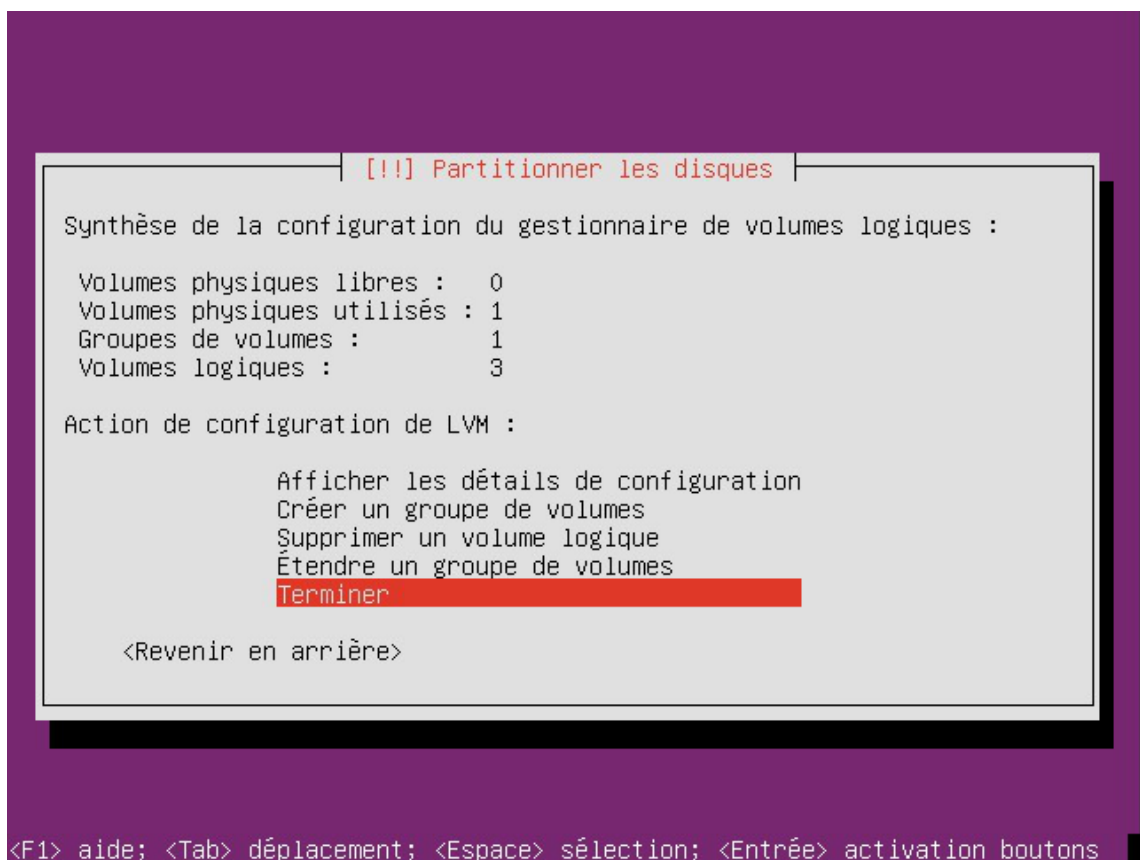
- Choisir le nom du nouveau volume logique



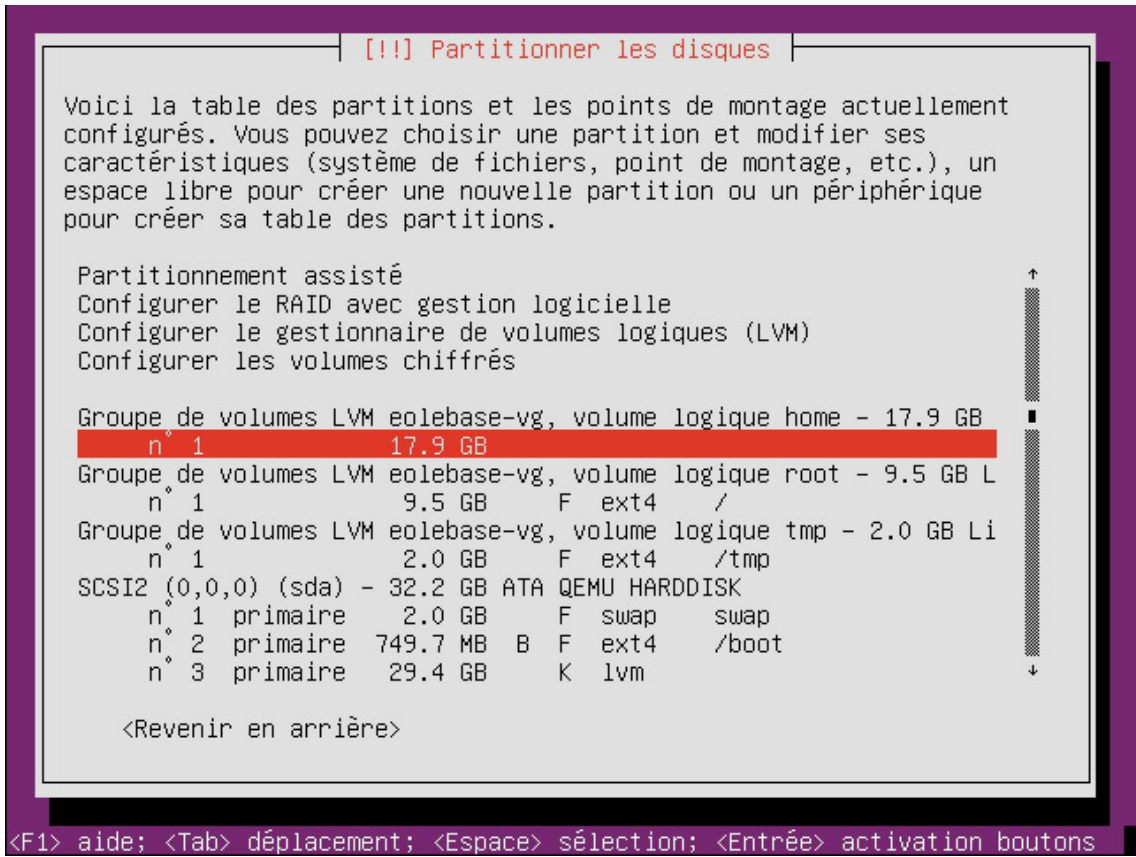
- Puis choisir l'espace à octroyer au nouveau volume, par défaut la taille affichée est la taille maximale



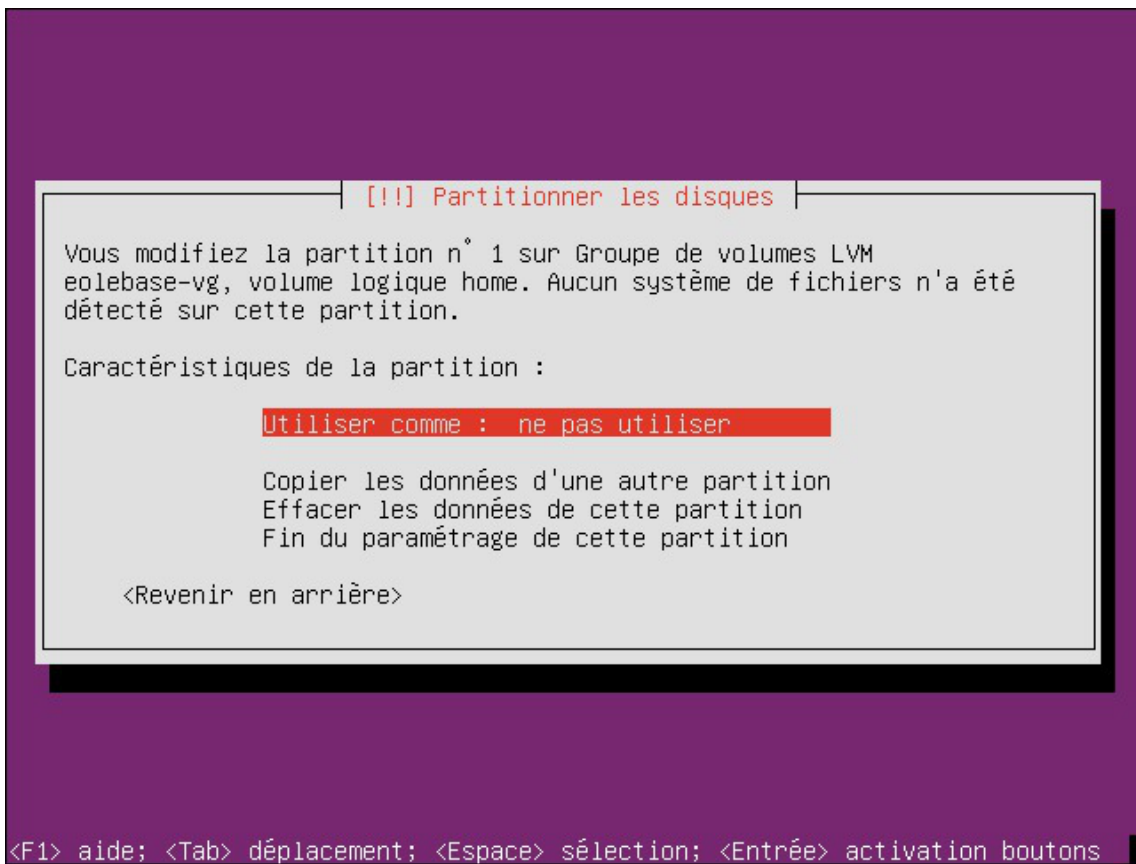
- De retour sur la synthèse de la configuration, sélectionner **Terminer**



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



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



- Sélectionner le type système de fichier

```

[!!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés

Groupe de volumes LVM eolebase-vg, volume logique home - 17.9 GB
n° 1 17.9 GB
Groupe de volumes LVM eolebase-vg, volume logique root - 9.5 GB L
n° 1 9.5 GB F ext4 /
Groupe de volumes LVM eolebase-vg, volume logique tmp - 2.0 GB Li
n° 1 2.0 GB F ext4 /tmp
SCSI2 (0,0,0) (sda) - 32.2 GB ATA QEMU HARDDISK
n° 1 primaire 2.0 GB F swap swap
n° 2 primaire 749.7 MB B F ext4 /boot
n° 3 primaire 29.4 GB K lvm

<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

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

```

[!!!] Partitionner les disques

Vous modifiez la partition n° 1 sur Groupe de volumes LVM
eolebase-vg, volume logique home. Aucun système de fichiers n'a été
détecté sur cette partition.

Caractéristiques de la partition :

Utiliser comme : système de fichiers journalisé ext4
Point de montage : /home
Options de montage : usrquota
Étiquette : aucune
Blocs réservés : 5%
Utilisation habituelle : standard

Copier les données d'une autre partition
Effacer les données de cette partition
Fin du paramétrage de cette partition

<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

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

```

[!!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Configurer les volumes chiffrés

Groupe de volumes LVM eolebase-vg, volume logique home - 17.9 GB
n° 1          17.9 GB    f  ext4    /home
Groupe de volumes LVM eolebase-vg, volume logique root - 9.5 GB L
n° 1          9.5 GB    F  ext4    /
Groupe de volumes LVM eolebase-vg, volume logique tmp - 2.0 GB Li
n° 1          2.0 GB    F  ext4    /tmp
SCSI2 (0,0,0) (sda) - 32.2 GB ATA QEMU HARDDISK
n° 1 primaire  2.0 GB    F  swap    swap
n° 2 primaire  749.7 MB B  F  ext4    /boot
n° 3 primaire  29.4 GB    K  lvm

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
<Revenir en arrière>

<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

- Sélectionner **Terminer le partitionnement et appliquer les changements**.

```

[!!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Configurer les volumes chiffrés

Groupe de volumes LVM eolebase-vg, volume logique home - 17.9 GB
n° 1          17.9 GB    f  ext4    /home
Groupe de volumes LVM eolebase-vg, volume logique root - 9.5 GB L
n° 1          9.5 GB    F  ext4    /
Groupe de volumes LVM eolebase-vg, volume logique tmp - 2.0 GB Li
n° 1          2.0 GB    F  ext4    /tmp
SCSI2 (0,0,0) (sda) - 32.2 GB ATA QEMU HARDDISK
n° 1 primaire  2.0 GB    F  swap    swap
n° 2 primaire  749.7 MB B  F  ext4    /boot
n° 3 primaire  29.4 GB    K  lvm

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
<Revenir en arrière>

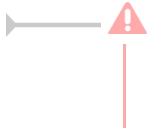
<F1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

```

Ajouter de l'espace disque à un volume LVM

Sur le nouveau périphérique physique, créer une partition de type Linux LVM (8E), avec `cdisk` par exemple.

La nouvelle partition s'appelle par exemple `/dev/sdb1` et peut être ajoutée au volume, par exemple pour agrandir `/var`.



Après avoir créé la nouvelle partition `/dev/sdb1` il peut être nécessaire de redémarrer le serveur pour la faire prendre en compte par le système.

Démonter la partition

Pour démonter la partition

```
# umount /var
```

Créer un volume physique

Créer un volume physique avec la nouvelle partition :

```
# pvcreate /dev/sdb1
```

Quel est le groupe de volumes

Rechercher dans quel groupe de volumes (VG Name) se trouve le volume logique `/var` :

```
1 root@scribe:/dev/mapper# lvdisplay /dev/scribe-vg/var
2 --- Logical volume ---
3 LV Path                /dev/scribe-vg/var
4 LV Name                 var
5 VG Name                 scribe-vg
6 LV UUID                 N4dHMU-htpz-AhEI-x5Ld-EvpM-ZFJX-M3LbHD
7 LV Write Access        read/write
8 LV Creation host, time scribe, 2017-01-16 19:17:09 +0100
9 LV Status               available
10 # open                 1
11 LV Size                 8,35 GiB
12 Current LE             2138
13 Segments               1
14 Allocation              inherit
15 Read ahead sectors     auto
16 - currently set to    256
17 Block device           252:3
18
19 root@scribe:/dev/mapper#
```

Ajouter ce volume physique au groupe de volumes contenant le volume logique `/var`, ici `scribe-vg` :

```
# vgextend scribe-vg /dev/sdb1
```

Agrandir le volume logique

Agrandir le volume logique correspondant à `/var` avec le nouvel espace libre :

```
# lvextend -l +100%FREE /dev/scribe-vg/var
```

```
# e2fsck -f /dev/scribe-vg/var
```

```
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM



Sur un serveur où une partition est saturée.

```

1 root@scribe:~# df -h
2 Sys. de fichiers          Taille Utilisé Dispo Uti% Monté sur
3 udev                      1,5G      0 1,5G   0% /dev
4 tmpfs                     301M      52M 250M  18% /run
5 /dev/mapper/scribe--vg-root 9,1G    2,6G 6,0G  30% /
6 tmpfs                     1,5G      28K 1,5G   1% /dev/shm
7 tmpfs                     5,0M      0 5,0M   0% /run/lock
8 tmpfs                     1,5G      0 1,5G   0% /sys/fs/cgroup
9 /dev/sda1                 687M    107M 531M  17% /boot
10 /dev/mapper/scribe--vg-tmp 1,8G    3,4M 1,7G   1% /tmp
11 /dev/mapper/scribe--vg-var 8,1G     8G 0,1G  99% /var
12 /dev/mapper/scribe--vg-home 18G    149M 18G   1% /home
13 tmpfs                    301M      0 301M   0% /run/user/0
14 root@scribe:~#

```

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.

Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

Pour démonter le périphérique :

```
root@scribe:~# umount /home
```

Si le périphérique est occupé, la commande `lsof` renvoie les programmes utilisant la partition :

```
# lsof | grep home
```

Il faut alors arrêter les services concernés puis démonter la partition.

Vérifier le support

Pour vérifier le support, lancer la commande :

```
# fsck -f /dev/mapper/scribe--vg-home
```

Diminuer la taille de la première partition

Réduire le système de fichiers :

```
# resize2fs -p /dev/scribe-vg/home 1G
```

Réduire la partition logique :

```
# lvresize -L-1G /dev/scribe-vg/home
```

Vérifier l'intégrité du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/home
```

Vérifier l'espace libéré

Pour vérifier que l'espace a bien été libéré il faut utiliser la commande `vgdisplay` :

```

# vgdisplay
1 root@scribe:~# vgdisplay
2 --- Volume group ---
3 VG Name          scribe-vg
4 System ID
5 Format           lvm2

```



```

6 Metadata Areas          1
7 Metadata Sequence No   6
8 VG Access               read/write
9 VG Status               resizable
10 MAX LV                 0
11 Cur LV                 5
12 Open LV                5
13 Max PV                 0
14 Cur PV                 1
15 Act PV                 1
16 VG Size                39,30 GiB
17 PE Size                4,00 MiB
18 Total PE               10060
19 Alloc PE / Size        10060 / 39,30 GiB
20 Free PE / Size         0 / 0
21 VG UUID                hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3
22
23 root@scribe:~#

```

La ligne `Free PE / Size` affiche l'espace libre.

Agrandir la taille de la deuxième partition

Les agrandissements peuvent se faire à chaud, ce qui est recommandé si la partition contient les commandes.

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/var
```

Agrandir la partition logique :

```
# lvresize -L+1G /dev/scribe-vg/var
```

Étendre le système de fichiers (sans option le système de fichiers prend toute la place possible) :

```
# resize2fs /dev/scribe-vg/var
```

Remonter le périphérique

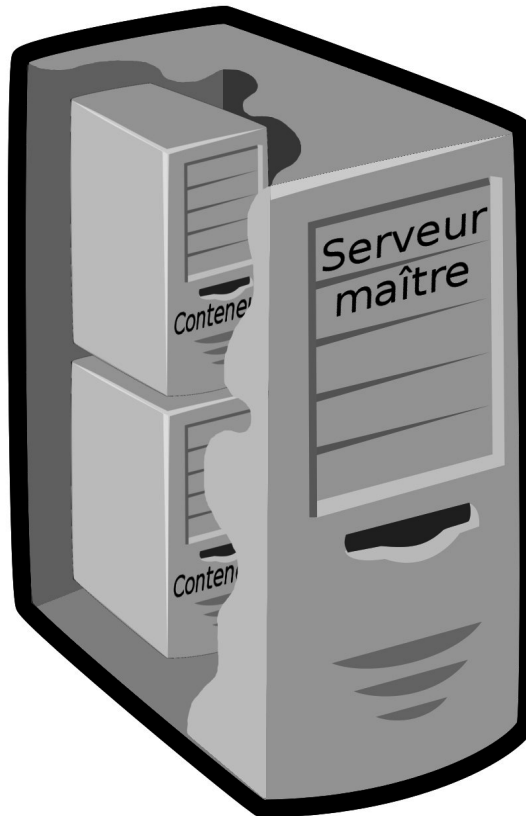
Procéder au montage du périphérique avec la commande `mount` :

```
# mount /var/home
```

Pensez à redémarrer les services qui ont précédemment été arrêtés.

5. Choisir le mode du module

Module



EOLE propose un système évolué et cohérent de conteneurs^[p.543].

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

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

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

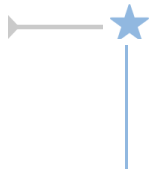
EOLE utilise les conteneurs pour séparer des processus sans augmenter le nombre de serveurs physiques.

Modules en mode non conteneur

La quasi totalité des modules EOLE 2.5 sont installables en mode non conteneur :

- [Amon](#) ;
- [eSBL](#) ;
- [eCDL](#) ;
- [Hâpy](#) et ses dérivés ;
- [Horus](#) ;

- `Scribe` ;
- `Seshat` ;
- `Thot` ;
- `Sphynx` ;
- `Zéphir`.



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

Mise à jour du module

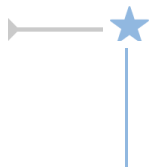
Après l'installation du module, la mise à jour n'est pas obligatoire mais fortement recommandée. Pour effectuer la mise à jour du module, utiliser la commande : `Maj-Auto`.

Module en mode conteneur

Contrairement à ceux cités précédemment, le module `AmonEcole` installable **obligatoirement** en *mode conteneur*.

Sur ce module, certains services installés sont dans différents conteneurs et ne sont pas compatibles entre eux. L'installation en *mode non conteneur* est donc impossible.

À partir d'un module



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

Mise à jour du module

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

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

Installation des conteneurs

La génération des conteneurs se fait à l'aide de la commande `gen_conteneurs`.

Les conteneurs seront installés sur le réseau **192.0.2.0/24**.

Le masque sera obligatoirement 255.255.255.0.

Attention si ce réseau est déjà utilisé dans votre architecture.

Comme sur la version 2.4 il n'est plus possible, sur un module en version 2.5.x, d'installer les conteneurs sur un réseau différent.

Des logs sur la génération des conteneurs sont disponibles après la génération des conteneurs dans le fichier `/var/log/isolation.log`.

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

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande `gen_conteneurs` suivie du paramètre `-h` permet d'obtenir de l'aide.

À partir d'EoleBase

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

La procédure recommandée actuellement est la suivante :

- installer un module `Eolebase`
- mettre à jour la liste des paquets :
`Query-Auto` ou `Query-Cd`
- installer le paquet `eole-lxc-controller` :
`apt-eole install eole-lxc-controller`
- installer le paquet méta-paquet du module souhaité (exemple : `eole-scribe-module`, `eole-amon-module`) :
`apt-eole install eole-scribe-module`

Mise à jour du module

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

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

Installation des conteneurs

La génération des conteneurs se fait à l'aide de la commande `gen_conteneurs`.

Les conteneurs seront installés sur le réseau **192.0.2.0/24**.

Le masque sera obligatoirement 255.255.255.0.

Attention si ce réseau est déjà utilisé dans votre architecture.

Comme sur la version 2.4 il n'est plus possible, sur un module en version 2.5.x, d'installer les conteneurs sur un réseau différent.

Des logs sur la génération des conteneurs sont disponibles après la génération des conteneurs dans le fichier `/var/log/isolation.log`.

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

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande `gen_conteneurs` suivie du paramètre `-h` permet d'obtenir de l'aide.

⚠ Il n'est pas possible de passer du mode non conteneur au mode conteneur et vice versa.

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

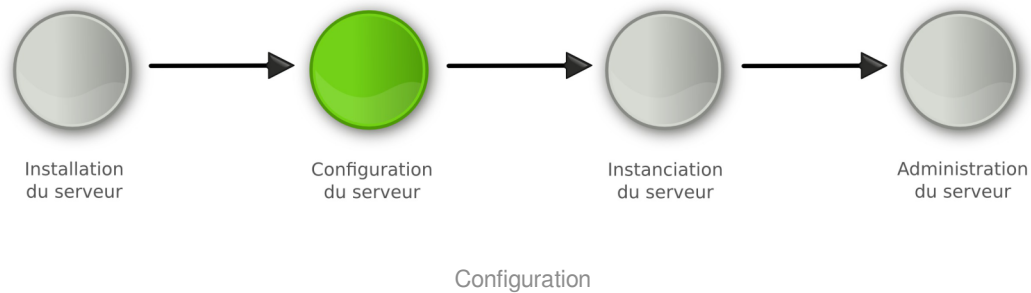
⚠ Si le mode conteneur est envisagé, le partitionnement doit prendre en compte le fait que les conteneurs sont mis en place dans le répertoire `/opt/lxc`.

Voir aussi...

Les mises à jour ^[p.336]

Chapitre 6

Configuration du module Amon



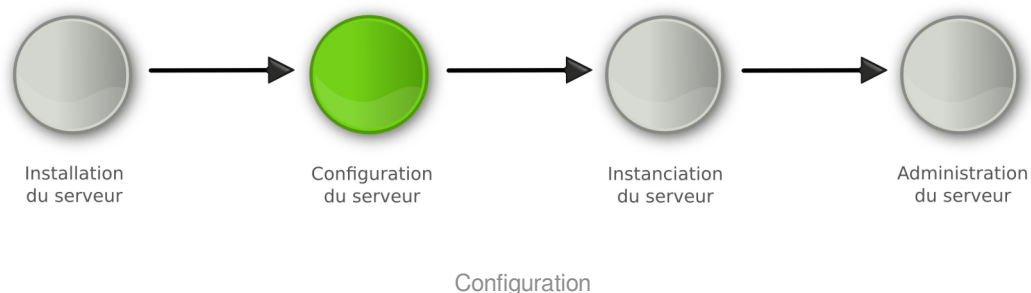
- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config`.

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

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

Cette phase de configuration peut permettre de prendre en compte des paramétrages de fichiers de configuration de produits tels que Squid^[p.561], e2guardian^[p.545], etc.

1. Configuration généralités



La configuration suit la phase d'installation du serveur.

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

Les paramètres saisis peuvent être internes au serveur (par exemple le nombre d'interfaces réseau) ou externes (par exemple l'adresse du DNS^[p.545], l'adresse du serveur de temps NTP^[p.556], ...). Cette étape nécessite une bonne connaissance de l'architecture réseau dans laquelle sera installé le serveur.

À condition d'avoir renseigné les valeurs obligatoires vous pouvez enregistrer la configuration pour l'effectuer en plusieurs temps.

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

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

Il existe deux modes de configuration :

- **mode autonome**

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

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

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

- **mode Zéphir**

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

1.1. Configuration en mode autonome

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

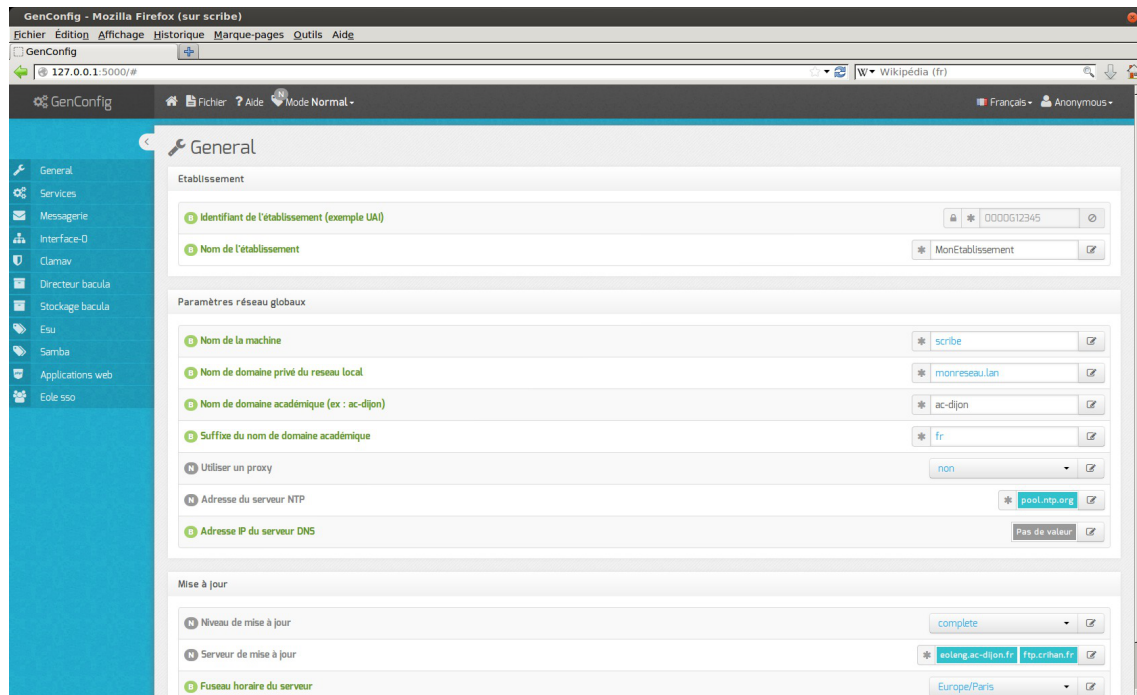
Ce mode est recommandé pour la configuration d'un petit nombre de serveurs.

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

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

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

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



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

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



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

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



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

L'interface se découpe en quatre zones :

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

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

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

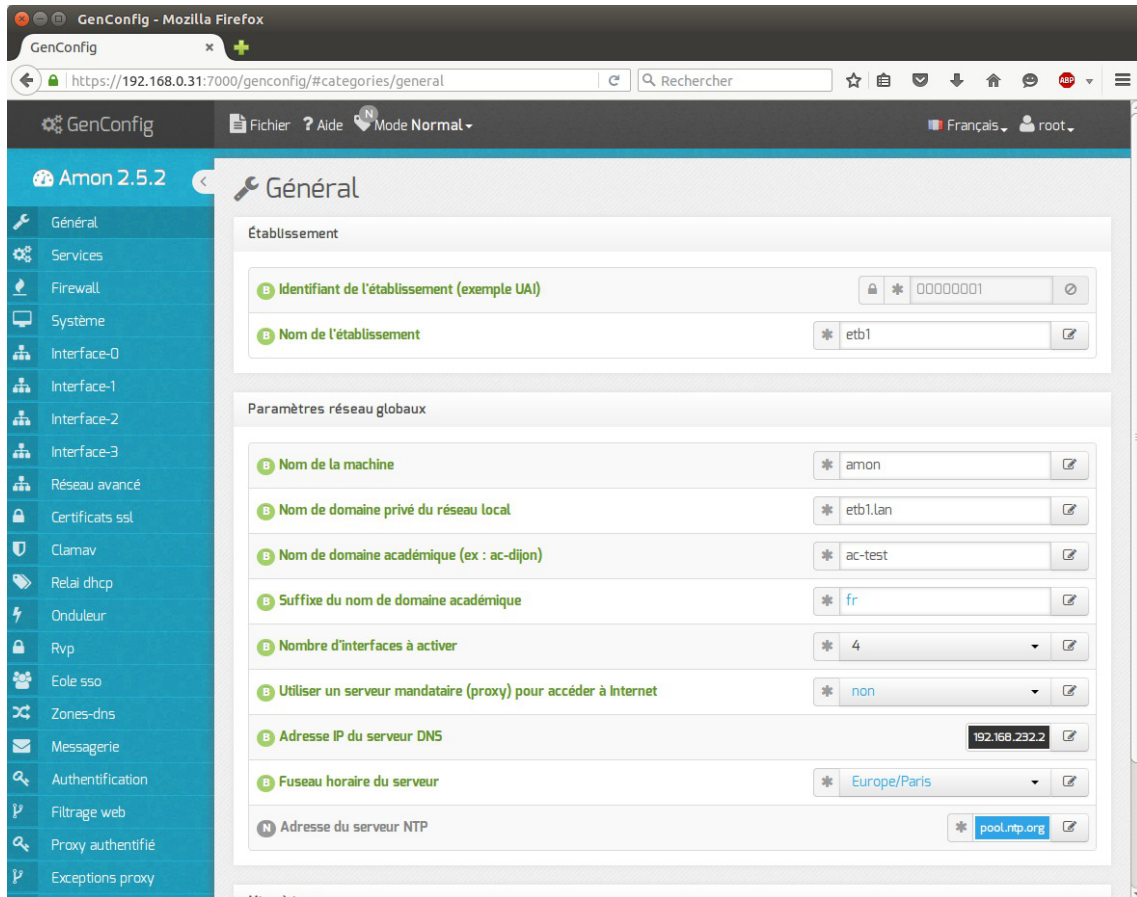
1.1.1. Accès distant

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

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

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

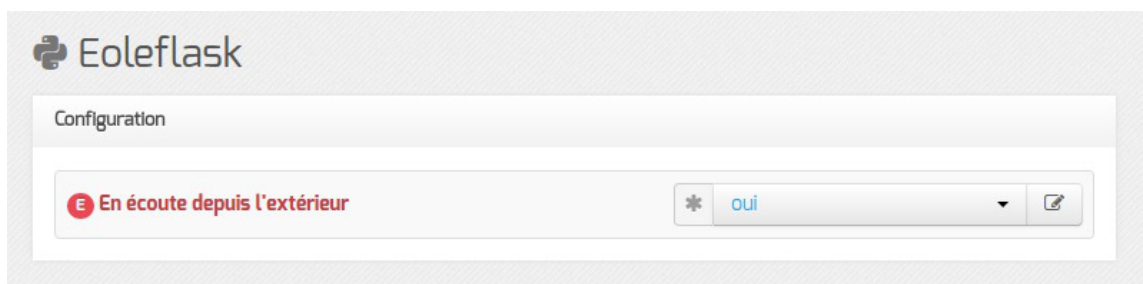
Il faut ensuite valider les certificats pour pouvoir accéder à l'interface.



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

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

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



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

1.1.2. La zone Menu

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

- Fichier : gestion de la configuration
- Aide : permet de lancer l'assistant et d'afficher l'aide de l'application

- Mode : choix des modes de configuration à activer
- Langue : choix de la langue pour l'interface
- Session : permet de se déconnecter.

Sous-menu Fichier

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



Sous menu Fichier

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

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

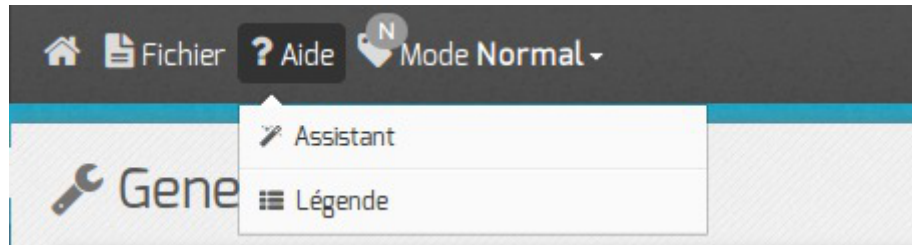
Re-synchroniser la configuration permet de récupérer les informations stockées en session sur le serveur si une coupure arrivait pendant la configuration.

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

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

Sous-menu Aide

- Assistant
- Légende



Sous menu Aide

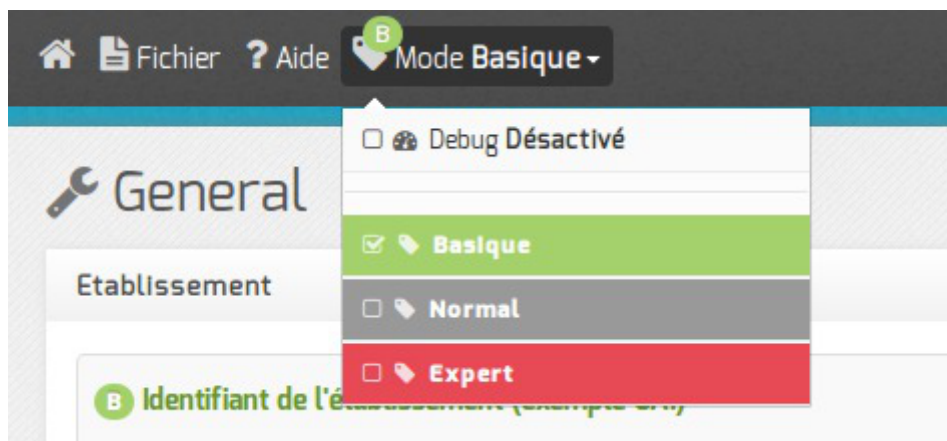
L'assistant bascule l'interface de configuration du module en mode *Basique* et propose une page synthétique qui récapitule l'essentiel des variables à configurer.

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

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

Sous-menu Mode

- Debug
- Basique
- Normal
- Expert



Sous menu Mode

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

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

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

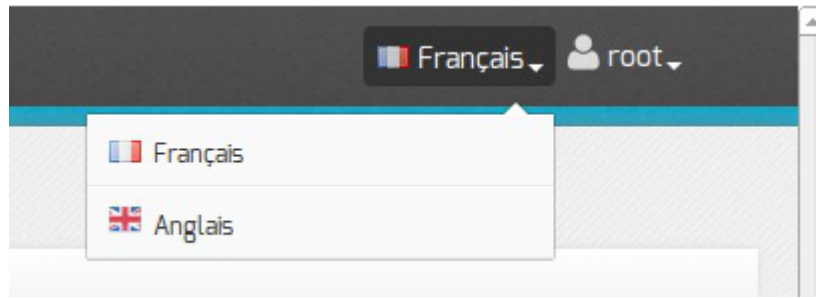
Le mode *Expert* active les onglets et les variables pour une configuration avancée.

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

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

Sous-menu Langue

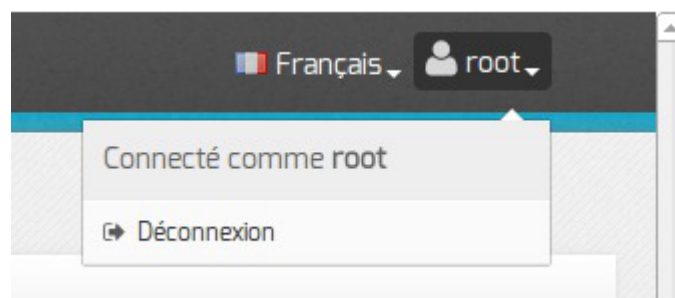
- Français
- Anglais



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

Sous-menu Session

- Connecté comme
- Déconnexion



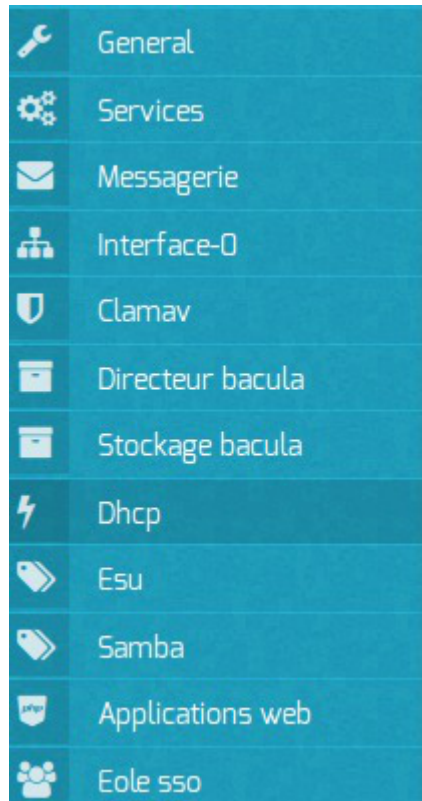
Session permet de connaître l'utilisateur courant et de se déconnecter.

1.1.3. La zone Onglet

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

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

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



L'onglet courant

1.1.4. La zone Formulaire

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

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

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



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

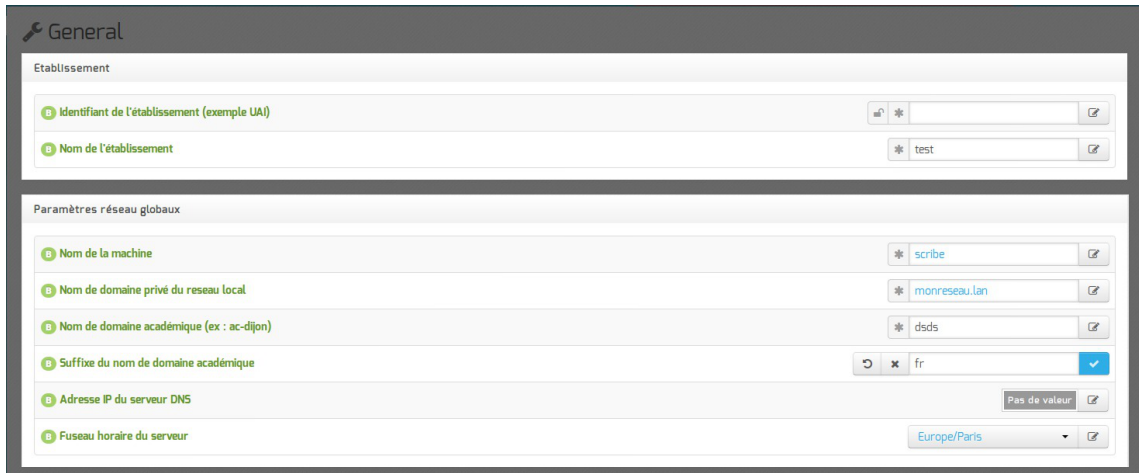


La légende de chaque icône se trouve dans l'aide de l'interface : **Aide** / **Légende** .

Regroupement des paramètres par bloc

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

Chaque bloc regroupe un ou plusieurs paramètres.

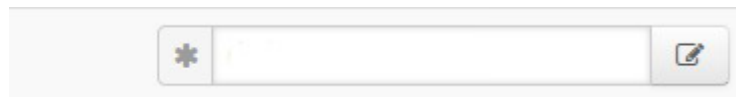


Les blocs thématiques

Les variables obligatoires

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

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



Les variables obligatoires sont précédées d'une étoile

Les variables des modes basiques, normales et expertes

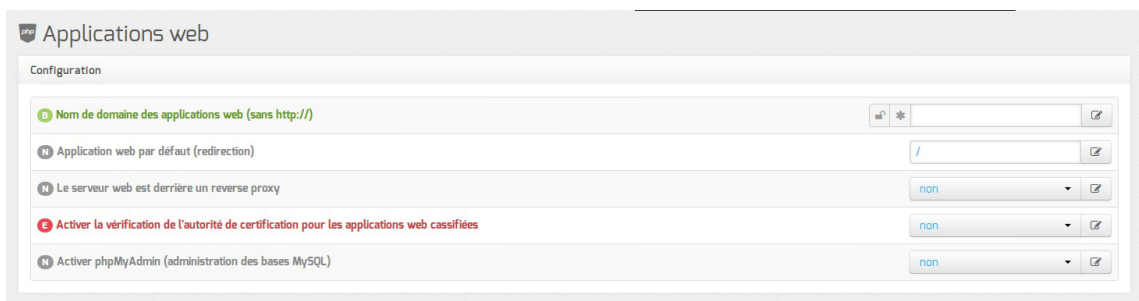
Le mode détermine l'affiche de variable plus ou moins complexes : basiques, normales ou expertes.

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

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

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

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



Les variables et leur niveau de complexité

Les variables simples

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

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

Établissement

B Identifiant de l'établissement (exemple UAI)	🔒 * 0000G12345	🗑️
B Nom de l'établissement	* MonEtablissement	✎

Les variables multiples

Certains paramétrages peuvent accueillir plusieurs valeurs, nous parlons alors de variable multiple. Les variables multiples se présentent sur fond coloré :

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

pool.ntp.org ✎

Pas de valeur ✎

Apparence graphique des variables multiples

Pour ajouter une valeur, il faut cliquer sur modifier pour faire apparaître le champ de saisie. Pour supprimer une valeur, il faut d'abord cliquer sur modifier puis sur la croix à droite du champ.

pool.ntp.org ✕ ↺ ✕ Ajouter ✓

Édition d'une variable multiple

Les variables multiples groupées

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

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

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

Validation des variables

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

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

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

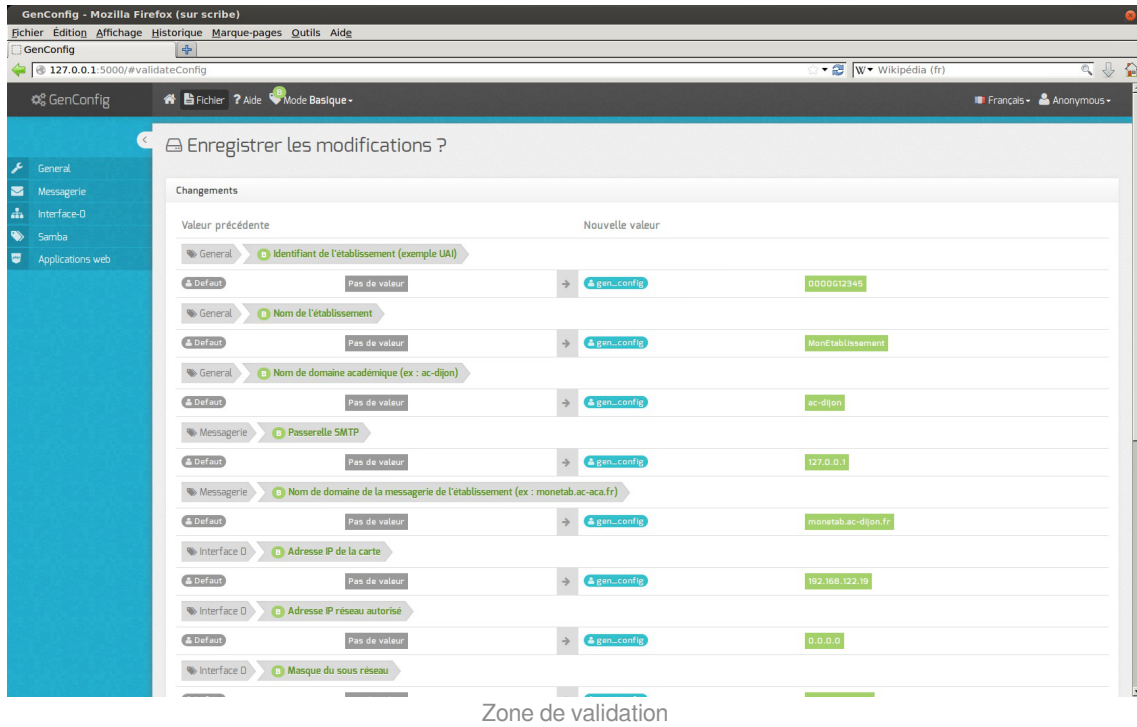
Validation d'une variable

1.1.5. La zone Validation

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

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

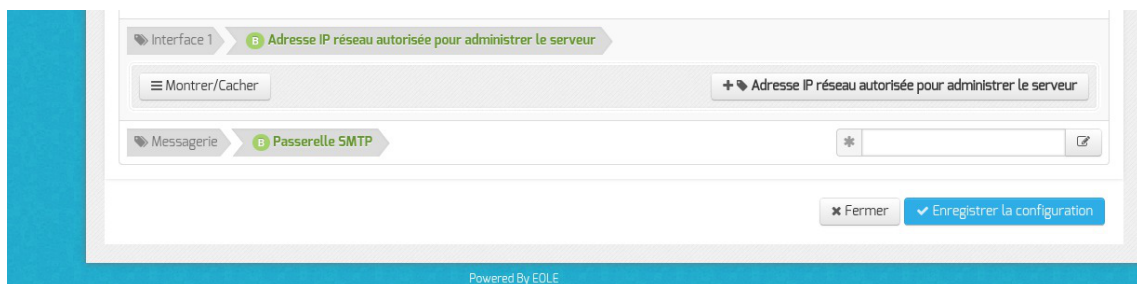
Lors d'une réédition de la configuration cette zone ne montre que les changements qui ont eu lieu.



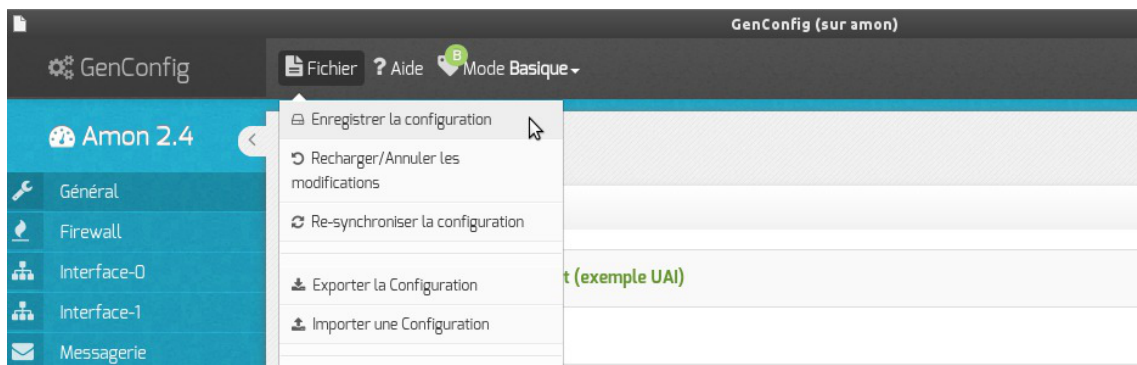
Zone de validation

1.1.6. Enregistrer la configuration

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



Dans les autres cas l'enregistrement de la configuration se fait en cliquant sur **Enregistrer la configuration** dans le menu **Fichier**.



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

Les différentes valeurs attribuées aux variables sont enregistrées dans un fichier `config.eol` au format

JSON^[p.550] dans le répertoire `/etc/eole/`.

Il convient donc de réaliser les modifications sur ce fichier en utilisant l'interface de configuration du module.



Un fichier `config.eol.bak` est 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.

À chaque reconfiguration du serveur, si la configuration a changé, un fichier `config.eole.bak.1` est généré. Celui-ci est une copie de l'avant-dernière configuration fonctionnelle.

S'il existe une différence entre les fichiers `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

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

Cela se traduit par des erreurs de timeout^[p.562] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Gunicorn^[p.549].



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

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

```
# CreoleService eoleflask restart
```

1.1.7. Le mode Debug

Dans la zone de Menu le sous-menu Mode propose le mode Debug.

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

Les valeurs des variables peuvent être modifiées par différentes applications.

En gris, à droite du nom de la variable, est précisé le nom de l'application et/ou de l'action ayant modifié en dernier sa valeur :

- `default` : valeur par défaut et/ou calculée (n'est jamais enregistrée dans le fichier `config.eol`) ;
- `gen_config` : valeur modifiée par l'interface de configuration du module ;
- `creoleset` : valeur modifiée avec la commande `CreoleSet` ;
- `zephir` : valeur modifiée pour un serveur donné dans l'interface web de Zéphir ;
- `variante` : valeur par défaut de la variante Zéphir ;
- `module` : valeur par défaut du module dans Zéphir ;
- `import` : valeur récupérée depuis un fichier de configuration importé dans l'interface de configuration du module ;
- `zephir_import` : valeur récupérée depuis un fichier de configuration importé dans l'interface web de Zéphir ;
- `upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE ;
- `zephir_upgrade` : valeur récupérée depuis un fichier de configuration d'une version antérieure d'EOLE dans l'interface web de Zéphir.



Cette information est également enregistrée dans le fichier de configuration `config.eol` du module.

La clé associée à cette valeur est `owner` :

```
"numero_etab": {"owner": "gen_config", "val": "0000000A"}
```

Voir aussi...

La zone Menu [p.66]

1.1.8. FAQ

Certaines interrogations reviennent souvent et ont déjà trouvées une ou des réponses.



Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.



Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :

1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet `Eoleflask`.
2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.

Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

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

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.



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

configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.

S'il existe une différence entre `config.eol` et `config.eole.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Comment modifier la valeur d'une variable verrouillée

Il est vivement recommandé de ne pas éditer manuellement le fichier `config.eol` pour éviter les erreurs de frappe ou de type de données.



Exporter puis importer le fichier de configuration courant permet de passer outre le verrouillage des variables.



Cette astuce demande une bonne maîtrise des implications que peut avoir le changement d'une valeur verrouillée. Et une valeur n'est jamais verrouillée sans raison.

Par exemple, le changement de l'identifiant de l'établissement ne se répercute pas sur l'annuaire dont le schéma n'est construit qu'une fois au moment de l'instance du serveur.



Pour modifier la valeur verrouillée Identifiant de l'établissement :

- ouvrir l'interface de configuration du module ;
- importer le fichier de configuration courant : `Fichier` → `Importer une Configuration` → `/etc/eole/config.eol` ;
- modifier la valeur de l'identifiant de l'établissement ;
- enregistrer la configuration : `Fichier` → `Enregistrer la configuration` ;
- procéder à une reconfiguration du serveur à l'aide de la commande `reconfigure` .

Erreurs de timeout ou erreur 504 avec Nginx

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

Cela se traduit par des erreurs de timeout^[p.562] avec Nginx ou une `erreur 504 (méthode not allowed)` dans l'interface de configuration du module et `[ERROR] WORKER TIMEOUT (pid:XXXX)` dans les logs de Unicorn^[p.549].



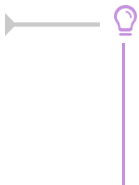
La valeur de timeout peut être changée à la ligne `timeout = '120'` dans le fichier de configuration de eoleflask : `/etc/eole/flask/eoleflask.conf`. Celui-ci n'est pas templatisé et n'est donc pas écrasé en cas de reconfiguration du serveur.

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

```
# CreoleService eoleflask restart
```

Interface de configuration en mode console

Impossible de trouver le mode console de l'interface de configuration du module.

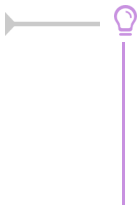


Le mode console a été supprimé par contre il est possible :

- d'accéder à distance à l'interface de configuration du module via un navigateur web ;
- d'utiliser la commande `CreoleSet` pour configurer une variable en ligne de commande.

Consultation des mots de passe dans l'interface de configuration

Sur les versions d'EOLE supérieures à 2.6.0, les valeurs des variables de type *password* sont masquées lorsque le champ n'est pas en mode édition, donc inaccessibles lorsque le champ est verrouillé.



La consultation d'un mot de passe non éditable (stocké dans une variable verrouillée par exemple) est possible en passant en mode Debug. Le mot de passe pouvant malgré tout apparaître tronqué, sa valeur intégrale est accessible dans l'info-bulle qui s'affiche lors du survol du champ.

1.2. Configuration en mode Zéphir

La configuration en mode Zéphir permet, au lancement de l'interface de configuration du module à l'aide de la commande `gen_config`, de faire apparaître un fenêtre d'identification qui permet de s'identifier avec un compte Zéphir. Les modifications apportées dans la configuration locale seront synchronisées avec le serveur Zéphir.

La configuration en mode Zéphir se fait en deux étapes :

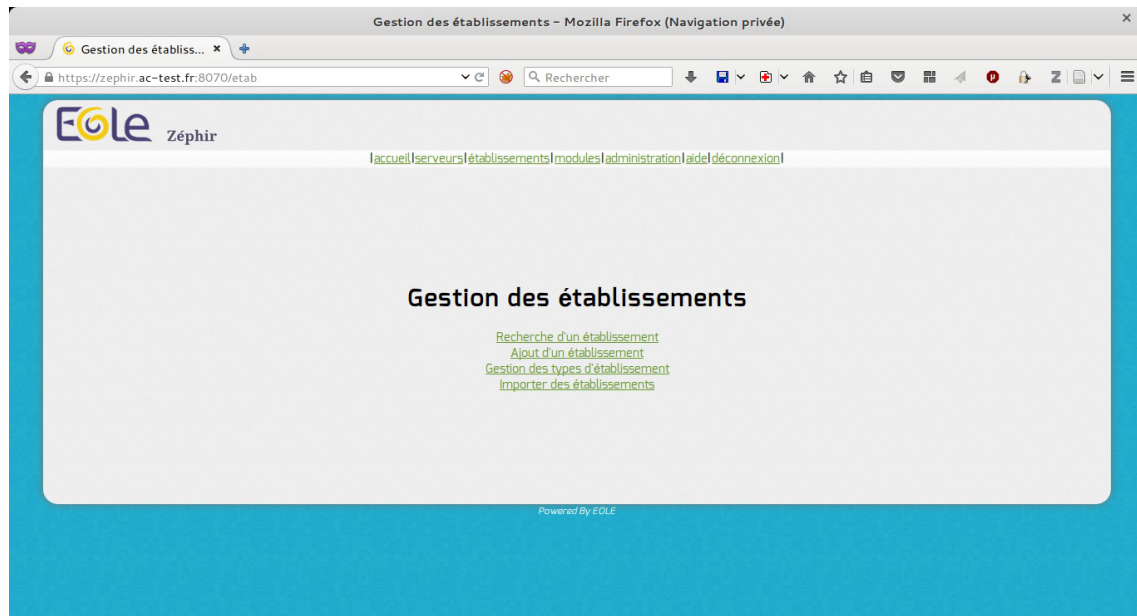
- configuration :
 - soit sur le serveur à enregistrer
 - soit sur le serveur Zéphir (utilisation éventuelle de variantes)
- enregistrement du serveur et synchronisation de la configuration.

Pré-requis

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

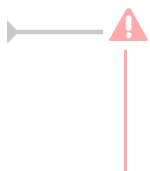
Enregistrement d'un établissement

Pour ajouter un établissement il faut se rendre dans l'application Zéphir et cliquer sur l'entrée `établissement` du menu.



Puis cliquer sur **Ajout d'un établissement**.

L'identifiant à saisir correspond au RNE de l'établissement (8 caractères maximum).



Le RNE est la seule information que l'on ne pourra pas modifier. Il faut donc prendre garde à saisir le bon numéro. En cas d'erreur, la seule solution sera de supprimer l'établissement fraîchement créé et le recréer.

Il faut ensuite renseigner la description de l'établissement (adresse physique, moyens de communication, ...).

(admin_zephir) Nouvel Étab - Mozilla Firefox (Navigation privée)

https://zephir.ac-test.fr:8070/etab/add2

Eole Zéphir

Accueil | serveurs | établissements | modules | administration | déconnexion

Remplissez les champs décrivant l'établissement

RNE 0000G123

Nom du site * Lycée Wikipédia

Adresse

Ville * Dijon

Code postal * 21000

Téléphone

Fax

Adresse électronique

Responsable

Remarques

Type d'établissement * LYCEE D ENSEIGNEMENT GENERAL

Ok Initialiser

[Retour à la gestion des établissements](#)

Powered By EOLE

Seuls les champs pourvus d'une * sont obligatoires (nom du site, ville, code postal et type d'établissement). Des types d'établissement peuvent être ajoutés dans [établissement / Gestion des types d'établissement](#) mais il faut le faire avant d'ajouter un nouvel établissement. Un fois validé avec le bouton [OK](#), l'établissement est créé.

L'établissement 0000G123 a bien été ajouté

[Affichage du détail de l'établissement](#)

Enregistrement d'un lot d'établissements

Il est possible d'importer un fichier texte comprenant la liste des établissements depuis l'application web Zéphir.

Pour cela il faut cliquer sur le menu [établissements](#) et choisir [Importer des établissements](#).

Importation d'établissements

Les établissements existants seront mis à jour

etablissement.csv

L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese^[p.559]) CSV^[p.544] avec comme séparateur un "|".

Les champs suivants sont attendus :

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

1 210024M | CLG | 340 | COLLEGE | CHAMPOLLION | 21000 | DIJON | ce.0210024M@ac-dijon.fr | 0380732

2 0210026P | CLG | 340 | COLLEGE | EPIREY | 21000 | DIJON | ce.0210026P@ac-dijon.fr | 0380732916 |

Après l'importation un rapport est affiché.

Import des établissements terminés

Les établissements suivants ont été créés :

Les établissements suivants ne sont pas référencés dans le fichier :

[retour au menu des établissements](#)

L'enregistrement

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

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

Configuration minimale du réseau

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

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



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

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

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

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



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

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

Déroulement de l'enregistrement

- saisir l'adresse du serveur Zéphir, ainsi qu'un nom d'utilisateur et un mot de passe autorisé en écriture dans l'application web Zéphir ;
- si le serveur n'a pas été pré-crée sur le serveur Zéphir, répondre `oui` à la question `Créer le serveur dans la base Zéphir ?` ;
- saisir le numéro RNE qui doit au préalable exister dans l'application Zéphir ;

- saisir le libellé du serveur ;
- répondre aux diverses questions sur le matériel ;
- répondre aux diverses questions sur l'installateur ;
- choisir un module et une variante dans les listes proposées ;
- synchronisation de la configuration :
 - si la configuration a été faite en mode autonome sur le module à enregistrer choisir **Sauver la configuration actuelle sur Zephir**
 - si la configuration a été réalisé sur le serveur Zéphir choisir **Récupérer les fichiers de variante sur Zéphir**
- un message indiquera que la configuration est bien sauvegardée et que les communications avec Zéphir sont configurées. Dans le cas où des paramètres du serveur ne seraient pas renseignés (paramètres provenant d'une variante), un message vous préviendra que ceux-ci doivent être saisis.

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

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

```
root@eolebase:~# enregistrement_zephir
Procédure d'enregistrement sur le serveur Zéphir
Entrez l'adresse du serveur Zéphir : 192.168.240.254
Entrez votre login pour l'application Zéphir (rien pour sortir) :
admin_zephir
Mot de passe pour l'application Zéphir pour admin_zephir :
Saisir l'adresse du serveur Zéphir, le compte et le mot de passe pour l'application Zéphir.
créer le serveur dans la base du serveur Zéphir (O/N) : o
Le script détecte que le module n'a jamais été enregistré et demande si vous souhaitez le
créer.
Etablissement du serveur (n° RNE) (0000G123 par défaut) :
libellé du serveur (eolebase Lycée de Dijon par défaut) :
matériel (Bochs () par défaut) :
processeur ( QEMU Virtual CPU version 1.0 2294 MHz par défaut) :
disque dur (43 Go par défaut) :
nom de l'installateur (admin_zephir par défaut) :
telephone de l'installateur :
commentaires :
Délai entre deux connexions à zephir
minutes (30 par défaut) :
** liste des modules disponibles **
```

```

47 amon-2.4
46 eolebase-2.4
42 horus-2.4
45 scribe-2.4
43 sentinelle-2.4
44 sphynx-2.4
48 thot-2.4
module (eolebase-2.4 par défaut):
** liste des variantes de ce module **
45 * standard
variante (45 par défaut):
Ici les paramètres proposés par défaut sont validés par un retour chariot.
** Configuration des communications vers le serveur Zéphir **
1 -> Ne rien faire
2 -> Récupérer les fichiers de variante sur le serveur Zéphir
3 -> Sauver la configuration actuelle sur le serveur Zéphir
4 -> Modifier la variante du serveur
Entrez le numéro de votre choix : 3
Pour l'enregistrement il faut choisir l'option 3.
-- sauvegarde en cours (veuillez patienter) --
-- OK --
--récupération des patchs et dictionnaires (veuillez patienter)--
** le numéro attribué à ce serveur sur le serveur Zéphir est : 1
**
root@eolebase:~#

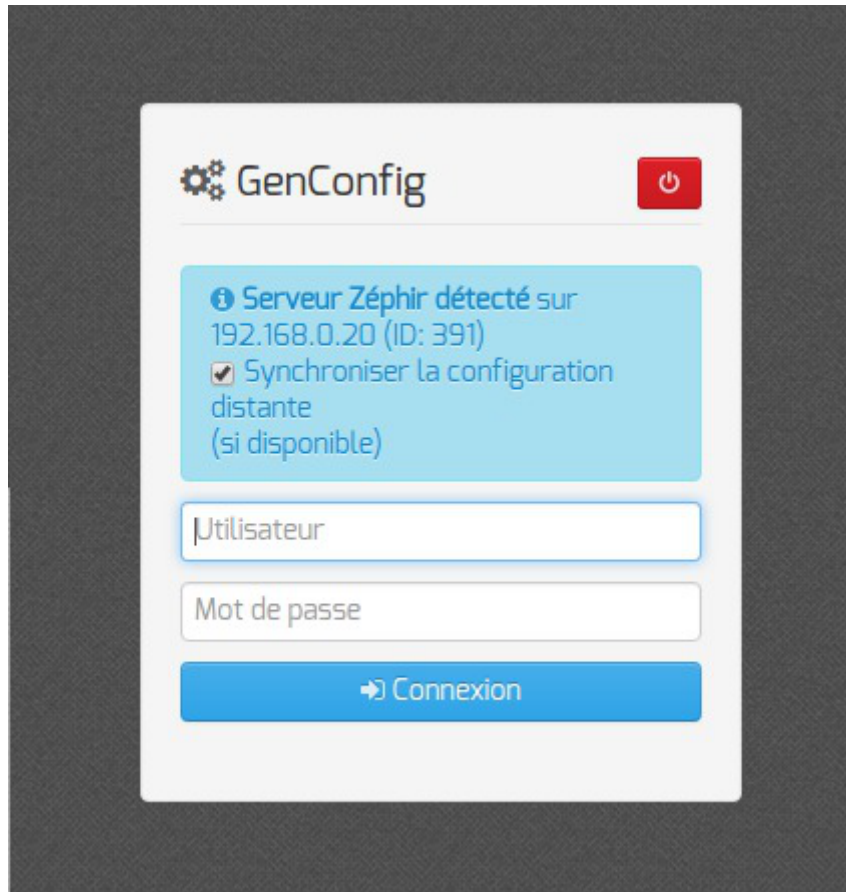
```

Le module est correctement enregistré sur le serveur Zéphir.

Lancement de l'interface de configuration

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

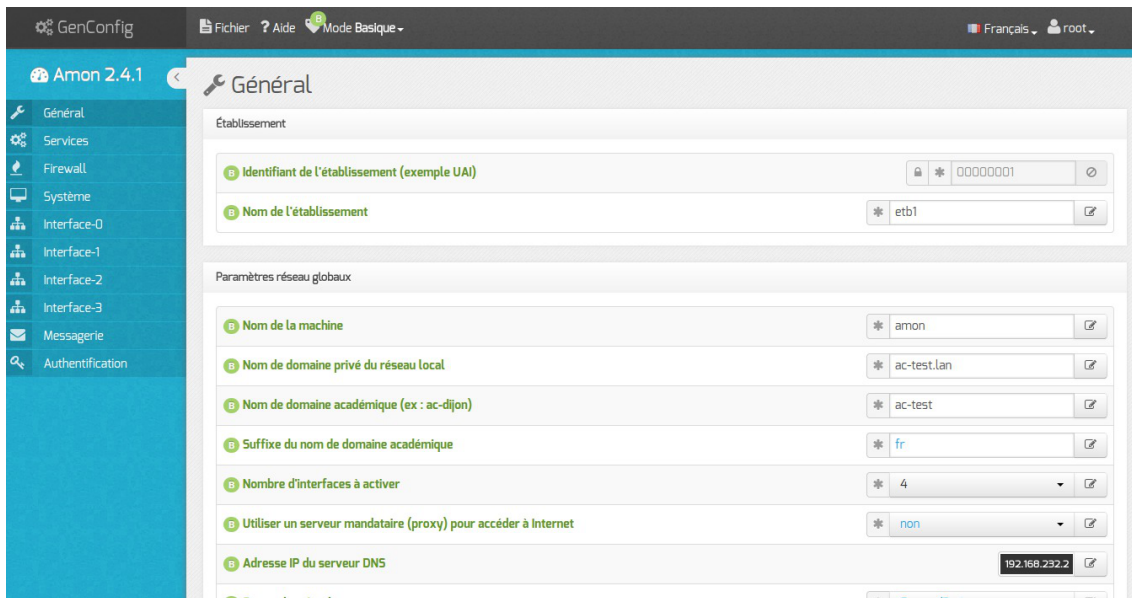
Lors de l'accès à l'interface d'administration d'un module enregistré sur un serveur Zéphir, la mire d'authentification permet d'ouvrir une session avec un compte utilisateur Zéphir ou un compte local.



2. Configuration en mode basique

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

- Général ;
- Firewall ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-1 (configuration de l'interface réseau) ;
- Messagerie ;
- Authentification .



Vue générale de l'interface de configuration du module

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

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

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

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

2.1. Onglet Général

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

Informations sur l'établissement



Deux informations sont importantes pour l'établissement :

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

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

Sur les modules fournissant un annuaire LDAP^[p.551] local, ces variables sont utilisées pour créer l'arborescence.



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

Paramètres réseau globaux

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

Cette information est découpée en plusieurs champs :

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

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



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

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

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

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



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



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

Nombre d'interfaces

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

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

The screenshot shows a configuration window with three main sections. The first section, 'Nombre d'interfaces à activer', has a dropdown menu open showing options 2, 3, 4, and 5. The second section, 'Utiliser un serveur mandataire (proxy) pour accéder à Internet', has a dropdown menu set to 'oui'. The third section, 'Adresse IP du serveur DNS', has a text input field.

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

Proxy

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

The screenshot shows the proxy configuration section. The first field, 'Utiliser un serveur mandataire (proxy) pour accéder à Internet', is a dropdown menu set to 'oui'. The second field, 'Nom ou adresse IP du serveur proxy', is an empty text input. The third field, 'Port du serveur proxy', is a text input set to '3128'.

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

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

DNS et fuseau horaire

The screenshot shows the DNS and time zone configuration section. The first field, 'Adresse IP du serveur DNS', is a text input containing three IP addresses: '192.168.232.2', '192.168.122.1', and '8.8.8.8'. The second field, 'Fuseau horaire du serveur', is a dropdown menu set to 'Europe/Paris'.

La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS^[p.545].

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

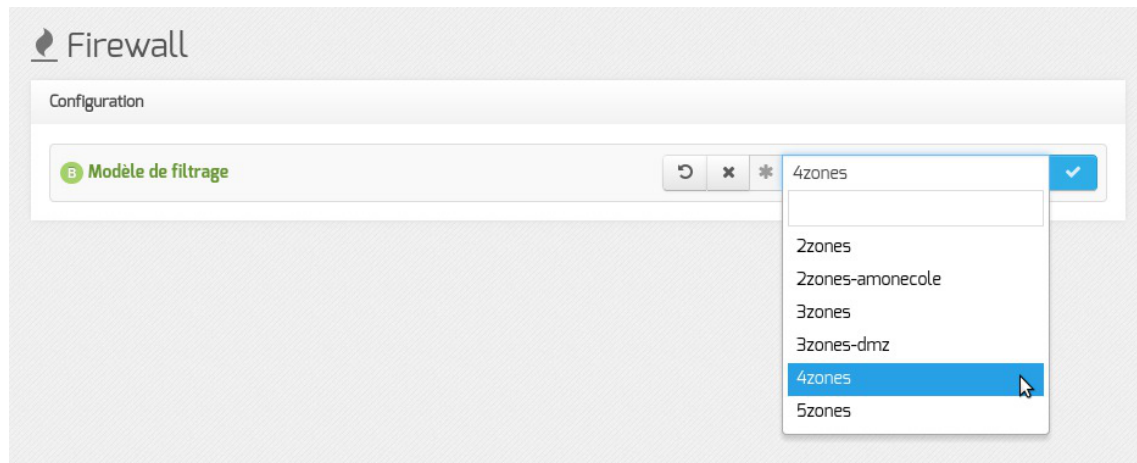
Voir aussi...

Onglet `Interface-n` ^[p.94]

2.2. Onglet Firewall

Modèle de filtrage

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



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

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

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



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



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

2.3. Onglet Interface-0

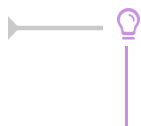
Configuration de l'interface

Configuration de l'interface

Méthode d'attribution de l'adressage pour l'interface	* statique
Adresse IP de la carte	* 192.168.122.20
Masque de sous réseau de la carte	* 255.255.255.0
Adresse IP de la passerelle par défaut	192.168.122.1

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP^[p.544] et PPPoE^[p.558].

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



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

Administration à distance

Administration distante sur l'interface

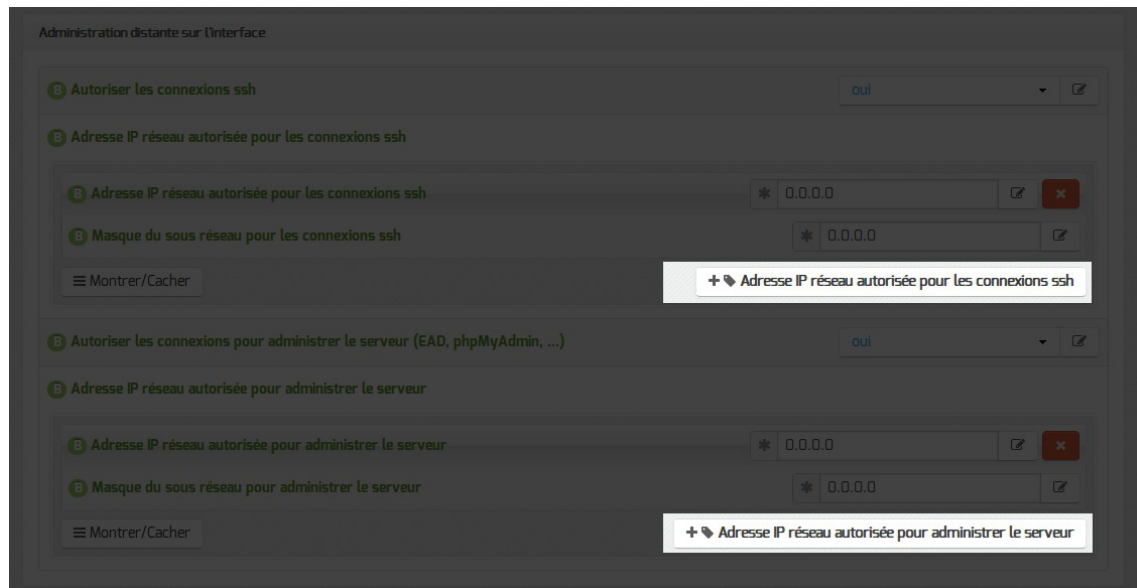
Autoriser les connexions SSH	* oui
Adresse IP réseau autorisée pour les connexions SSH	
Adresse IP réseau autorisée pour les connexions SSH	* 192.168.122.22
Masque du sous réseau pour les connexions SSH	* 255.255.255.255
Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH	
Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...)	* oui
Adresse IP réseau autorisée pour administrer le serveur	
Adresse IP réseau autorisée pour administrer le serveur	* 192.168.122.22
Masque du sous réseau pour administrer le serveur	* 255.255.255.255
Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur	

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



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

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



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



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

2.4. Onglet Interface-1

Nombre d'interfaces

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

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



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

Configuration de l'interface

Configuration de l'interface

B Adresse IP de l'interface *

B Masque de sous réseau de l'interface * 255.255.255.0

Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

Administration à distance

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

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

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

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur * 255.255.255.255

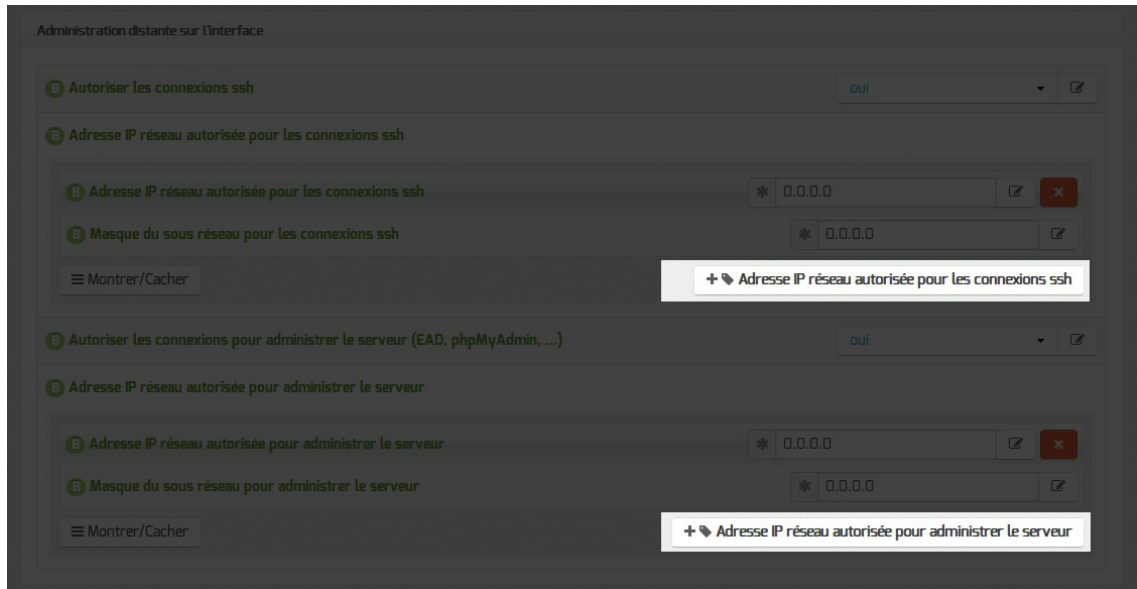
Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



Le masque réseau d'une station isolée est `255.255.255.255`.
 Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.



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



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

2.5. Onglet Interface-n

Nombre d'interfaces

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

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



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

Configuration de l'interface

Configuration de l'interface

B Adresse IP de l'interface *

B Masque de sous réseau de l'interface * 255.255.255.0

Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

Administration à distance

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

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

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

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur * 255.255.255.255

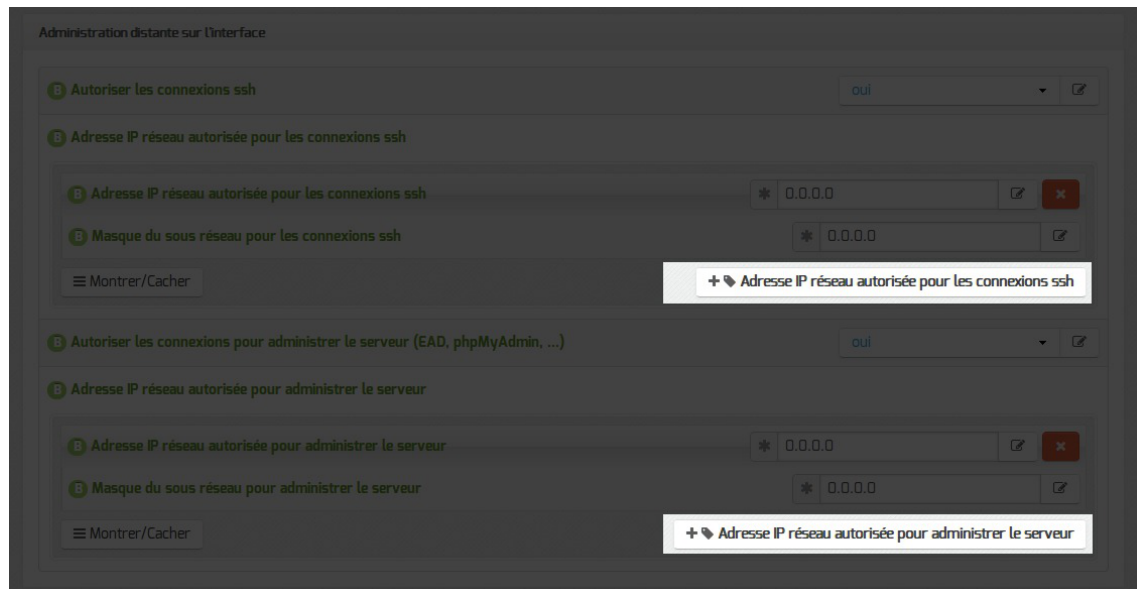
Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



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

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



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



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

2.6. Onglet Messagerie

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

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

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

Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

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



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

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

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

Relai des messages

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



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

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

2.7. Onglet Proxy authentifié : 5 méthodes d'authentification

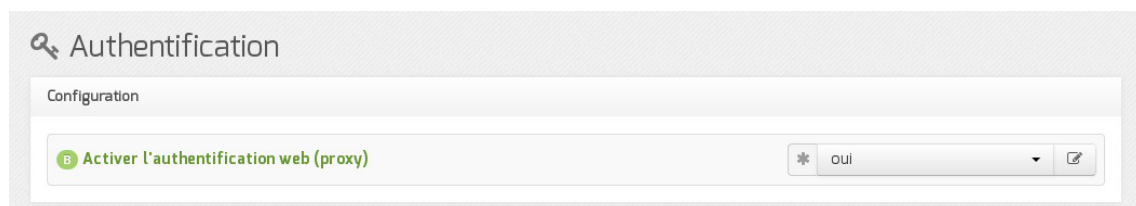
EOLE propose un mécanisme d'authentification web via un proxy.

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

Cette fonctionnalité offre deux avantages :

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

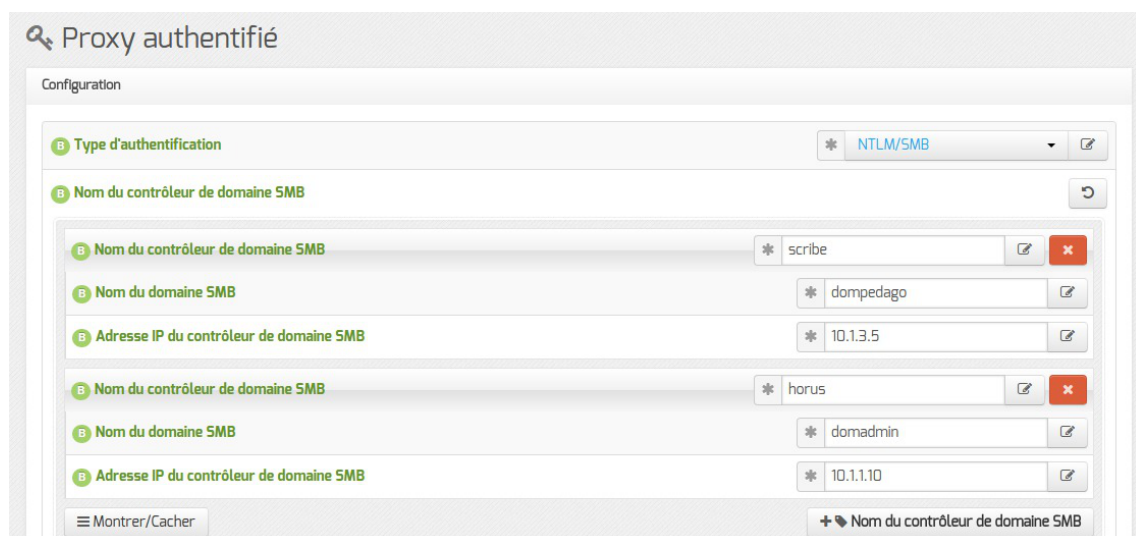
Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet **Authentification** : Activer l'authentification web (proxy).



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

Authentification NTLM/SMB

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



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

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

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



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

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
```

```
"LMCompatibilityLevel"=dword:00000001
```

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

Authentification NTLM/KERBEROS

The screenshot shows the configuration page for 'Proxy authentifié'. Under the 'Configuration' section, the following settings are visible:

- Type d'authentification: NTLM/KERBEROS
- Nom du contrôleur de domaine KERBEROS: srv2k3r2
- Nom du domaine KERBEROS (fqdn): domaine.lan
- Nom du domaine Windows: domaine
- Adresse IP du contrôleur de domaine KERBEROS: 10.1.2.73

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

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

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

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



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

Authentification LDAP

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

The screenshot shows the configuration page for 'Proxy authentifié'. Under the 'Configuration' section, the following settings are visible:

- Type d'authentification: Ldap
- Adresse du premier serveur LDAP: 10.1.1.10
- Suffixe racine de l'annuaire LDAP (base DN): o=gouv,c=fr

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

Authentification LDAP (Active Directory)

The screenshot shows the 'Proxy authentifié' configuration window. Under the 'Configuration' tab, the 'Type d'authentification' is set to 'Ldap (Active Directory)'. Other fields include: 'Adresse IP du serveur LDAP (Active Directory)' set to '10.1.2.73', 'Suffixe racine de l'annuaire LDAP (base DN Active Directory)' set to 'DC=domaine,DC=lan', 'Nom du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'Administrateur', and 'Mot de passe du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'P@sswOrd'. Each field has a search icon and a refresh icon.

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory. Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local

The screenshot shows the 'Proxy authentifié' configuration window. Under the 'Configuration' tab, the 'Type d'authentification' is set to 'Fichier local'. The rest of the configuration area is empty.

Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux. Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

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

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

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

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

```
# ssh proxy
```

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

ou

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

Désactivation de l'authentification sur une interface

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

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau eth2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette`

interface (s'applique aussi aux VLAN).

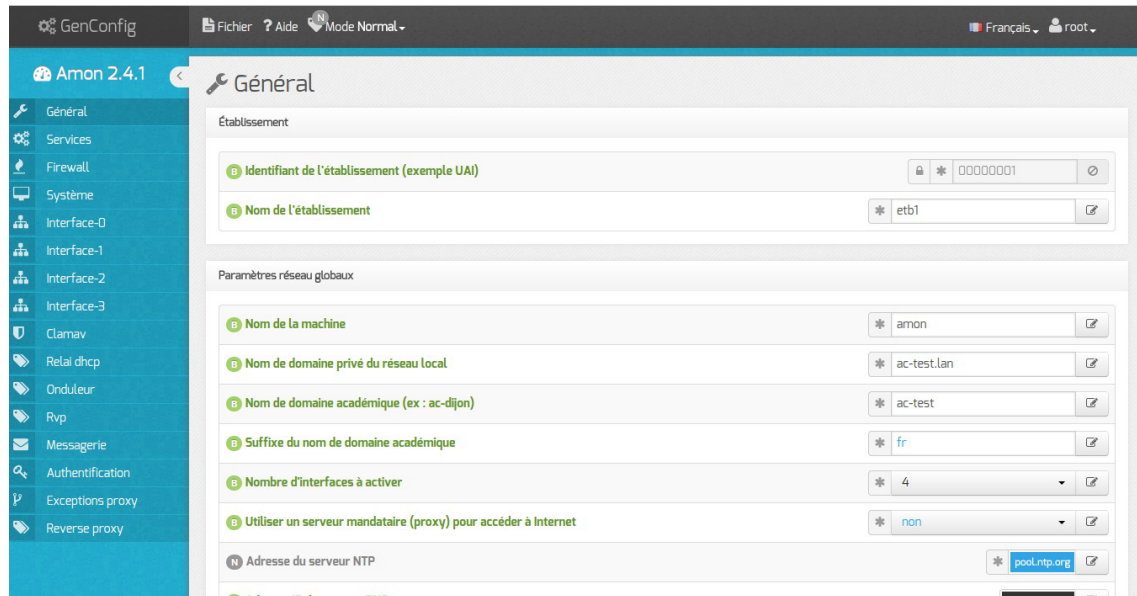
3. Configuration en mode normal

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

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

- Général ;
- Services ;
- Firewall ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-1 (configuration de l'interface réseau) ;
- Agregation ** ;
- Clamav * ;
- Relai dhcp * ;
- Onduleur * ;
- Rvp * ;
- Eole sso * ;
- Messagerie ;
- Authentification ;
- Proxy authentifié ;
- Proxy authentifié 2 ** ;
- Wpad ;
- Exceptions proxy ;
- Reverse proxy * ;
- Freeradius .

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



Vue générale de l'interface de configuration du module

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

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

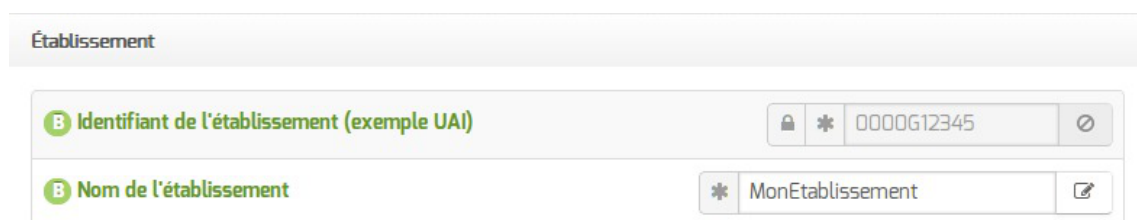
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

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

3.1. Onglet Général

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

Informations sur l'établissement

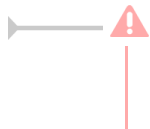


Deux informations sont importantes pour l'établissement :

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

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

Sur les modules fournissant un annuaire LDAP^[p.551] local, ces variables sont utilisées pour créer l'arborescence.



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

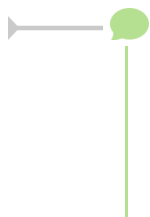
Paramètres réseau globaux

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

Cette information est découpée en plusieurs champs :

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

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

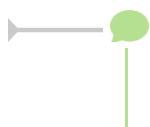


Les domaines de premier niveau .com, .fr sont en vigueur sur Internet, mais sont le résultat d'un choix arbitraire.

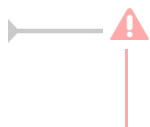
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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

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



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



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

Nombre d'interfaces

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

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

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

Proxy

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

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

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

DNS et fuseau horaire

La variable `Adresse IP du serveur DNS` donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS^[p.545].

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

NTP

Une valeur par défaut est attribuée pour le serveur de temps NTP^[p.556]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

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

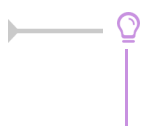
Voir aussi...

Onglet Interface-n [p.94]

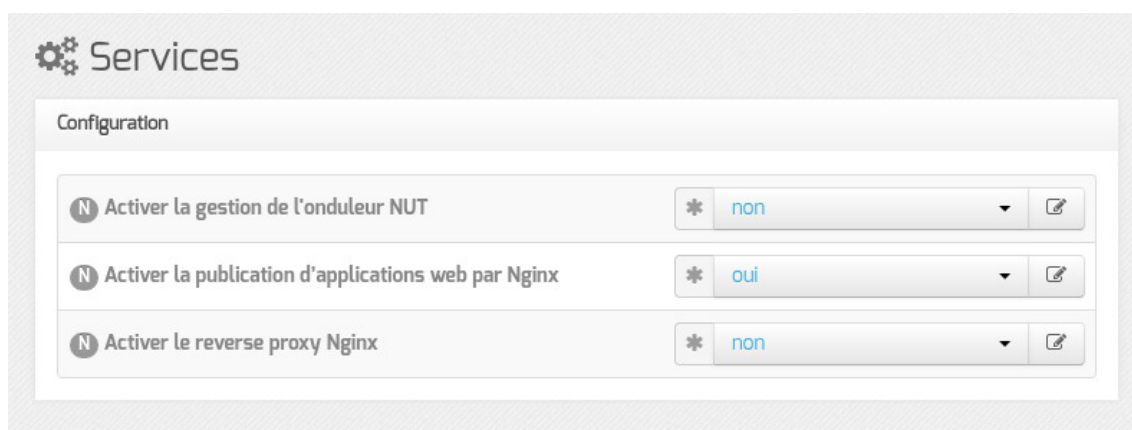
Les différents types de mises à jour [p.337]

3.2. Onglet Services

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



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



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT [p.556].

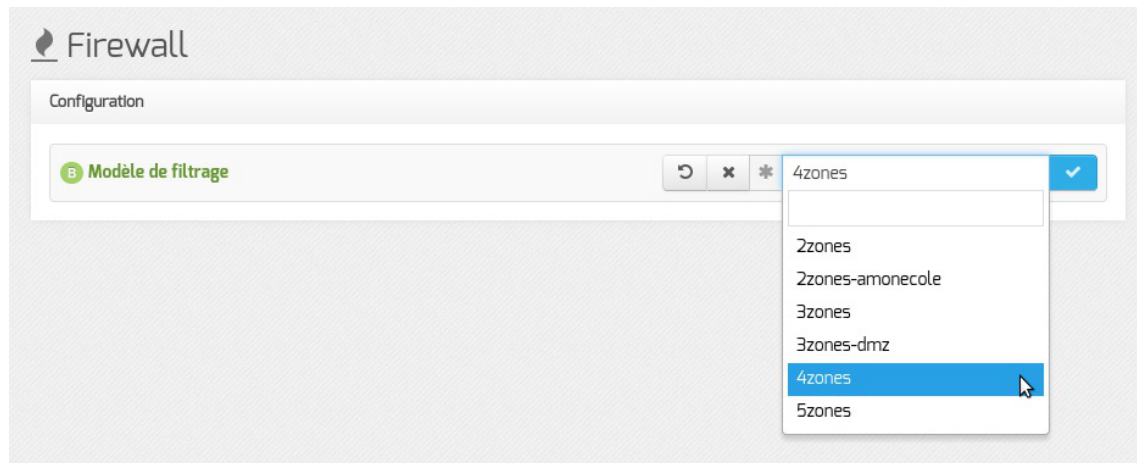
Les services de base propres au module Amon sont les suivants :

- l'anti-virus ClamAv ;
- le relai DHCP ;
- le réseau virtuel privé RVP ;
- le serveur EoleSSO ;
- le support WPAD ;
- le proxy inverse Nginx.

3.3. Onglet Firewall

Modèle de filtrage

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



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

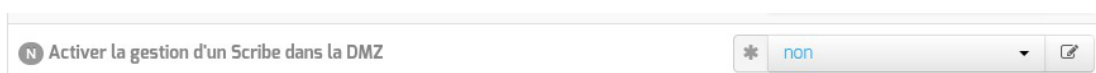
Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

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

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

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

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion^[p.542] des règles propres à la DMZ^[p.545].



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

- un réseau administratif ;
- un réseau pédagogique ;

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

La configuration recommandée sera :

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

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ

[p.256]

3.4. Onglet Interface-0

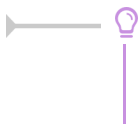
Configuration de l'interface

Configuration de l'interface

Méthode d'attribution de l'adressage pour l'interface	* statique
Adresse IP de la carte	* 192.168.122.20
Masque de sous réseau de la carte	* 255.255.255.0
Adresse IP de la passerelle par défaut	192.168.122.1

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP^[p.544] et PPPoE^[p.558].

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



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

Administration à distance

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

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

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

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur 255.255.255.255

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

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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

Administration distante sur l'interface

B Autoriser les connexions ssh oui

B Adresse IP réseau autorisée pour les connexions ssh

B Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

B Masque du sous réseau pour les connexions ssh * 0.0.0.0

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

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

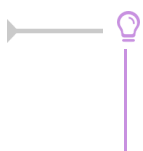
B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

B Masque du sous réseau pour administrer le serveur * 0.0.0.0

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

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



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

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

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



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



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

Configuration des alias sur l'interface

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

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

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

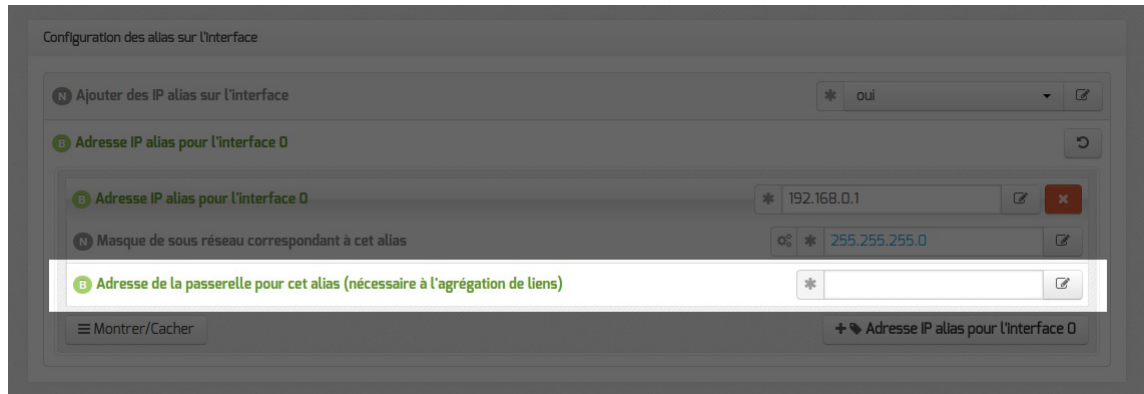
Agrégation de liens

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

Un nouvel onglet, `Agrégation`, est disponible.

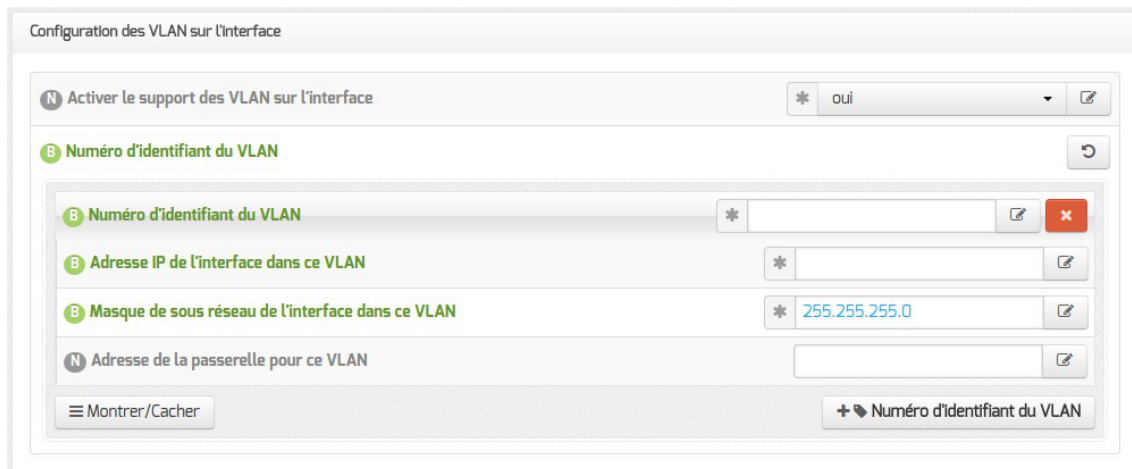


Si l'agrégation de liens est activée il faut obligatoirement configurer une passerelle particulière pour l'alias activé dans la rubrique Configuration des alias sur l'interface.



Configuration des VLAN sur l'interface

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



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

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

Voir aussi...

Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.119]

3.5. Onglet Interface-1

Nombre d'interfaces

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

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



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

Configuration de l'interface

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

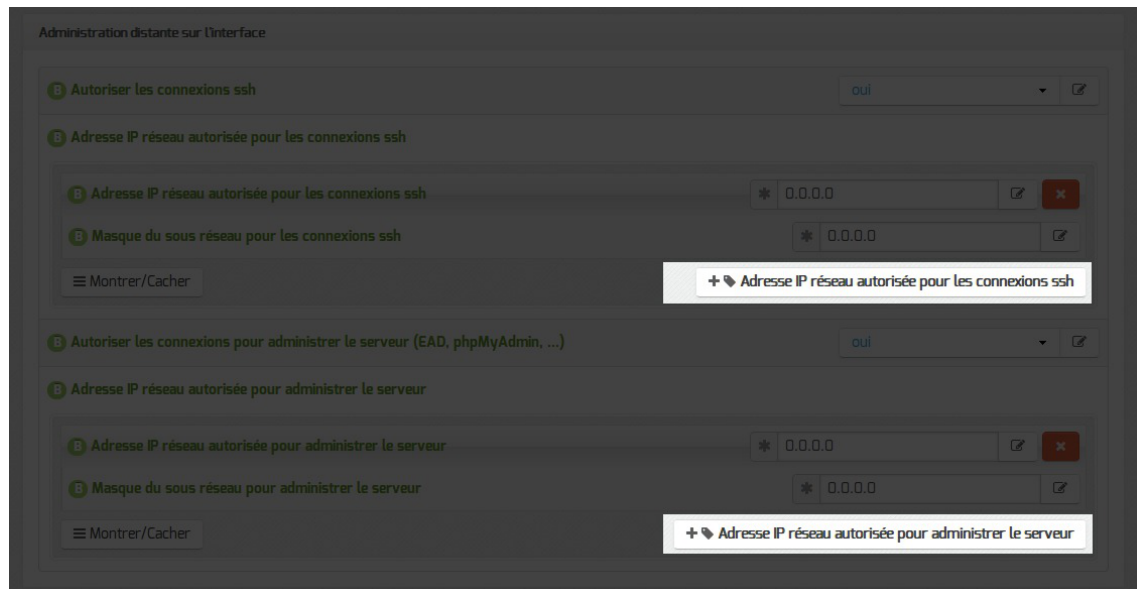
Administration à distance

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



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

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



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



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

Configuration des alias sur l'interface

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

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

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



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

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

Configuration des VLAN sur l'interface

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

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

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

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

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

Configuration DNS sur l'interface

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

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

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

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

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

Configuration de la politique de filtrage

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

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



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

Voir aussi...

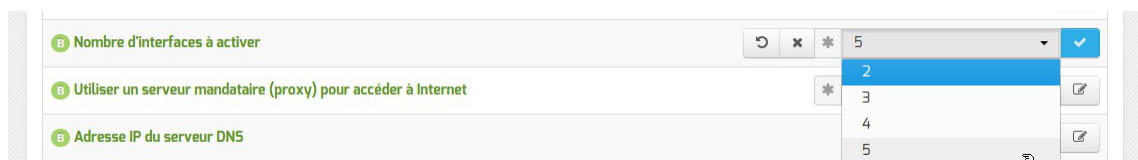
Onglet Filtrage web : Configuration du filtrage web [p.226]

3.6. Onglet Interface-n

Nombre d'interfaces

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

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



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

Configuration de l'interface



Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

Administration à distance

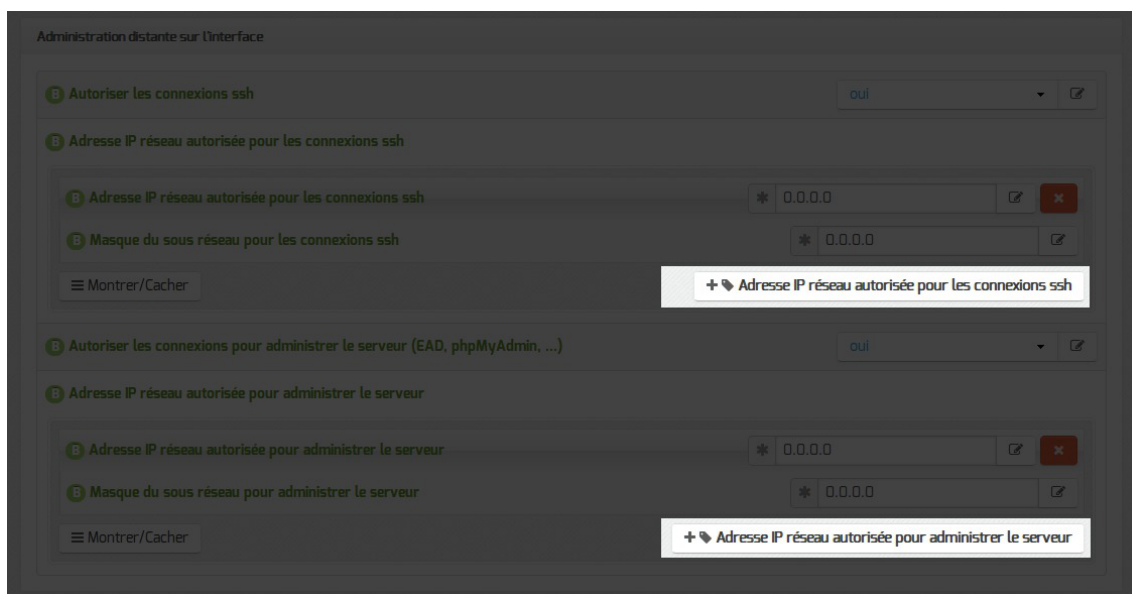


Configuration de l'administration à distance sur une interface

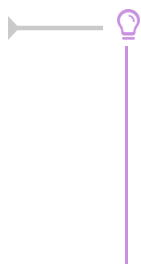
Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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

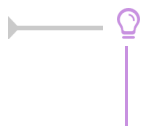


Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour...`

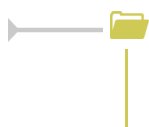


Le masque réseau d'une station isolée est `255.255.255.255`.

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



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



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

Configuration des alias sur l'interface

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

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

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



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

- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau

AGRIATES (onglet Rvp) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

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

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

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

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

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

Configuration DNS sur l'interface

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

- **Serveur master DNS de cette zone** : sert à activer le DNS sur l'interface.
- **Autoriser le réseau ethX à utiliser les DNS des zones forward additionnelles** : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section **Forward de zone DNS** de l'onglet **Zones-dns**.
- **Nom à donner à l'interface (pour résolution DNS)** : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

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

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

Configuration de la politique de filtrage

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

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

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

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.226]

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

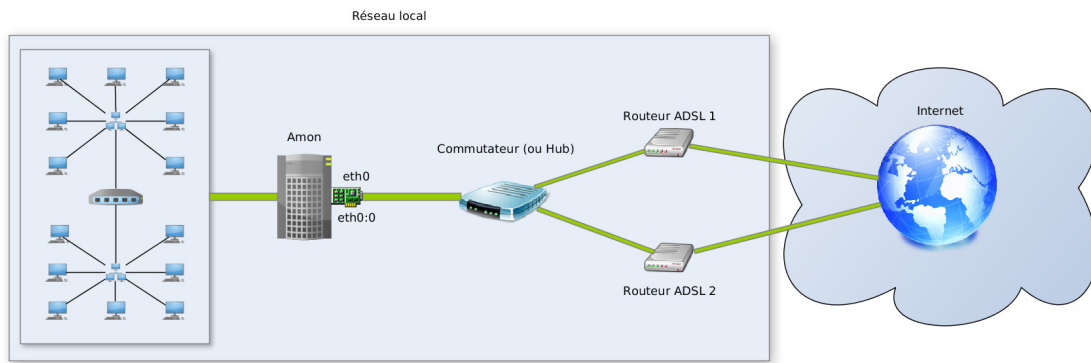
Présentation et mise en place de l'agrégation de liens

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

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

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP^[p.559] et OSPF^[p.556] ;
- il faut un service qui surveille l'état de chacun des liens.



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

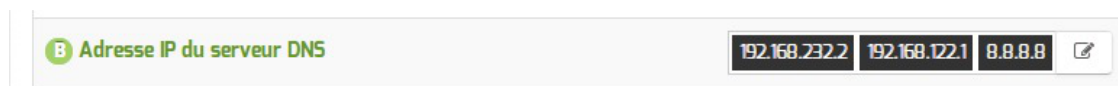


La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie.

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

Onglet Général

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



Onglet Interface-0

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

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

Configuration des alias sur l'interface

Ajouter des IP alias sur l'interface * oui

Adresse IP alias pour l'interface 0

Adresse IP alias pour l'interface 0 * 10.144.250.252

Masque de sous réseau correspondant à cet alias * 255.255.255.128

Adresse de la passerelle pour cet alias (nécessaire à l'agrégation de liens) * 10.144.250.254

Montrer/Cacher + Adresse IP alias pour l'interface 0

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

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

Agrégation de liens

Répartition de charge entre 2 lignes Internet * oui

Un nouvel onglet, **Agrégation**, est disponible.

Onglet Agrégation : Configuration de l'agrégation de liens

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

Agrégation

Mode d'agrégation

N Mode load balancing ou fail-over * mode_lb

Lien 1

N Destination forcée sur le lien 1

Montrer/Cacher + Destination forcée sur le lien 1

B Adresse du DNS sur le lien 1 * Pas de valeur

B Débit mesuré sur le lien 1 (entier en Mbps) *

Lien 2

N Destination forcée sur le lien 2

Montrer/Cacher + Destination forcée sur le lien 2

B Adresse du DNS sur le lien 2 * Pas de valeur

B Débit mesuré sur le lien 2 (entier en Mbps) *

Divers

N Délai entre les tests d'état (en secondes) * 10

N Timeout de la requête DNS (en secondes) * 1

N Adresse DNS testée * www.google.com

N Nombre de succès avant changement d'état * 4

N Nombre d'échecs avant changement d'état * 1

Alerte mail

N Activation des alertes mail * non

Paramétrage de l'agrégation de liens

Modes d'agrégation

Agrégation

Mode d'agrégation

N Mode load balancing ou fail-over * mode_lb

Il existe deux modes d'agrégation :

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

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

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



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

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

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

Adresse des DNS

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



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

Adresse DNS testée

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



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

Alerte mail

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

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

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

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

<http://www.clamav.net>

Activation de l'anti-virus

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

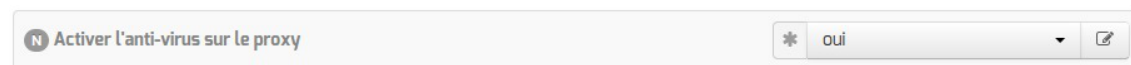
Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.



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

Activation de l'anti-virus sur le proxy

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



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

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU^[p.544]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

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



Contribuer

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

Il est possible de faire des signalements :

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

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



Il ne faut pas signaler des PUA^[p.559] comme étant des faux positifs.

3.9. Onglet Relai DHCP

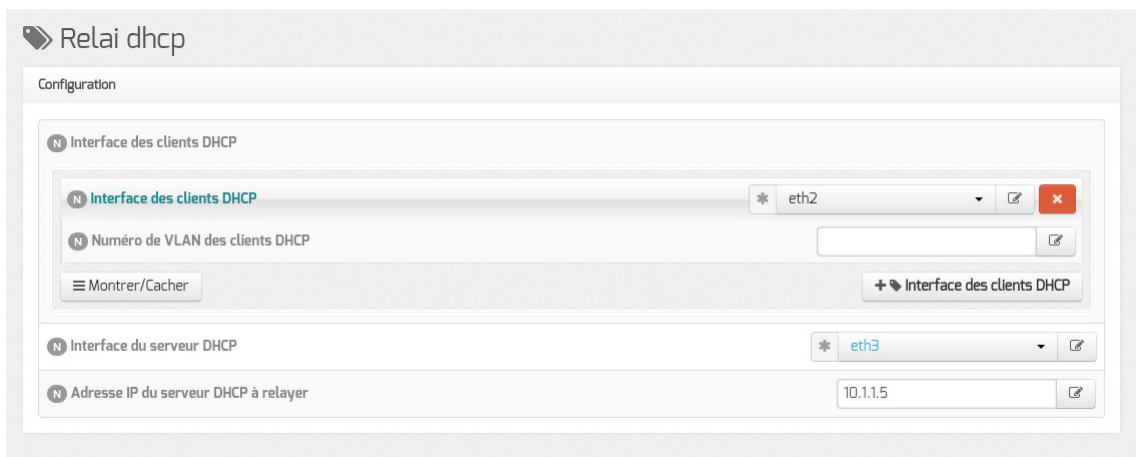
Pour des raisons de sécurité, le service DHCP^[p.544] n'a pas, à priori, à être installé sur le module Amon. Il vaut mieux utiliser un autre module (module Scribe ou module Horus par exemple) pour fournir ce service.

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast^[p.542].

De ce fait, les trames ne sont, par défaut, pas routables d'un réseau vers un autre.

Si le serveur DHCP ne se situe pas sur la même zone que les stations, il faut mettre en place un relai DHCP.

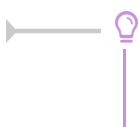
L'onglet `Relai dhcp` n'est accessible que si le service est activé dans l'onglet `Services`. Pour ce faire, passer la variable `Activer le relai DHCP` à `oui`.



Vue de l'onglet Relai dhcp de l'interface de configuration du module

Dans la configuration ci-dessus (4zones), on déclare que l'on veut relayer le DHCP du module Scribe (adresse IP : 10.1.1.5) qui se trouve dans la DMZ (eth3 est la 4ème interface) vers le réseau pédagogique (eth2 est la 3ème interface).

Il est possible de restreindre le relaiage sur un VLAN^[p.563] particulier en renseignant son numéro dans la variable `Numéro de VLAN des clients DHCP`.



Grâce au découpage des paquets par services, la mise en œuvre d'un DHCP sur le module Amon, bien que déconseillée, est facilitée par le paquet `eole-dhcp`.

Voir aussi...

`eole-dhcp` ^[p.415]

Configuration du module Amon avec le module Scribe en DMZ

[p.256]

3.10. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT^[p.556]. Il permet d'installer plusieurs clients sur le même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

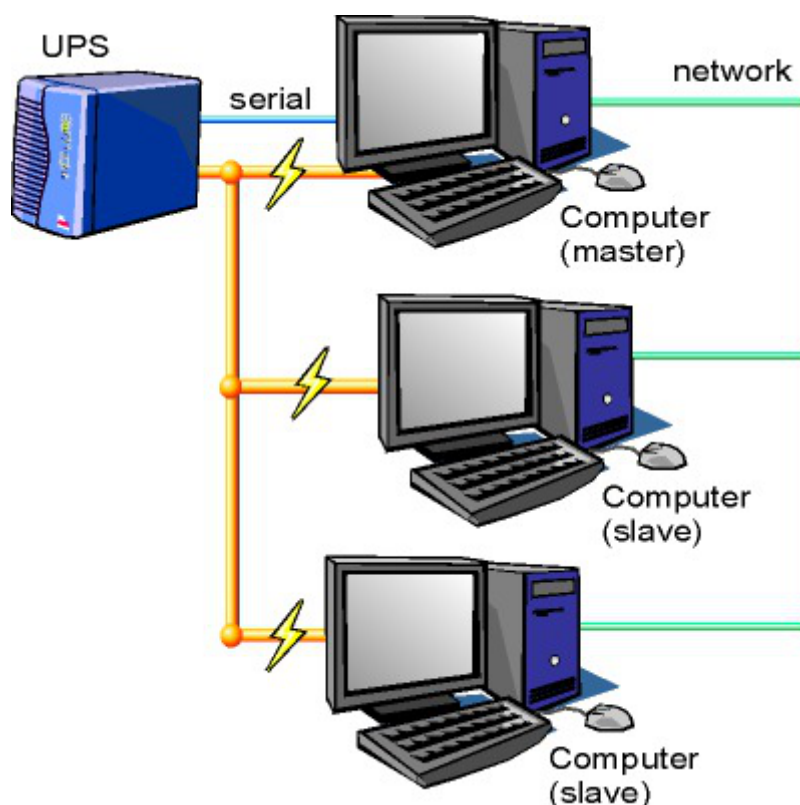


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - <http://ovanhoof.developpez.com/upsusb/>

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

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

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

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



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

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

ou encore :

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

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

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

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

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

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

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

La configuration sur un serveur maître

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

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

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



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

Configuration d'un second onduleur sur un serveur maître

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

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

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

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

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

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

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

Deux onduleurs de même marque

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

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

Deux onduleurs différents

Un onduleur sur port série :

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

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

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

Onduleur sur port USB :

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

La majorité des onduleurs USB sont détectés automatiquement.



Attention, seul le premier onduleur sera surveillé.

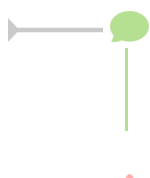
Autoriser des esclaves distants à se connecter

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

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

Pour chaque utilisateur, il faut saisir :

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



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



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



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

Configurer un serveur esclave

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

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

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

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

Exemple de configuration



Sur le serveur maître :

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

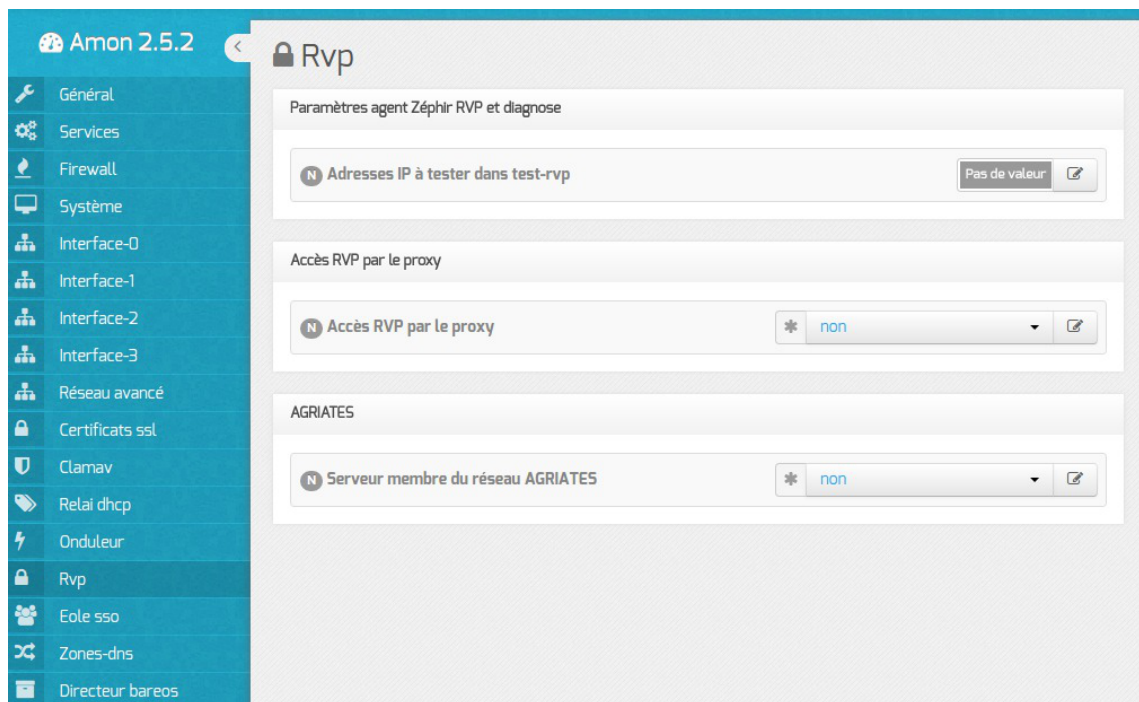
- Masque de l'IP du réseau de l'esclave : 255.255.255.255 .



Sur le serveur esclave :

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

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

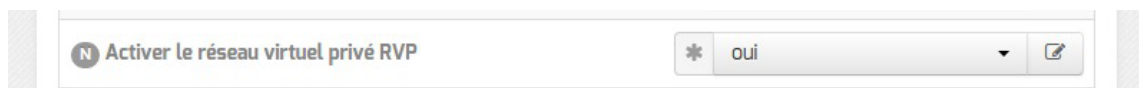


Onglet Rvp mode Normal

Le réseau virtuel privé^[p.559] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

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



Configuration des tunnels



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



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

Accès RVP par le proxy

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

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

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

Paramètres agent Zéphir RVP et diagnose

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

AGRIATES

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

- Adresse du DNS permettant de résoudre les in.ac-acad.fr permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;

- `Nom DNS de la zone résolue par le DNS AGRIATES` : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

Application de la configuration et gestion du RVP

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

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

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

Vous devez répondre `oui` à cette question.

Deux choix sont alors proposés :

1. `Manuel` permet de prendre en compte la configuration RVP présente sur une clé USB ;
2. `Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

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

Activation du RVP sur des modules Amon déjà en exploitation

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



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

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

Suppression du RVP

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

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

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

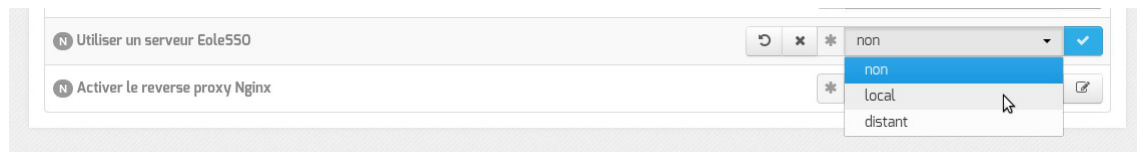
Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

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

d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

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



La variable Utiliser un serveur EoleSSO permet :

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

Adresse et port d'écoute

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

Eole sso
Configuration

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

Configuration d'un serveur EoleSSO local

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

Eole sso
Configuration

- Nom de domaine du serveur d'authentification SSO: etb1.ac-test.fr
- Port utilisé par le service EoleSSO: 8443
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200

Configuration d'un serveur EoleSSO distant

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

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

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

Configuration LDAP

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

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

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre `Gestion des sources d'authentifications multiples`) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire `/usr/share/sso/interface/info_homonymes` ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP^[p.557] si disponible (*voir plus loin*).



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

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

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

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

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

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

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

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

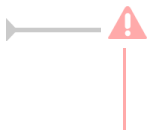
Passer la variable Information LDAP supplémentaires (applications) à oui permet de configurer pour chaque annuaire LDAP déclaré des attributs supplémentaires qui seront utilisés par les applications web (DN racine de l'arbre utilisateurs, DN racine de l'arbre groupes, Champ 'nom d'affichage' de l'utilisateur,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

Serveur SSO parent

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

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essaiera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC^[p.564] en HTTPS, sur le port défini pour le serveur EoleSSO).

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



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

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID^[p.560] de la société EMC (précédemment RSA).

Pour cela il faut :

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

Des champs supplémentaires apparaissent :

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

uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation^[p.550] du serveur et sont utilisés par défaut.

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

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autres types de serveurs compatibles avec le protocole SAML^[p.560] (version 2).

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

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

Autres options

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

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

Voir aussi...

Gestion des sources d'authentification multiples

3.13. Onglet Messagerie

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

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

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

Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

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



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

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

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

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



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

Toujours en mode normal d'autres paramètres sont modifiables.

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

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

Relai des messages

The screenshot shows a configuration window titled 'Relai des messages'. It contains two rows of settings:

- Row 1: A green circle with 'B' followed by the text 'Router les courriels par une passerelle SMTP'. To the right is a dropdown menu with 'oui' selected and an edit icon.
- Row 2: A green circle with 'B' followed by the text 'Passerelle SMTP'. To the right is a text input field containing 'smtp.ac-dijon.fr' and an edit icon.

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

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

The screenshot shows a configuration window with one row of settings:

- Row 1: A blue circle with 'N' followed by the text 'Utilisation du TLS (SSL) par la passerelle SMTP'. To the right is a dropdown menu with 'non' selected and an edit icon.

`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS^[p.563] pour l'envoi de message. Si la passerelle SMTP^[p.560] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS^[p.561] (port 25) ou non (port 465).

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

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

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

Cette fonctionnalité offre deux avantages :

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

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

The screenshot shows a configuration window titled 'Authentification'. It contains one row of settings:

- Row 1: A green circle with 'B' followed by the text 'Activer l'authentification web (proxy)'. To the right is a dropdown menu with 'oui' selected and an edit icon.

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

Activer une deuxième instance de Squid

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

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

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

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



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

Activer le service FreeRADIUS

EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS^[p.559].

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



Cela fera apparaître l'onglet **Freeradius**.

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

Voir aussi...

Onglet Proxy authentifié : 5 méthodes d'authentification [p.142]

Onglets Proxy authentifié 2 : Double authentification [p.147]

Onglet Freeradius : Configuration de l'authentification Radius [p.153]

3.15. Onglet Proxy authentifié : 5 méthodes d'authentification

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

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

Cette fonctionnalité offre deux avantages :

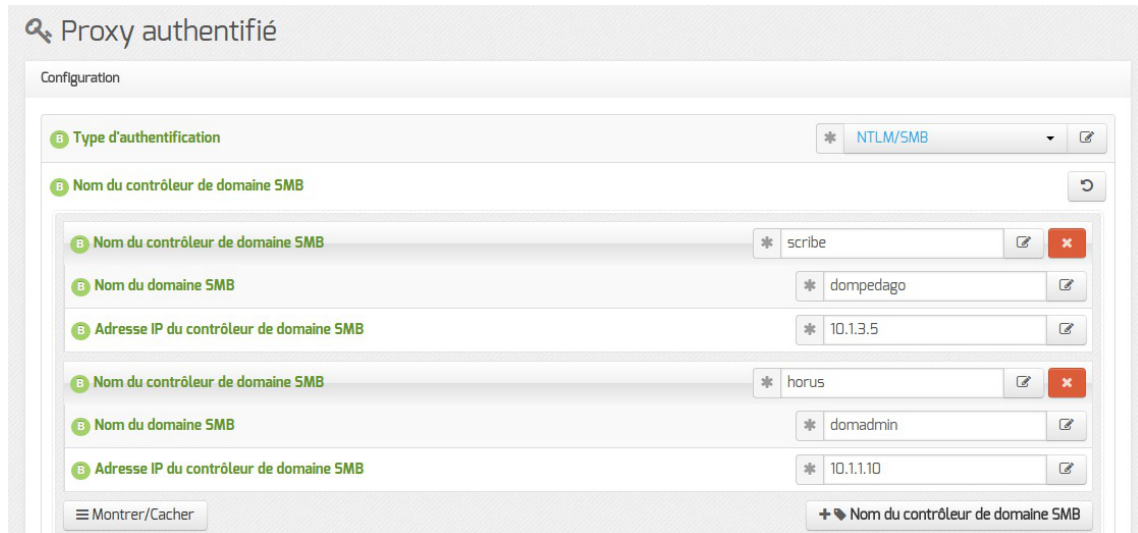
- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

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

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

Authentification NTLM/SMB

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



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

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

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

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

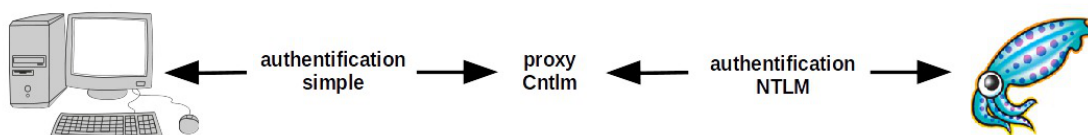
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"LMCompatibilityLevel"=dword:00000001
```

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

Authentification NTLM/SMB poste hors domaine

En mode normal, l'authentification NTLM^[p.555] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm^[p.543].

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



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

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

The image shows a configuration interface with a label 'Activer le proxy NTLM' and a dropdown menu. The dropdown menu is currently set to 'oui'.

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

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

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

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



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

Authentification NTLM/KERBEROS

The image shows a configuration page titled 'Proxy authentifié'. Under the 'Configuration' section, there are several fields:

- Type d'authentification: NTLM/KERBEROS
- Nom du contrôleur de domaine KERBEROS: srv2k3r2
- Nom du domaine KERBEROS (fqdn): domaine.lan
- Nom du domaine Windows: domaine
- Adresse IP du contrôleur de domaine KERBEROS: 10.1.2.73

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

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

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

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

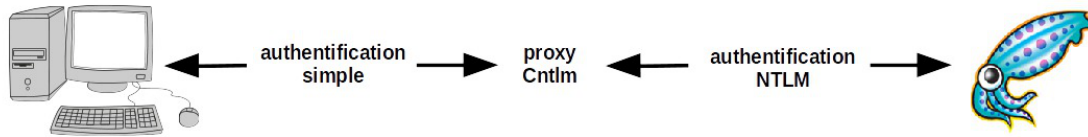


Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification NTLM/KERBEROS poste hors domaine

En mode normal, l'authentification NTLM^[p.555] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm^[p.543].

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



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

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

Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert. Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm. Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm. Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

Authentification LDAP

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

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

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

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

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

Authentification LDAP (Active Directory)

The screenshot shows the configuration page for 'Proxy authentifié'. Under the 'Configuration' section, the 'Type d'authentification' is set to 'Ldap (Active Directory)'. Other fields include: 'Adresse IP du serveur LDAP (Active Directory)' set to '10.1.2.73', 'Suffixe racine de l'annuaire LDAP (base DN Active Directory)' set to 'DC=domaine,DC=lan', 'Nom du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'Administrateur', and 'Mot de passe du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'P@ssw0rd'.

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory. Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local

The screenshot shows the configuration page for 'Proxy authentifié'. The 'Type d'authentification' is set to 'Fichier local'.

Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux. Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

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

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

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

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

```
# ssh proxy
```

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

ou

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

Désactivation de l'authentification sur une interface

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

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

3.16. Onglets Proxy authentifié 2 : Double authentification

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

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

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

Configuration pas à pas

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

Activer une deuxième instance de Squid * oui

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

Proxy authentifié 2

Configuration

Type d'authentification * Ldap

Adresse du premier serveur LDAP * 10.21.11.5

Adresse du second serveur LDAP (si le 1er ne répond pas)

Suffixe racine de l'annuaire LDAP (base DN) o=gouv,c=fr

Notes techniques

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

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

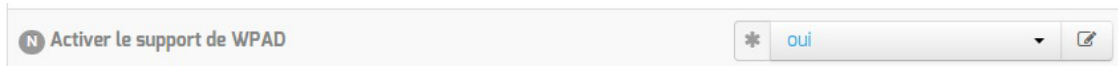
Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

3.17. Onglet Wpad : découverte automatique du proxy

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom_domaine_local>` corresponde à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet **Services** de l'interface de configuration du module **Activer le support de WPAD** doit être placé à **oui**.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet **Wpad** au sein duquel le **Nom de domaine du service WPAD** doit être rempli avec la même valeur que le **Nom de domaine privé du réseau local** présent dans l'onglet **Général**.

⚠ Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au **Nom de domaine privé du réseau local** de l'onglet **Général**, il faut le déclarer dans le champ **Nom domaine local supplémentaire ou rien** de l'onglet **Zones-dns**.

⚠ Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande **reconfigure** sur le module.

💡 WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.
En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Voir aussi...

➤ Configurer la découverte automatique du proxy avec WPAD ^[p.267]

3.18. Onglet Exceptions proxy

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

Il est possible de déclarer différents types d'exceptions.

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

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



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

Exception sur un nom de domaine

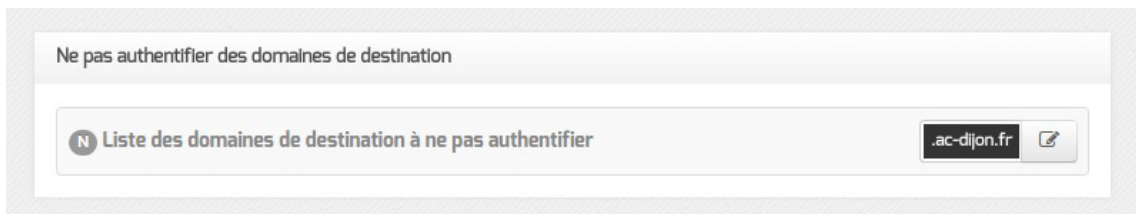
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour laquelle on ne passe pas par le proxy.



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

Exception au niveau de l'authentification des domaines

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



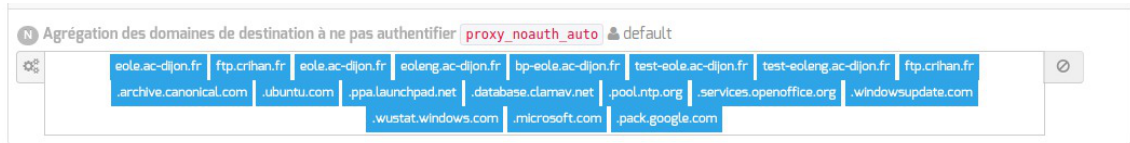
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

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

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

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

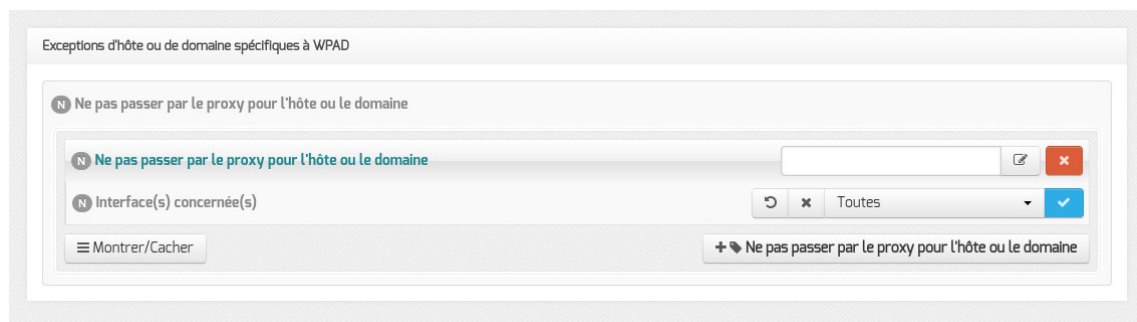
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



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

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

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



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

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

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

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

<http://findproxyforurl.com/netscape-documentation/#dnsDomains>

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

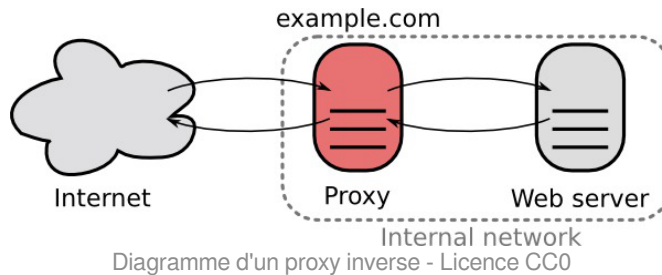
<http://findproxyforurl.com/netscape-documentation/#localHostOrDomains>

3.19. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx^[p.555].

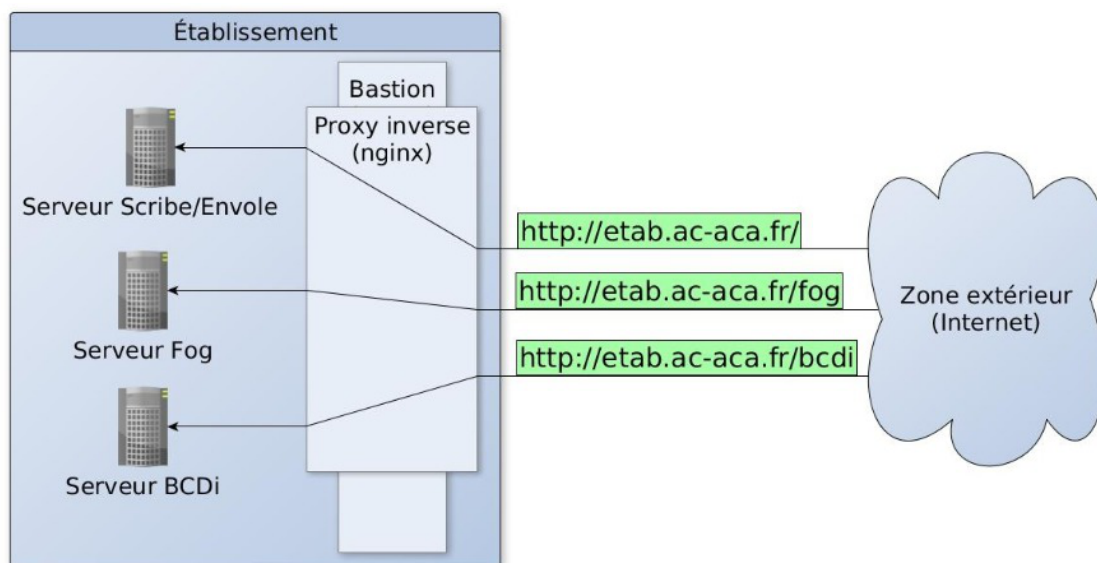
Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ^[p.545] par exemple). Cela le différencie grandement d'un proxy classique comme Squid^[p.561].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situés "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles iptables^[p.550]/DNAT.

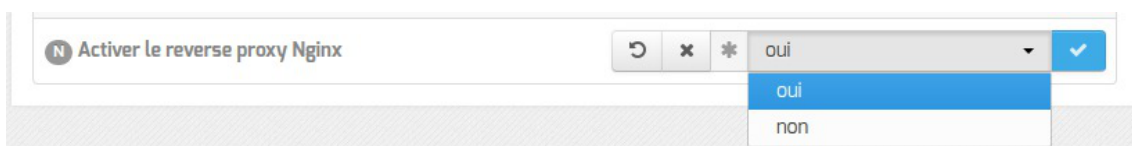


Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD^[p.545] ;
- application EOP ;
- protocole HTTP^[p.549] ;
- protocole HTTPS^[p.549].



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



L'activation du service fait apparaître un nouvel onglet.

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

Redirection de services particuliers

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



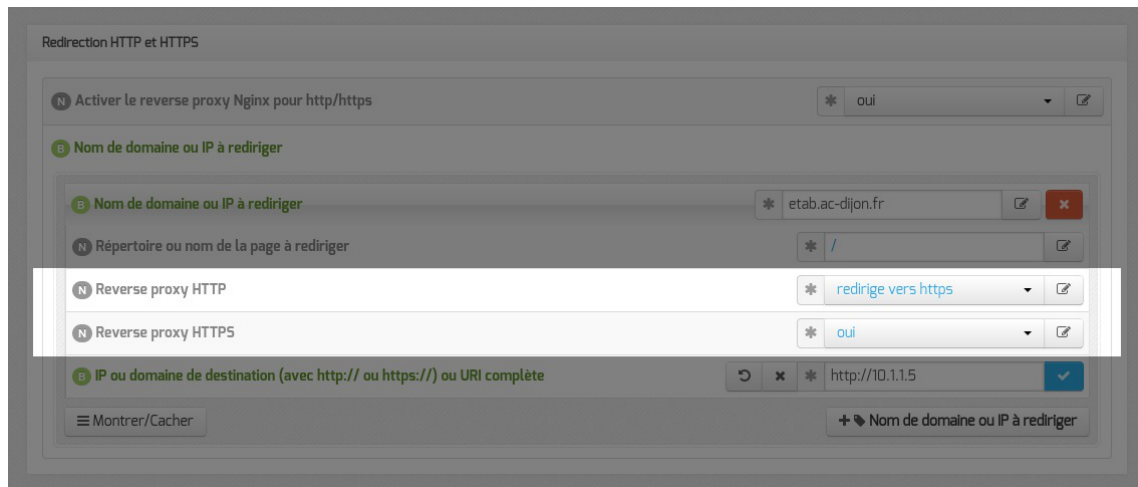
Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

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

- le Nom de domaine ou IP à rediriger : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- le Répertoire ou nom de la page à rediriger permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est / ;

- l'IP ou domaine de destination (avec http:// ou https://) ou URI complète permet de saisir l'adresse IP (exemple : http://192.168.10.1), le nom de domaine (exemple : http://scribe.monetab.fr) ou l'URI^[p.563] (exemple : http://scribe.monetab.fr/webmail/) du serveur de destination hébergeant la ou les applications.

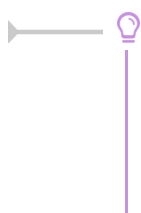


Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse http://monetab.fr sera automatiquement redirigé vers https://monetab.fr

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

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

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton Nom de domaine ou IP à rediriger.

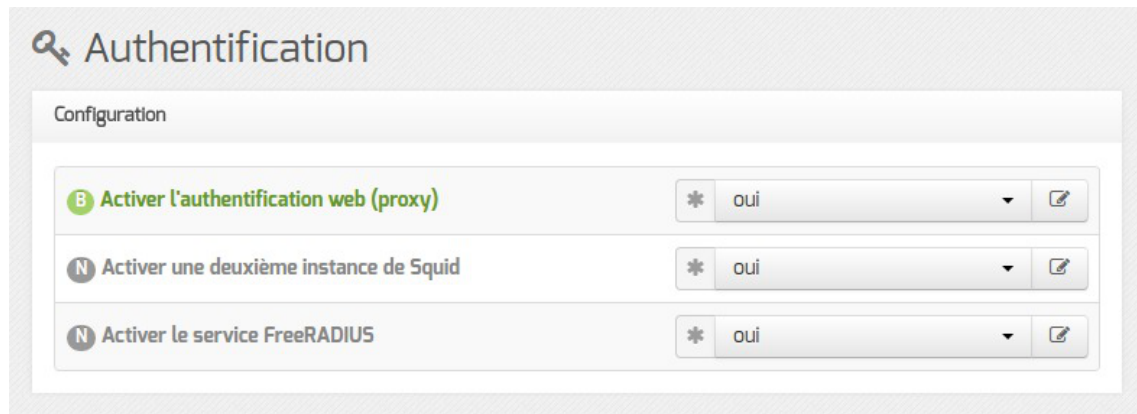


Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote^[p.558], https://monetab.fr/pronote/ peut être redirigé vers http://pronote.monetab.fr/ (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

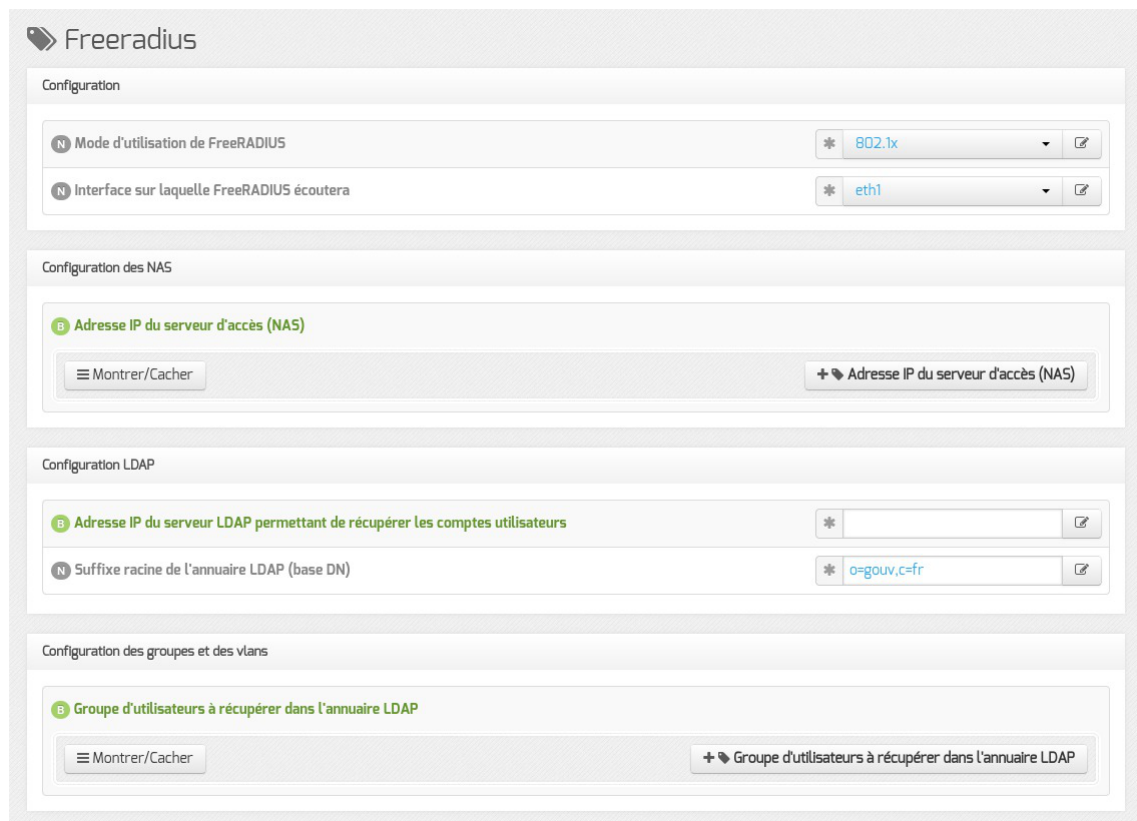
3.20. Onglet Freeradius : Configuration de l'authentification Radius

EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS^[p.559].

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



Cela fera apparaître l'onglet **Freeradius**.



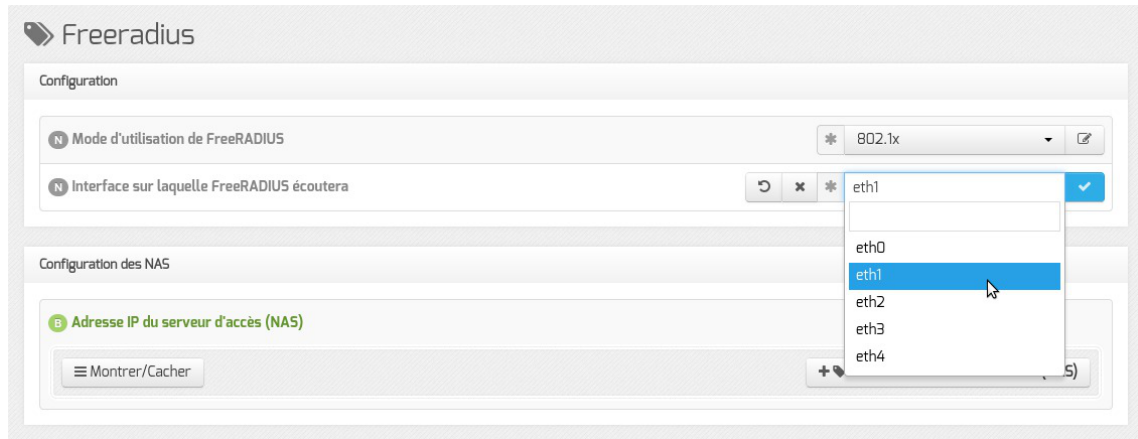
Vue de l'onglet Freeradius de l'interface de configuration du module

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

- 802.1x ;
- accounting.

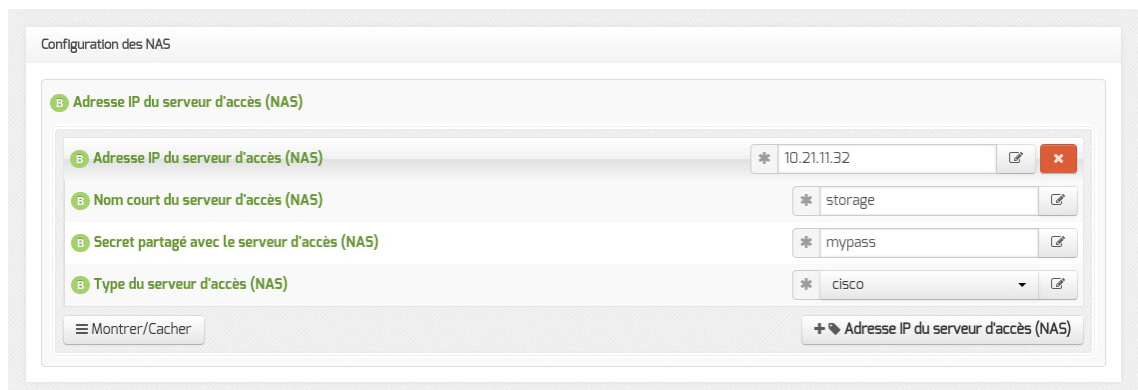
Le mode 802.1x

Le mode 802.1x permet de taguer dynamiquement des ports d'un switch (NAS^[p.554]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



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

Configuration des NAS



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

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

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

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

Configuration LDAP



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

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

Configuration des groupes et des VLAN

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

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

Le mode accounting

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

Onglet Freeradius - mode accounting

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

Configuration des NAS

Onglet Freeradius - mode accounting

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

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

CIDR^[p.543] si le réseau est de classe C.

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

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

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

Configuration LDAP

Onglet Freeradius - mode accounting

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

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

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

4. Configuration en mode expert

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

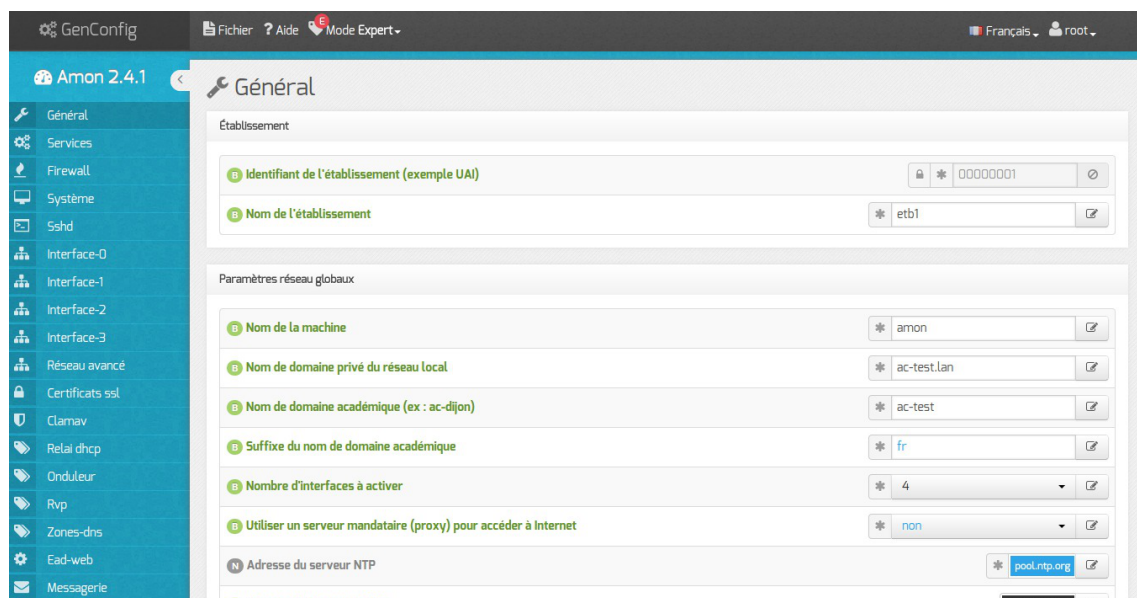
Dans l'interface de configuration du module voici les onglets propres à la configuration du module Amon :

- Général ;
- Services ;
- Firewall ;
- Système ;
- Sshd ;
- Logs * ;
- Interface-0 (configuration de l'interface réseau) ;
- Interface-1 (configuration de l'interface réseau) ;
- Réseau avancé ;
- Certificat ssl ;
- Agregatation ** ;
- Clamav * ;
- Relai dhcp * ;

- Onduleur * ;
- Eole sso * ;
- Rvp * ;
- Zone-dns ;
- Ead-web ;
- Messagerie ;
- Authentification ;
- Filtrage web ;
- Squid ;
- Squid2 **;
- Proxy authentifié ;
- Proxy authentifié 2 **;
- Wpad ;
- Exceptions proxy ;
- Proxy parent ;
- Reverse proxy * ;
- Freeradius **;
- Eoleflask .

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

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



Vue générale de l'interface de configuration du module

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

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

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

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

4.1. Onglet Général

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

Informations sur l'établissement

The screenshot shows a configuration window titled 'Établissement'. It contains two input fields:

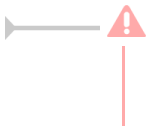
- Identifiant de l'établissement (exemple UAI)**: A text input field containing '0000G12345'. It has a lock icon on the left and a refresh icon on the right.
- Nom de l'établissement**: A text input field containing 'MonEtablissement'. It has a lock icon on the left and an edit icon on the right.

Deux informations sont importantes pour l'établissement :

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

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

Sur les modules fournissant un annuaire LDAP^[p.551] local, ces variables sont utilisées pour créer l'arborescence.



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

Paramètres réseau globaux

The screenshot shows a configuration window titled 'Paramètres réseau globaux'. It contains two input fields:

- Nom de domaine académique (ex : ac-dijon)**: A text input field containing 'ac-test'. It has a lock icon on the left and an edit icon on the right.
- Suffixe du nom de domaine académique**: A text input field containing 'fr'. It has a lock icon on the left and an edit icon on the right.

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

Cette information est découpée en plusieurs champs :

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

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

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

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

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

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

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

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

Nombre d'interfaces

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

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



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

Proxy

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



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

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

DNS et fuseau horaire

La variable Adresse IP du serveur DNS donne la possibilité de saisir une ou plusieurs adresses IP du ou des serveur(s) de noms DNS^[p.545].

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

NTP

Une valeur par défaut est attribuée pour le serveur de temps NTP^[p.556]. Il est possible de changer cette valeur pour utiliser un serveur de temps personnalisé.

Mise à jour

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

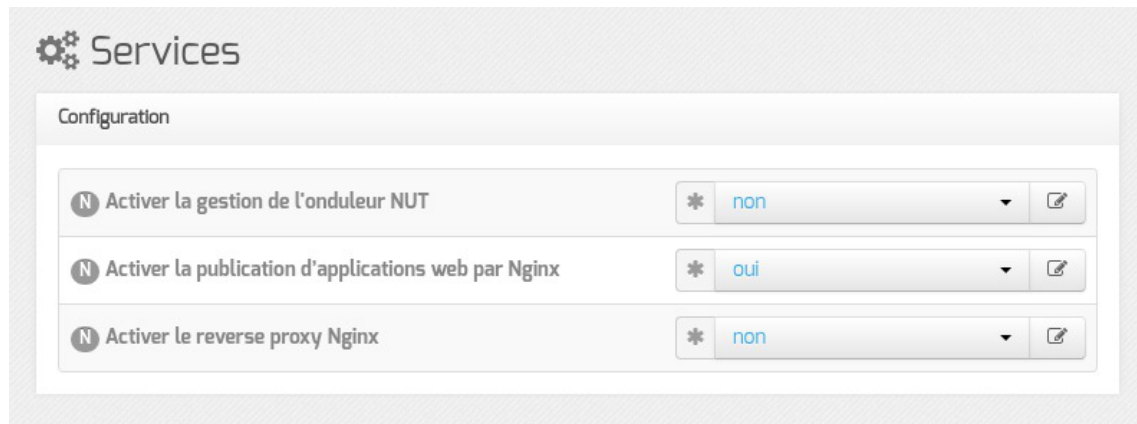
Il est possible de définir d'autres adresses pour le serveur de mise à jour Ubuntu que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.

Le champ Adresse web de mise à jour des blacklists permet de personnaliser l'adresse à utiliser pour le téléchargement des bases de filtres (blacklists^[p.551]).

Voir aussi...

- ▶ Onglet Interface-n ^[p.94]
- ▶ Les différents types de mises à jour ^[p.337]
- ▶ Bases de filtres optionnels ^[p.368]

4.2. Onglet Services



Vue de l'onglet Services en mode normal

Le service de base commun à tous les modules est la gestion de l'onduleur NUT^[p.556].

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

- l'anti-virus ClamAv ;
- le relai DHCP ;
- le réseau virtuel privé RVP ;
- le serveur EoleSSO ;
- le support WPAD ;
- le proxy inverse Nginx.

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

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

En mode expert le seul service propre au module Amon est le filtrage sur le proxy qui est activé par défaut.

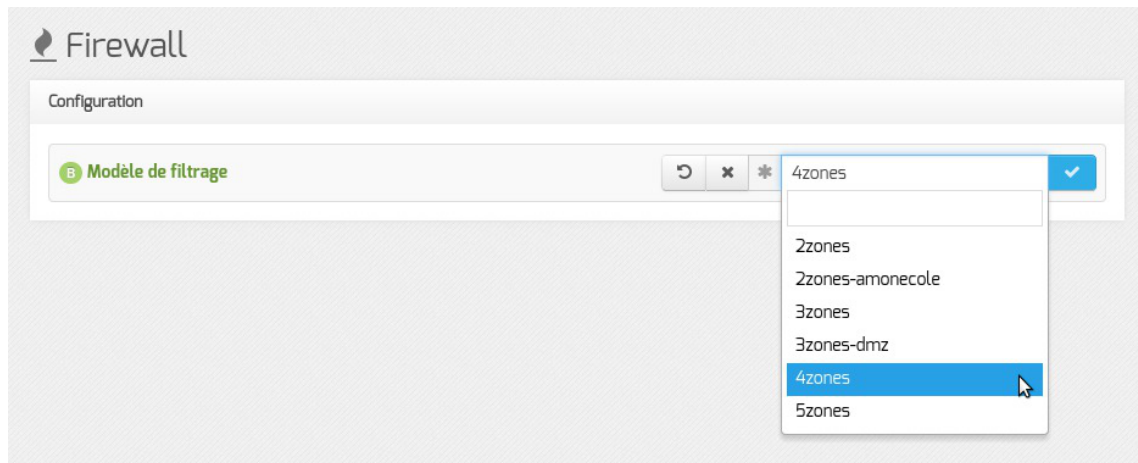
Voir aussi...

Onglet Logs : Gestion des logs centralisés ^[p.167]

4.3. Onglet Firewall

Modèle de filtrage

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



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

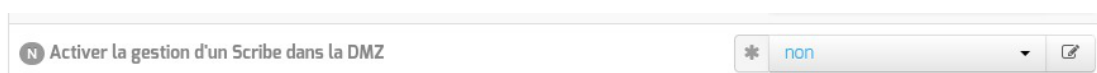
Les modèles de zone par défaut proposés supportent jusqu'à 5 cartes réseau :

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

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

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

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion^[p.542] des règles propres à la DMZ^[p.545].



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

- un réseau administratif ;
- un réseau pédagogique ;

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

La configuration recommandée sera :

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

Voir aussi...

Configuration du module Amon avec le module Scribe en DMZ

[p.256]

4.4. Onglet Système

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

Paramétrage de la console

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

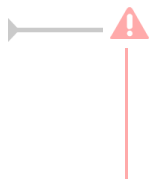
- Activer le reboot sur ctrl-alt-suppr : si cette variable est passée à non, la séquence ctrl - alt - suppr est désactivée et affiche le message suivant Control-Alt-Delete - séquence désactivée.

Optimisations système

Optimisations système

Poids relatif de l'utilisation de la swap par rapport à la mémoire vive	* 0	[✎]
Activer le service de génération de nombres aléatoires rng-tools	* non	[✎]

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



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

erreur Starting Hardware RNG entropy gatherer daemon: (failed)

Validation des mots de passe

Validation des mots de passe des utilisateurs système (root, eole, ...)

Vérifier la complexité des mots de passe	* oui	[✎]
Taille minimum du mot de passe utilisant une seule classe de caractères	* 0	[✎]
Taille minimum du mot de passe utilisant deux classes de caractères	* 9	[✎]
Taille minimum du mot de passe utilisant trois classes de caractères	* 8	[✎]
Taille minimum du mot de passe utilisant quatre classes de caractères	* 8	[✎]
Taille maximale du mot de passe	* 40	[✎]

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

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

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

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

- Taille minimum du mot de passe utilisant une seule classe de caractères ;

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

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



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

Voir aussi...

Les mots de passe [p.273]

4.5. Onglet Sshd : Gestion SSH avancée

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

Ils permettent :

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



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

`Permission denied (publickey).`

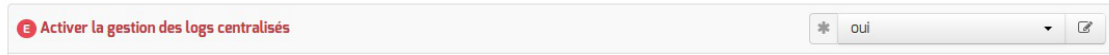


Par défaut les groupes Unix autorisés sont `root` et `adm`.

4.6. Onglet Logs : Gestion des logs centralisés

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog^[p.565]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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



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

 A screenshot of the 'Logs' configuration tab. The tab is titled 'Logs' with a pencil icon. It is divided into three main sections:

- Réception**: Contains four rows of settings. Each row has a checkbox (all checked), a label, and a dropdown menu.
 - Activer la réception des logs de machines distantes: dropdown set to 'oui'.
 - Activer la réception des logs de machines distantes via le protocole RELP (fiable, non compatible TLS): dropdown set to 'non'.
 - Activer la réception des logs de machines distantes via le protocole UDP: dropdown set to 'non'.
 - Activer la réception des logs de machines distantes via le protocole TCP (compatible TLS): dropdown set to 'non'.
- Envoi**: Contains three rows of settings.
 - Activer l'envoi des logs à une machine distante (TCP si TLS activé, RELP sinon): dropdown set to 'oui'.
 - Adresse IP du serveur de log central: a text input field with a blue gear icon and a document icon.
 - Activer le chiffrement des transferts pour l'envoi (TLS): dropdown set to 'non'.
- Choix des journaux à envoyer**: Contains two rows of settings.
 - Envoyer tous les journaux: dropdown set to 'oui'.
 - Utiliser une plage temporelle pour le transfert des logs: dropdown set to 'non'.

Vue de l'onglet Logs

Les options de cet onglet sont réparties en plusieurs sections :

- la configuration de la réception des logs permet de spécifier les protocoles de communication entre des machines distantes émettrices identifiées par leur adresse IP et le poste configuré ;
- la configuration de l'envoi des logs permet de spécifier l'adresse de la machine distante réceptrice. Le protocole (TCP^[p.562] ou RELP^[p.559]) utilisé est contraint par l'activation ou non du chiffrement (TLS^[p.563]) ;
- la configuration des journaux à envoyer permet de sélectionner les journaux à envoyer ainsi que l'heure de début et de fin de transfert.

Réception des journaux

Si la réception des journaux est activée (**Activer la réception des logs de machines distantes** à **oui**), il faut activer au moins l'un des 3 protocoles de réception : RELP, UDP et TLS over TCP.

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

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

⚠ Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI^[p.541].

Envoi des journaux

L'activation de l'envoi des journaux (Activer l'envoi des logs à une machine distante à oui) nécessite la saisie de l'adresse IP du serveur centralisateur de journaux.

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

⚠ Lors du choix des protocoles d'envoi et de réception des journaux, pensez à suivre les préconisations de l'ANSSI^[p.541].

Choix des journaux à envoyer

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

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

4.7. Onglet Interface-0

Configuration de l'interface

The screenshot shows the 'Configuration de l'interface' window with the following settings:

- Méthode d'attribution de l'adressage pour l'interface:** statique
- Adresse IP de la carte:** 192.168.122.20
- Masque de sous réseau de la carte:** 255.255.255.0
- Adresse IP de la passerelle par défaut:** 192.168.122.1

Avant toute chose, il faut savoir comment la carte réseau est configurée. Pour cela, il existe trois possibilités : statique, DHCP [p.544] et PPPoE [p.558].

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



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

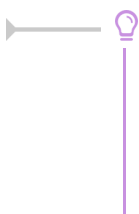
En mode expert quelques variables supplémentaires sont disponibles.

The screenshot shows the 'Configuration de l'interface' window with the following advanced settings:

- Nom de l'interface réseau:** eth0
- Nom de l'interface réseau de la zone:** eth0
- L'interface réseau de la zone est un bridge:** non
- Mode de connexion pour l'interface:** (dropdown menu)

Nom de l'interface réseau

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



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

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

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

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



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

Mode de connexion pour l'interface

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

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

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

Liste des valeurs possible :

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



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

Administration à distance

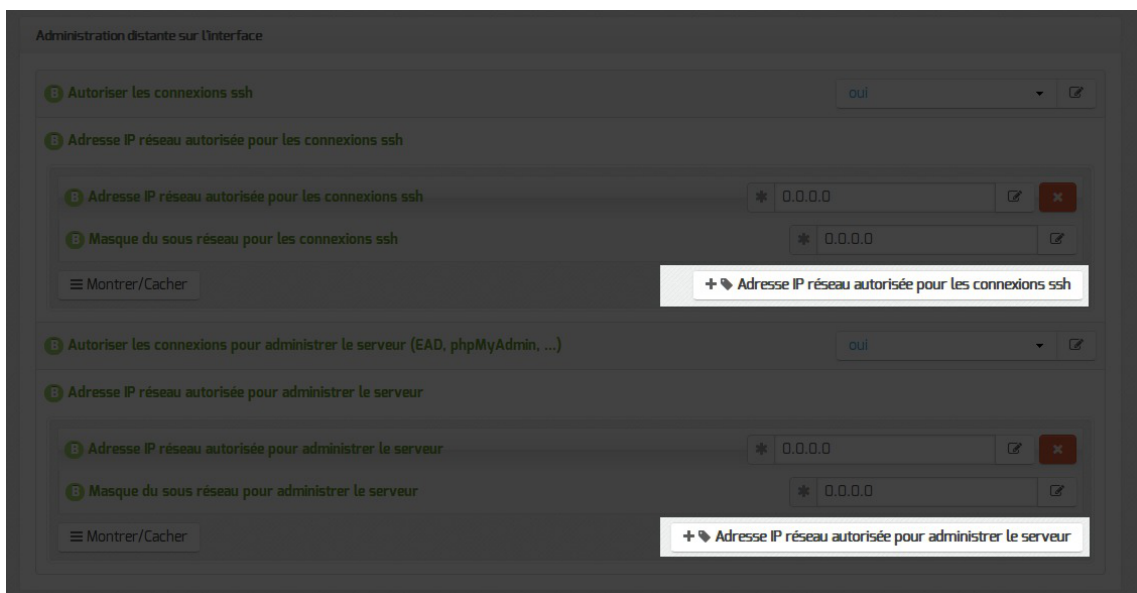


Configuration de l'administration à distance sur une interface

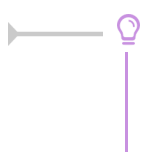
Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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



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



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

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

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



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



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

Configuration des alias sur l'interface

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

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

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

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

Configuration des VLAN sur l'interface

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

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

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

Configuration DNS sur l'interface-0

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

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

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



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

Voir aussi...

▶ Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.119]

4.8. Onglet Interface-1

Nombre d'interfaces

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

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



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

Configuration de l'interface



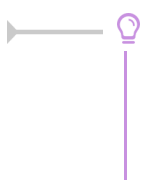
Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

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



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

Un rechargement du module réseau ou plus simplement un redémarrage du système est

| nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

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

L'interface réseau de la zone est un bridge

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



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

Mode de connexion pour l'interface

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

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

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

Liste des valeurs possible :

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



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

Administration à distance

Administration distante sur l'interface

Autoriser les connexions SSH * oui

Adresse IP réseau autorisée pour les connexions SSH

Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

Masque du sous réseau pour les connexions SSH * 255.255.255.255

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

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

Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

Masque du sous réseau pour administrer le serveur * 255.255.255.255

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

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

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

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

Administration distante sur l'interface

Autoriser les connexions ssh oui

Adresse IP réseau autorisée pour les connexions ssh

Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

Masque du sous réseau pour les connexions ssh * 0.0.0.0

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

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

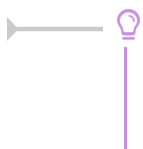
Adresse IP réseau autorisée pour administrer le serveur

Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

Masque du sous réseau pour administrer le serveur * 0.0.0.0

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

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



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

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

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



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



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

Configuration des alias sur l'interface

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

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

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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration des VLAN sur l'interface

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

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

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

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un VLAN donné.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration DNS sur l'interface

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

- Serveur master DNS de cette zone : sert à activer le DNS sur l'interface.
- Autoriser le réseau ethX à utiliser les DNS des zones forward additionnelles : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.
- Nom à donner à l'interface (pour résolution DNS) : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

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

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

Configuration de la politique de filtrage

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

La différenciation se fait en modifiant la valeur choisie pour Filtre Web à appliquer à cette interface dans la configuration de chaque interface (onglets : Interface-1 , Interface-2 , ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet Filtrage web.

Configuration de la détection automatique du proxy

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour l'interface.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Si le proxy NTLM est activé, la variable Activer le proxy NTLM sur cette interface permet de le désactiver pour cette interface de façon spécifique.



Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.226]

4.9. Onglet Interface-n

Nombre d'interfaces

Un module Amon peut avoir de 2 à 5 cartes réseau.

Le nombre d'interfaces activées se définit dans l'onglet **Général** de l'interface de configuration du module.



Cela ajoute autant d'onglets **Interface-n** que le nombre d'interfaces à activer choisi.

Configuration de l'interface



Dans les modes basique et normal, un adressage statique est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

Le nom de l'interface est proposé dans l'interface de configuration du module est de la forme `eth0` mais celui-ci ne correspond pas toujours à la réalité du système. Il peut donc être adapté prendre la forme utilisé par le système, par exemple `em0`.



Le changement de nom d'une interface réseau dans le système se fait en éditant le fichier

`/etc/udev/rules.d/70-persistent-net.rules`.

Un rechargement du module réseau ou plus simplement un redémarrage du système est nécessaire pour la prise en charge du changement.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface réseau de la zone.

L'interface réseau de la zone est un bridge

S'il existe un pont sur l'interface il est possible d'appliquer la configuration sur celui-ci en passant `L'interface réseau de la zone est un bridge` à `oui`. Il faut également saisir le nom du pont dans le champ `Nom de l'interface réseau de la zone`.



L'option ne crée pas le pont sur l'interface.

Mode de connexion pour l'interface

Le paramètre nommé `Mode de connexion pour l'interface` pour l'interface-0 et nommé `Mode de connexion pour l'interface interne-x` pour les autres interfaces permet de forcer les propriétés de la carte réseau.

Par défaut, toutes les interfaces sont en mode `auto négociation`.

Ces paramètres ne devraient être modifiés que s'il y a un problème de négociation entre un élément actif et une des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

Liste des valeurs possible :

- `speed 100 duplex full autoneg off` : permet de forcer la vitesse à 100Mbps/s en full duplex sans chercher à négocier avec l'élément actif en face ;
- `autoneg on` : active l'auto-négociation (mode par défaut) ;
- `speed 10 duplex half autoneg off` : permet de forcer la vitesse à 10Mbps/s en half duplex et désactiver l'auto-négociation ;
- `speed 1000 duplex full autoneg off` : permet de forcer la vitesse à 1Gbits/s en full duplex et désactiver l'auto-négociation.



Plus d'informations : [http://fr.wikipedia.org/wiki/Auto-négociation_\(ethernet\)](http://fr.wikipedia.org/wiki/Auto-négociation_(ethernet)).

Administration à distance

Administration distante sur l'interface

B Autoriser les connexions SSH * oui

B Adresse IP réseau autorisée pour les connexions SSH

B Adresse IP réseau autorisée pour les connexions SSH * 192.168.122.22

B Masque du sous réseau pour les connexions SSH * 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions SSH

B Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) * oui

B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 192.168.122.22

B Masque du sous réseau pour administrer le serveur 255.255.255.255

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Configuration de l'administration à distance sur une interface

Par défaut les accès SSH^[p.561] et aux différentes interfaces d'administration (EAD, phpMyAdmin, CUPS, ARV... selon le module) sont bloqués.

Pour chaque interface réseau activée (onglets `Interface-n`), il est possible d'autoriser des adresses IP ou des adresses réseau à se connecter.

Les adresses autorisées à se connecter via SSH sont indépendantes de celles configurées pour accéder aux interfaces d'administration.

Administration distante sur l'interface

B Autoriser les connexions ssh oui

B Adresse IP réseau autorisée pour les connexions ssh

B Adresse IP réseau autorisée pour les connexions ssh * 0.0.0.0

B Masque du sous réseau pour les connexions ssh * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour les connexions ssh

B Autoriser les connexions pour administrer le serveur (EAD, phpMyAdmin, ...) oui

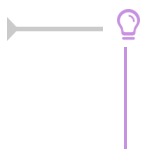
B Adresse IP réseau autorisée pour administrer le serveur

B Adresse IP réseau autorisée pour administrer le serveur * 0.0.0.0

B Masque du sous réseau pour administrer le serveur * 0.0.0.0

Montrer/Cacher + Adresse IP réseau autorisée pour administrer le serveur

Il est possible d'autoriser plusieurs adresses en cliquant sur `Adresse IP réseau autorisée pour...`



Le masque réseau d'une station isolée est `255.255.255.255`.

Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs

Adresse IP réseau autorisée pour les connexions SSH et Masque du sous réseau pour les connexions SSH autorise les connexions SSH depuis n'importe quelle adresse IP.



La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -nni $(CreoleGet nom_carte_eth0) port 22`



Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Sshd` en mode expert.

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.

Pour cela, il faut activer son support (Ajouter des IP alias sur l'interface à oui) et configurer l'adresse IP et le masque de sous réseau.

Il est possible de configurer une passerelle particulière pour cet alias, ce paramètre est obligatoire si l'agrégation de liens est activée.

Autoriser cet alias à utiliser les DNS de zones forward additionnelles permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.

Pour cela, il faut activer son support (Activer le support des VLAN sur l'interface à oui et ajout d'un numéro identifiant du VLAN avec le bouton + Numéro d'identifiant du VLAN) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un VLAN donné.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.

- Serveur master DNS de cette zone : sert à activer le DNS sur l'interface.
- Autoriser le réseau ethX à utiliser les DNS des zones forward additionnelles : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.
- Nom à donner à l'interface (pour résolution DNS) : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

Si le support du RVP est activé une option supplémentaire est disponible :

- Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES : Si le service RVP est activé (onglet Services) et que le serveur est membre du réseau AGRIATES (onglet Rvp) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

Configuration de la politique de filtrage

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour Filtre Web à appliquer à cette interface dans la configuration de chaque interface (onglets : Interface-1, Interface-2, ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage. La configuration de chacun des filtres se fait dans l'onglet Filtrage web.

Configuration de la détection automatique du proxy

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour l'interface.

Par défaut, le port du proxy est défini à 3128 mais si le proxy NTLM est activé sur cette interface, il passe à 3127.

Si le proxy NTLM est activé, la variable Activer le proxy NTLM sur cette interface permet de le désactiver pour cette interface de façon spécifique.

⚠ Activer le proxy NTLM sur cette interface

⚙️ oui

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.226]

Onglet Proxy authentifié : 5 méthodes d'authentification [p.142]

4.10. Onglet Réseau avancé

Présentation des différents paramètres de l'onglet Réseau avancé accessible en mode expert.

Configuration IP



Réseau avancé

Configuration

- ⚠ Restreindre le ping aux réseaux autorisés pour administrer le serveur * oui
- ⚠ Activer le support IPv6 * non
- ⚠ Activer le routage IPv4 entre les interfaces * oui



Même si la fonctionnalité Restreindre le ping aux réseaux autorisés pour administrer le serveur apparaît dans l'onglet Réseau avancé du présent module, elle n'a aucun effet.

C'est dans les modèles ERA que sont décrites les restrictions liées au protocole ICMP^[p.549].



À partir de la version 2.5.2, cette variable n'apparaît plus sur le présent module.

La variable Activer le support IPv6 est par défaut à non et est utilisée pour désactiver explicitement le support de l'IPv6 dans la configuration de certains logiciels (BIND, Proftpd).

Le support de l'IPv6^[p.550] peut être activé en passant la variable Activer le support IPv6 à oui mais sa prise en charge ne se sera faite qu'au niveau du noyau.

Si la variable Activer le routage IPv4 entre les interfaces est à oui, alors le routage IPv4 est activé au niveau du noyau (`/proc/sys/net/ipv4/ip_forward` passe à 1)

L'activation du support IPv6 entraîne l'apparition de la variable : Activer le routage IPv6 entre les interfaces.

Si cette dernière est à oui le routage IPv6 est activé au niveau du noyau (`/proc/sys/net/ipv6/conf/all/forwarding` passe à 1).

Sécurité

Sécurité

Journaliser les "martian sources" * non

Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets utilisant des adresses IP réservées à un usage particulier (<http://tools.ietf.org/html/rfc5735>) seront enregistrés dans les journaux.

Activer l'anti-spoofing sur toutes les interfaces * non

Par défaut, l'anti-spoofing^[p.541] est activé sur l'interface-0 des modules EOLE.

Sur les serveurs ayant 2 interfaces réseau ou plus d'activées (cas par défaut pour Amon et Sphynx), il est possible de demander l'activation de l'anti-spoofing sur les autres interfaces en passant la variable `Activer l'anti-spoofing sur toutes les interfaces` à `oui`.

Ajout d'hôtes

Ajout d'hôtes

Déclarer des noms d'hôtes supplémentaires * oui

Adresse IP de l'hôte

Adresse IP de l'hôte * [input] [✓] [✗]

Nom long de l'hôte * [input] [✎]

Nom court de l'hôte [input] [✎]

Montrer/Cacher

+ Adresse IP de l'hôte

Passer la variable `Déclarer des noms d'hôtes supplémentaires` à `oui`, permet de déclarer des noms d'hôtes qui seront ajoutés au fichier `/etc/hosts`.

Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte`.

Le champ `Nom court de l'hôte` est optionnel.



Sur les serveurs EOLE faisant office de serveur DNS, comme les modules Amon et AmonEcole, pour que le logiciel BIND^[p.542] puisse résoudre un nom, il faut que le suffixe DNS de ce nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet Général.

Si ce n'est pas le cas, il faut déclarer un `Nom de domaine local supplémentaire` dans l'onglet Zones-dns pour permettre au serveur de résoudre ce nom d'hôte.

Ajout de routes statiques

Ajout de routes statiques

Ajouter des routes statiques * oui

Adresse IP ou réseau à ajouter dans la table de routage

Adresse IP ou réseau à ajouter dans la table de routage *

Masque de sous réseau (mettre à 255.255.255.255 si adresse host) *

Adresse IP de la passerelle pour accéder à ce réseau *

Interface réseau reliée à la passerelle *

Numéro d'identifiant du VLAN ou rien

Autoriser ce réseau à utiliser les DNS du serveur * oui

Passer par le VPN pour accéder à ce réseau * non

Autoriser ce réseau à utiliser les DNS des zones forward additionnelles * oui

Montrer/Cacher

+ Adresse IP ou réseau à ajouter dans la table de routage

Ce bloc de paramètres permet d'ajouter, manuellement, des routes afin d'accéder à des adresses ou à des plages d'adresses par un chemin différent de celui par défaut (défini par le routeur par défaut).

Après avoir passé la variable `Ajouter des routes statiques` à `oui` il faut ajouter les paramètres suivants :

- `Adresse IP ou réseau à ajouter dans la table de routage` : permet de définir l'adresse de sous-réseau (ou l'adresse de l'hôte) vers lequel le routage doit s'effectuer ;
- `Masque de sous réseau` : permet de définir le masque du réseau défini ci-dessus (s'il s'agit d'une machine seule, il faut mettre l'adresse du masque à 255.255.255.255) ;
- `Adresse IP de la passerelle pour accéder à ce réseau` : permet de renseigner l'adresse de la passerelle permettant d'accéder au sous-réseau ou à l'hôte défini ci-dessus ;
- `Interface réseau reliée à la passerelle` : permet d'associer la route à une interface donnée. Ce champ, de type liste déroulante, comporte un certain nombre d'interfaces pré-définies. Il est possible d'en ajouter une en tapant son nom (par exemple : `ppp0`) ;
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Si le support du RVP est activé une option supplémentaire est disponible :

Autoriser ce réseau à utiliser les DNS de Forward RVP/AGRIATES * oui

- `Autoriser ce réseau à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau AGRIATES (onglet `Rvp`) la variable est disponible pour autoriser ou non les machines du réseau à résoudre les noms d'hôte de la zone AGRIATES.

Configuration du MTU

La variable `Désactiver le path MTU discovery` permet d'activer ou non le path MTU discovery [p.554] (`/proc/sys/net/ipv4/ip_no_pmtu_disc`).

Cette option est à `non` par défaut (`ip_no_pmtu_disc=0`) ce qui est le fonctionnement normal.

Cela peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP [p.549] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTU discovery est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Si vous rencontrez des problèmes d'accès à certains sites (notamment messagerie ou site intranet via le VPN, Gmail ou Gmail Apps), vous pouvez passer ce paramètre à `oui` (`ip_no_pmtu_disc=1`).

Il est possible de forcer une valeur de MTU [p.554] pour l'interface externe.

Si le champ n'est pas renseigné, la valeur par défaut est utilisée (1500 octets pour un réseau de type Ethernet).

Si l'interface est de type Ethernet et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le premier champ : `Valeur du MTU pour l'interface eth0`.

Si l'interface est de type PPPoE et que vous souhaitez forcer une valeur de MTU différente, il faut renseigner le second champ : `Valeur du MTU pour l'interface ppp0`.



Les commandes `ping`, `ip route` et `tracert` sont utilisées pour ajuster les valeurs.

Configuration de la "neighbour table"

Les variables `ipv4_neigh_default_gc_thresh1`, `ipv4_neigh_default_gc_thresh2` et `ipv4_neigh_default_gc_thresh3` servent à gérer la façon dont la table ARP évolue :

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;

- **gc_thresh2** : seuil qui, s'il est dépassé depuis un certain temps (5 secondes par défaut), déclenche le recyclage des entrées de la table qui ne sont plus utilisées ;
- **gc_thresh3** : seuil au-delà duquel le recyclage est immédiatement déclenché pour contenir la taille de la table.

Test de l'accès distant



Cette variable permet de définir le ou les domaines qui sont utilisés lorsque le module EOLE a besoin de tester son accès à Internet.

En pratique, seul l'accès au premier domaine déclaré est testé sauf dans le cas où il n'est pas accessible. Les domaines définis sont utilisés dans les outils `diagnose` et dans l'agent Zéphir.

Voir aussi...

▶ Onglet Zones-dns : Configuration du DNS [p.218]

▶ Résoudre des dysfonctionnements liés au MTU [p.408]

4.11. Onglet Certificats ssl : gestion des certificats SSL

La gestion des certificats a été standardisée pour faciliter leur mise en œuvre.

Ils sont désormais gérés par l'intermédiaire des outils Creole.

Certificats par défaut

Un certain nombre de certificats sont mis en place lors de la mise en œuvre d'un module EOLE :

- `/etc/ssl/certs/ca_local.crt` : autorité de certification propre au serveur (certificats auto-signés) ;
- `/etc/ssl/private/ca.key` : clef privée de la CA ci-dessus ;
- `/etc/ssl/certs/ACInfraEducation.pem` : contient les certificats de la chaîne de certification de l'Éducation nationale (igca/education/infrastructure) ;
- `/etc/ssl/req/eole.p10` : requête de certificat au format pkcs10, ce fichier contient l'ensemble des informations nécessaires à la génération d'un certificat ;
- `/etc/ssl/certs/eole.crt` : certificat serveur généré par la CA locale, il est utilisé par les applications (apache, ead2, eole-sso, ...) ;
- `/etc/ssl/certs/eole.key` : clé du certificat serveur ci-dessus.

Après génération de la CA locale, un fichier `/etc/ssl/certs/ca.crt` est créé qui regroupe les certificats suivants :

- `ca_local.crt` ;
- `ACInfraEducation.pem` ;

- tout certificat présent dans le répertoire `/etc/ssl/local_ca/`

Détermination du nom de serveur (commonName) dans le certificat

Le nom du sujet auquel le certificat s'applique est déterminé de la façon suivante (important pour éviter les avertissements dans les navigateurs) :

- si la variable `ssl_server_name` est définie dans l'interface de configuration du module (onglet `Certifs ssl` -> `Nom DNS du serveur`), elle est utilisée comme nom de serveur dans les certificats ;
- sinon, si un nom de domaine académique est renseigné, le nom sera : `nom machine.numero etab.nom domaine academique` (exemple : `amon monetab.0210001A.mon dom acad.fr`) ;
- le cas échéant, on utilise : `nom machine.numero etab.debut(nom academie).min(ssl_country name)` (exemple : `amon_monetab.0210001A.ac-dijon.fr`).

Mise en place d'un certificat particulier

Pour que les services d'un module EOLE utilisent un certificat particulier (par exemple, certificat signé par une autorité tierce), il faut modifier deux variables dans l'onglet `Certificats ssl` de l'interface de configuration du module.

- `Nom long du certificat SSL par défaut` (`server_cert`) : chemin d'un certificat au format PEM à utiliser pour les services ;
- `Nom long de la clé privée du certificat SSL par défaut` (`server_key`) : chemin de la clé privée correspondante (éventuellement dans le même fichier).

Dans le cas d'un certificat signé par une autorité externe, copier le certificat de la CA en question dans `/etc/ssl/local_ca/` pour qu'il soit pris en compte automatiquement (non nécessaire pour les certificats de l'IGC nationale).

Le répertoire `/etc/ssl/certs/` accueille le fichier de certificat issu de la CA interne ainsi que la clé privée correspondant au certificat.

Il faut déclarer les bons chemins dans l'interface de configuration du module.

Pour appliquer les modifications, utilisez la commande `reconfigure`.

Si les certificats configurés ne sont pas trouvés, ils sont générés à partir de la CA locale.

⚠ Le répertoire `/etc/ssl/local_ca/` n'accueille que des certificats CA.

Création de nouveaux certificats

Le script `/usr/share/creole/gen_certif.py` permet de générer rapidement un nouveau certificat SSL.

🔗 Génération d'un certificat avec `gen_certif.py`

```
root@eole:~# /usr/share/creole/gen_certif.py -fc
/etc/ssl/certs/test.crt
Generation du certificat machine
* Certificat /etc/ssl/certs/test.crt généré
```

Obtention d'un certificat signé par l'IGC de l'Éducation nationale

Étapes à suivre :

1. récupérer la requête du certificat située dans le répertoire `/etc/ssl/req/` : `eole.p10` ;
2. se connecter sur l'interface web de demande des certificats et suivre la procédure ;
3. récupérer le certificat depuis l'interface (copier/coller dans un fichier) ;
4. copier le fichier dans le répertoire `/etc/ssl/certs/`.



Seuls les ISR/OSR des académies sont accrédités pour effectuer les demandes.

Certificats intermédiaires

En attendant que la prise en compte des certificats intermédiaires soit automatisée pour l'ensemble des services de base (fixme #13362 [<https://dev-eole.ac-dijon.fr/issues/13362>]), les manipulations nécessaires pour éviter des avertissements dans les navigateurs sont documentées dans la page wiki suivante : https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Gestion_certificats

4.12. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité

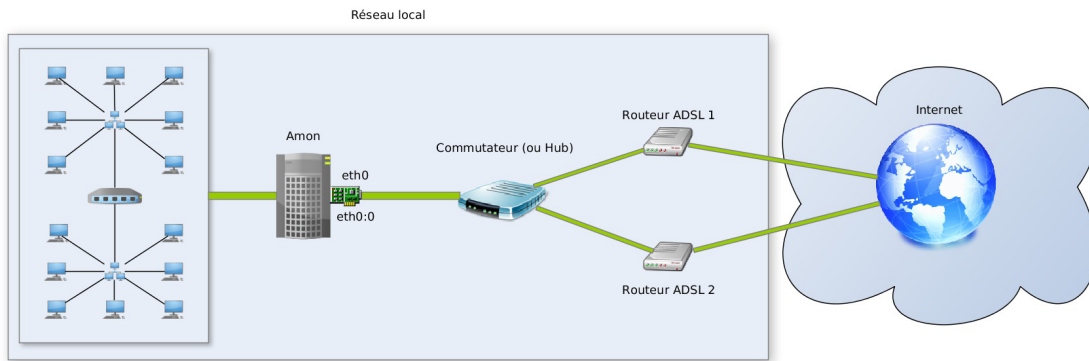
Présentation et mise en place de l'agrégation de liens

L'agrégation de liens permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

Les deux routeurs sont reliés entre eux par un commutateur (ou un Hub) à la carte eth0 du module Amon.

Dans ce cas :

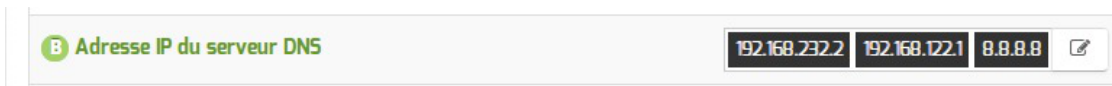
- pas besoin d'utiliser les protocoles d'annonce de routes RIP^[p.559] et OSPF^[p.556] ;
- il faut un service qui surveille l'état de chacun des liens.



- ! Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.
- La configuration de l'agrégation est le résultat de plusieurs contributions de collègues en académie. La première version a été réalisée par l'académie de Versailles, puis elle a été améliorée successivement par les académies de Nantes et de Lyon.

Onglet Général

Dans la section Adresse IP du serveur DNS de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

Il faut, en premier lieu, déclarer un alias sur l'interface eth0 dans la section Configuration des alias sur l'interface.

Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



Création d'un alias sur eth0 pour l'agrégation de liens

L'activation d'un alias IP, fait apparaître un nouveau paramètre, Répartition de charge entre 2 lignes Internet, qu'il faut passer à oui.

Agrégation de liens

N Répartition de charge entre 2 lignes Internet * oui

Un nouvel onglet, Agrégation, est disponible.

Onglet Agrégation : Configuration de l'agrégation de liens

Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la Répartition de charge entre 2 lignes Internet dans l'onglet Interface-0 comme expliqué précédemment.

Agrégation

Mode d'agrégation

N Mode load balancing ou fail-over * mode_lb

Lien 1

N Destination forcée sur le lien 1

Montrer/Cacher + Destination forcée sur le lien 1

B Adresse du DNS sur le lien 1 * Pas de valeur

B Débit mesuré sur le lien 1 (entier en Mbps) *

Lien 2

N Destination forcée sur le lien 2

Montrer/Cacher + Destination forcée sur le lien 2

B Adresse du DNS sur le lien 2 * Pas de valeur

B Débit mesuré sur le lien 2 (entier en Mbps) *

Divers

N Délai entre les tests d'état (en secondes) * 10

N Timeout de la requête DNS (en secondes) * 1

N Adresse DNS testée * www.google.com

N Nombre de succès avant changement d'état * 4

N Nombre d'échecs avant changement d'état * 1

Alerte mail

N Activation des alertes mail * non

Paramétrage de l'agrégation de liens

Modes d'agrégation



Il existe deux modes d'agrégation :

- le mode `mode_lb` (pour load balancing) correspond à la répartition de charge et fonctionne avec la notion de poids à utiliser sur les différentes passerelles ;
- le mode `mode_fo`, (pour fail-over) un seul lien est utilisé à la fois, il n'y a plus de notion de poids et il n'y a plus qu'une seule route par défaut.

Dans les deux modes il est possible de forcer des destinations IP ou réseau, et dans les deux cas si un lien tombe tous les flux (et également les destinations forcées) sont redirigés vers le second lien.

Quand les deux liens sont fonctionnels, on se retrouve dans la configuration de départ.



Le VPN, de par son mode de fonctionnement, ne peut pas être réparti entre plusieurs abonnements.

Tout le trafic devant passer par un seul lien, il est nécessaire d'utiliser le mécanisme de destination forcée.

Que le `Lien_1` ou le `Lien_2` soit choisi pour faire transiter le VPN, s'il devient indisponible, le VPN ne fonctionnera plus.

Adresse des DNS

Les champs `Adresse du DNS sur le lien 1` et `Adresse du DNS sur le lien 2` sont des champs obligatoires pour le bon fonctionnement de l'agrégation.



Les adresses DOIVENT être différentes sur chaque lien car c'est avec ces DNS que se font les tests d'état des liens.

Adresse DNS testée

Il est possible de spécifier plusieurs mires de tests qui seront testées afin de déterminer l'état des liens (résolution DNS avec le serveur DNS de chacun des liens).



L'ensemble des DNS doit être déclaré dans l'onglet `Général`.

Alerte mail

Alerte mail

Activation des alertes mail * oui

Adresse mail d'alerte * admin@ac-acad.fr

Lorsque l'un des liens est coupé, le message suivant est envoyé : Seul le lien 2 est actif, redirection des flux sur ce lien.

Quand les deux liens sont de nouveau fonctionnels, le message suivant est envoyé : Rechargement de la répartition sur les 2 liens.

4.13. Onglet Clamav : Configuration de l'anti-virus

EOLE propose un service anti-virus réalisé à partir du logiciel libre ClamAV.

<http://www.clamav.net>

Activation de l'anti-virus

L'onglet Clamav n'est accessible que si le service est activé dans l'onglet Services. Pour ce faire, passer la variable Activer l'anti-virus ClamAV à oui.

Sur le module Amon, il n'est possible d'activer l'anti-virus que sur le proxy et sur la messagerie.

Clamav

Freshclam

Activer l'anti-virus sur le proxy * non

Activer l'anti-virus sur la messagerie * non



Si aucun service n'utilise l'anti-virus, il est utile de le désactiver dans l'onglet Services. Il faut passer la variable Activer l'anti-virus ClamAV à non. L'onglet Clamav n'est alors plus visible.

Activation de l'anti-virus sur le proxy

Pour activer l'anti-virus en temps réel sur les fichiers filtrés par le proxy Internet, il faut passer la variable Activer l'anti-virus sur le proxy à oui dans l'onglet Clamav.

Activer l'anti-virus sur le proxy * oui

L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.



L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU^[p.544]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

Pour activer l'anti-virus sur la messagerie il faut passer la variable Activer l'antivirus sur la messagerie à oui dans l'onglet Clamav .

Activer l'anti-virus sur la messagerie

* oui

Forcer l'activation du service clamd

Si Activer l'anti-virus ClamAV est à oui dans l'onglet Service mais qu'aucun service EOLE ne l'utilise alors seul le service de mise à jour de la base de signatures (freshclam) sera actif sur le serveur.

À partir de la version 2.5.2 d'EOLE, il est possible de forcer l'activation du service anti-virus (clamd) en passant la variable du mode expert Forcer l'activation du démon clam sur le serveur à oui dans l'onglet Clamav .

Services utilisant ClamAV

Forcer l'activation du démon clam sur le serveur

* oui

Configuration avancée

En mode expert, l'onglet Clamav comporte de nombreuses variables qui permettent d'affiner la configuration de ClamAV.

Clamav

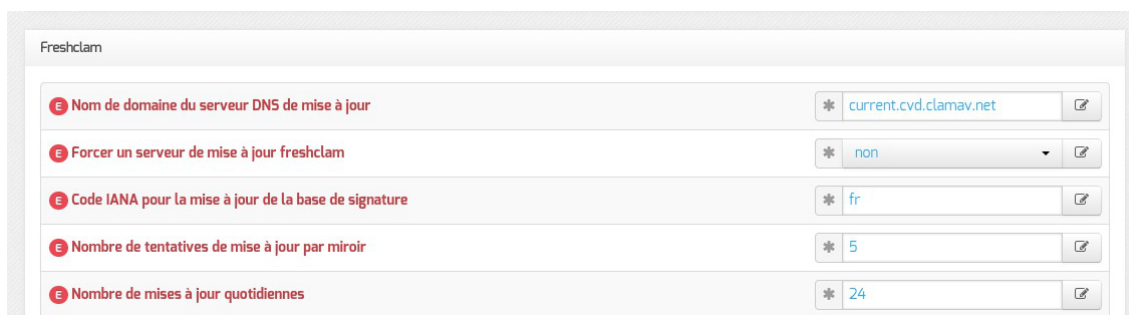
ClamAV

Taille maximum pour un fichier à scanner (en Mo)	* 5
Quantité de données maximum à scanner pour une archive (en Mo)	* 20
Profondeur maximale pour le scan des archives	* 12
Nombre maximum de fichiers à scanner dans une archive	* 5000
Arrêter le démon en cas de surcharge mémoire	* no
Détection des applications indésirables	* no
Scan du contenu des fichiers ELF	* no
Scan du contenu des fichiers PDF	* yes
Scan des fichiers courriels	* no
Détection des fichiers exécutables corrompus	* no

- Taille maximum pour un fichier à scanner (en Mo) ;
- Quantité de données maximum à scanner pour une archive (en Mo) ;
- Profondeur maximale pour le scan des archives ;

- Nombre maximum de fichiers à scanner dans une archive ;
- Arrêter le démon en cas de surcharge mémoire ;
- Détection des applications indésirables ;
- Scan du contenu des fichiers ELF ^[p.546] ;
- Scan du contenu des fichiers PDF ;
- Scan des fichiers courriels ;
- Détection des fichiers exécutables corrompus.

En mode expert, l'onglet **Clamav** comporte des variables qui permettent d'affiner la configuration de Freshclam, le service de mise à jour de la base de signatures.



Variable	Valeur
Nom de domaine du serveur DNS de mise à jour	current.cvd.clamav.net
Forcer un serveur de mise à jour freshclam	non
Code IANA pour la mise à jour de la base de signature	fr
Nombre de tentatives de mise à jour par miroir	5
Nombre de mises à jour quotidiennes	24

- Nom de domaine du serveur DNS de mise à jour permet de spécifier un miroir interne pour les signatures ;
- Forcer un serveur de mise à jour freshclam permet d'ajouter un ou plusieurs miroirs pour les signatures ;
- Code IANA pour la mise à jour de la base de signature ;
- Nombre de tentatives de mise à jour par miroir permet de réduire le nombre de tentatives de mise à jour, en effet des fichiers sont récupérés systématiquement à chaque tentative ;
- Nombre de mises à jour quotidiennes permet de réduire le nombre de mises à jour quotidiennes.

Contribuer

La base de données de virus est mise à jour avec l'aide de la communauté.

Il est possible de faire des signalements :

- signaler de nouveaux virus qui ne sont pas détectés par ClamAV ;
- signaler des fichiers propres qui ne sont pas correctement détectés par ClamAV (faux-positif).

Pour cela il faut utiliser le formulaire suivant (en) : <http://www.clamav.net/contact#reports>

L'équipe de ClamAV examinera votre demande et mettra éventuellement à jour la base de données.

En raison d'un nombre élevé de déposants, il ne faut pas soumettre plus de deux fichiers par jour.



Il ne faut pas signaler des PUA^[p.559] comme étant des faux positifs.

4.14. Onglet Relai DHCP

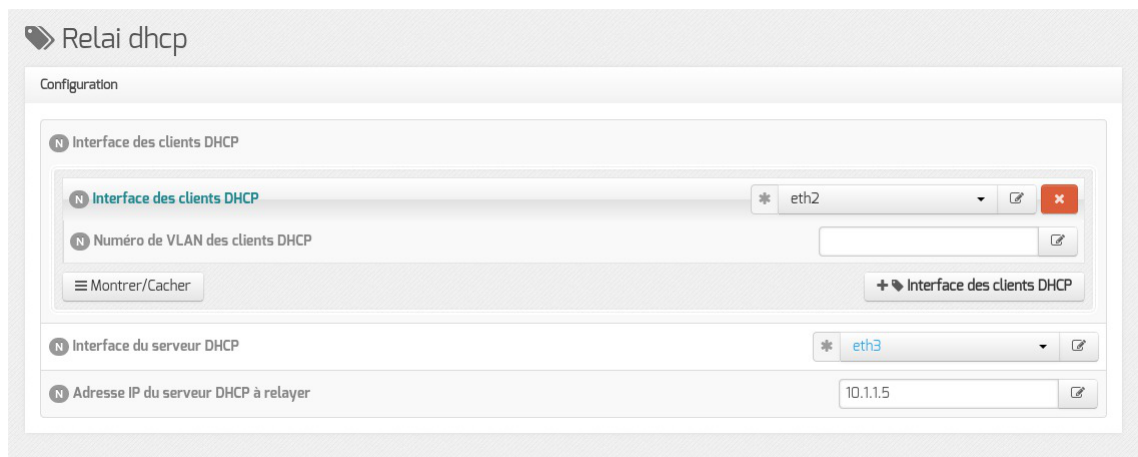
Pour des raisons de sécurité, le service DHCP^[p.544] n'a pas, à priori, à être installé sur le module Amon. Il vaut mieux utiliser un autre module (module Scribe ou module Horus par exemple) pour fournir ce service.

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast^[p.542].

De ce fait, les trames ne sont, par défaut, pas routables d'un réseau vers un autre.

Si le serveur DHCP ne se situe pas sur la même zone que les stations, il faut mettre en place un relai DHCP.

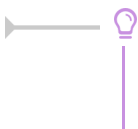
L'onglet **Relai dhcp** n'est accessible que si le service est activé dans l'onglet **Services**. Pour ce faire, passer la variable Activer le relai DHCP à oui.



Vue de l'onglet Relai dhcp de l'interface de configuration du module

Dans la configuration ci-dessus (4zones), on déclare que l'on veut relayer le DHCP du module Scribe (adresse IP : 10.1.1.5) qui se trouve dans la DMZ (eth3 est la 4ème interface) vers le réseau pédagogique (eth2 est la 3ème interface).

Il est possible de restreindre le relayage sur un VLAN^[p.563] particulier en renseignant son numéro dans la variable Numéro de VLAN des clients DHCP.



Grâce au découpage des paquets par services, la mise en œuvre d'un DHCP sur le module Amon, bien que déconseillée, est facilitée par le paquet eole-dhcp.

Voir aussi...

[eole-dhcp](#) ^[p.415]

[Configuration du module Amon avec le module Scribe en DMZ](#)

[p.256]

4.15. Onglet Onduleur

Sur chaque module EOLE, il est possible de configurer votre onduleur.

Le logiciel utilisé pour la gestion des onduleurs est NUT^[p.556]. Il permet d'installer plusieurs clients sur le

même onduleur. Dans ce cas, une machine aura le contrôle de l'onduleur (le maître/master) et en cas de coupure, lorsque la charge de la batterie devient critique, le maître indiquera aux autres machines (les esclaves) de s'éteindre avant de s'éteindre lui-même.

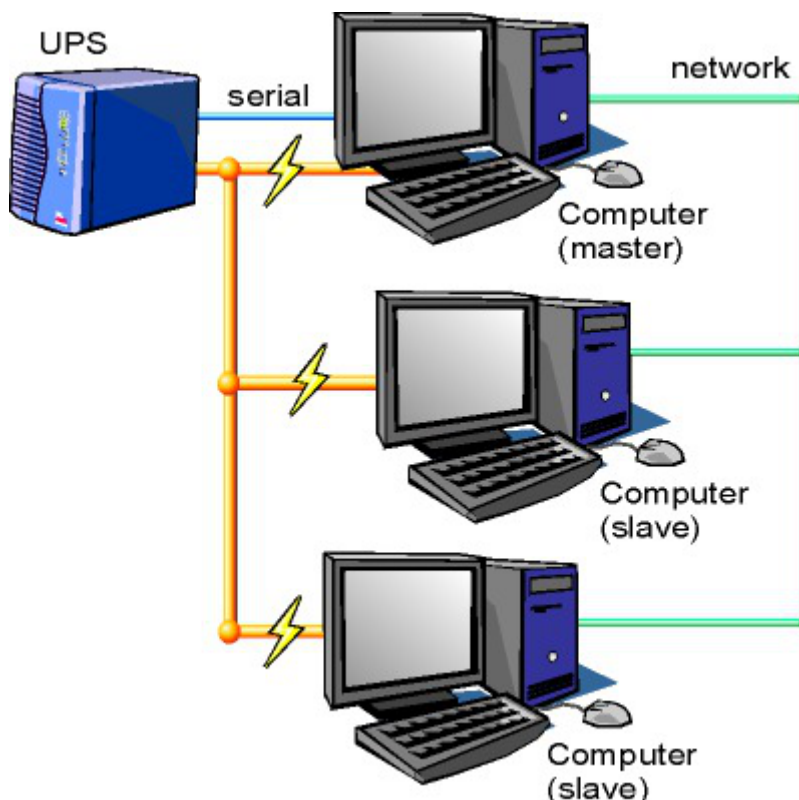


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - <http://ovanhoof.developpez.com/upsusb/>

Certains onduleurs sont assez puissants pour alimenter plusieurs machines.

<http://www.networkupstools.org/>

Le projet offre une liste de matériel compatible avec le produit mais cette liste est donnée pour la dernière version du produit :

<http://www.networkupstools.org/stable-hcl.html>



Pour connaître la version de NUT qui est installée sur le module :

```
# apt-cache policy nut
```

ou encore :

```
# apt-show-versions nut
```

Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :

<http://www.networkupstools.org/source/2.7/new-2.7.1.txt>

Si le matériel n'est pas dans la liste, on peut vérifier que sa prise en charge soit faite par une version plus récente et donc non pris en charge par la version actuelle :

<http://www.networkupstools.org/source/2.7/new-2.7.3.txt>

L'onglet **Onduleur** n'est accessible que si le service est activé dans l'onglet **Services**.

Si l'onduleur est branché directement sur le module il faut laisser la variable Configuration sur un serveur maître à oui, cliquer sur le bouton + Nom de l'onduleur et effectuer la configuration liée au serveur maître.

La configuration sur un serveur maître

Même si le nom de l'onduleur n'a aucune conséquence, il est obligatoire de remplir cette valeur dans le champ Nom pour l'onduleur.

Il faut également choisir le nom du pilote de l'onduleur dans la liste déroulante Pilote de communication de l'onduleur et éventuellement préciser le Port de communication si l'onduleur n'est pas USB.

Les champs Numéro de série de l'onduleur, Productid de l'onduleur et Upstype de l'onduleur sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.

Configuration d'un second onduleur sur un serveur maître

Si le serveur dispose de plusieurs alimentations, il est possible de les connecter chacune d'elle à un

onduleur différent.

Il faut cliquer sur le bouton `+ Nom de l'onduleur` pour ajouter la prise en charge d'un onduleur supplémentaire dans l'onglet `Onduleur` de l'interface de configuration du module.

Si les onduleurs sont du même modèle et de la même marque, il faut ajouter de quoi permettre au pilote NUT de les différencier.

Cette différenciation se fait par l'ajout d'une caractéristique unique propre à l'onduleur. Ces caractéristiques dépendent du pilote utilisé, la page de `man` du pilote vous indiquera lesquelles sont disponibles.

Exemple pour le pilote Solis :

```
# man solis
```

Afin de récupérer la valeur il faut :

- ne connecter qu'un seul des onduleurs ;
- le paramétrer comme indiqué dans la section précédente ;
- exécuter la commande : `upsc <nomOnduleurDansGenConfig>@localhost | grep <nom variable>` ;
- débrancher l'onduleur ;
- brancher l'onduleur suivant ;
- redémarrer `nut` avec la commande : `# service nut restart` ;
- exécuter à nouveau la commande pour récupérer la valeur de la variable.

Une fois les numéros de série connus, il faut les spécifier dans les champ `Numéro de série de l'onduleur` de chaque onduleur.

Deux onduleurs de même marque

Pour deux onduleurs de marque MGE, reliés à un module Scribe par câble USB, il est possible d'utiliser la valeur "serial", voici comment la récupérer :

```
# upsc <nomOnduleurDansGenConfig>@localhost | grep serial
driver.parameter.serial: AV4H4601W
ups.serial: AV4H4601W
```

Deux onduleurs différents

Un onduleur sur port série :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `apcsmart` ;
- Port de communication de l'onduleur : `/dev/ttyS0`.

Si l'onduleur est branché sur le port série (en général : `/dev/ttyS0`), les droits doivent être adaptés.

Cette adaptation est effectuée automatiquement lors de l'application de la configuration.

Onduleur sur port USB :

- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l'onduleur : `usbhid-ups` ;

- Port de communication de l'onduleur : `auto`.
- La majorité des onduleurs USB sont détectés automatiquement.



Attention, seul le premier onduleur sera surveillé.

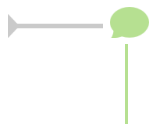
Autoriser des esclaves distants à se connecter

Pour déclarer un serveur esclave, il faut passer la variable `Autoriser des esclaves distants à se connecter` à `oui` puis ajouter un utilisateur sur le serveur maître afin d'autoriser l'esclave à se connecter avec cet utilisateur.

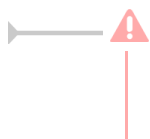
Idéalement, il est préférable de créer un utilisateur différent par serveur même s'il est possible d'utiliser un unique utilisateur pour plusieurs esclaves. Pour configurer plusieurs utilisateurs il faut cliquer sur le bouton `+ Utilisateur de surveillance de l'onduleur`.

Pour chaque utilisateur, il faut saisir :

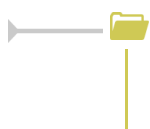
- un `Utilisateur de surveillance de l'onduleur` ;
- un `Mot de passe de surveillance de l'onduleur` associé à l'utilisateur précédemment créé ;
- l'`Adresse IP du réseau de l'esclave` (cette valeur peut être une adresse réseau plutôt qu'une adresse IP) ;
- le `Masque de l'IP du réseau de l'esclave` (comprendre le masque du sous réseau de l'adresse IP de l'esclave)



Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : `[a-z][0-9]` sans espaces, ni caractères spéciaux.



Chaque utilisateur doit avoir un nom différent.
Les noms `root` et `localmonitor` sont réservés.



Pour plus d'informations, vous pouvez consulter la page de manuel : `man ups.conf`

ou consulter la page web suivante :
<http://manpages.ubuntu.com/manpages/trusty/en/man5/ups.conf.5.html>

Configurer un serveur esclave

Une fois qu'un serveur maître est configuré et fonctionnel, il est possible de configurer le ou les serveurs esclaves.

Pour configurer le module en tant qu'esclave, il faut activer le service dans l'onglet **Services** puis, dans l'onglet **Onduleur**, passer la variable Configuration sur un serveur maître à non.

Il faut ensuite saisir les paramètres de connexion à l'hôte distant :

- le Nom de l'onduleur distant (valeur renseignée sur le serveur maître) ;
- l'Hôte gérant l'onduleur (adresse IP ou nom d'hôte du serveur maître) ;
- l'Utilisateur de l'hôte distant (nom d'utilisateur de surveillance créé sur le serveur maître) ;
- le Mot de passe de l'hôte distant (mot de passe de l'utilisateur de surveillance créé sur le serveur maître).

Exemple de configuration



Sur le serveur maître :

- Nom de l'onduleur : eoleups ;
- Pilote de communication de l'onduleur : usbhid-ups ;
- Port de communication de l'onduleur : auto ;
- Utilisateur de surveillance de l'onduleur : scribe ;
- Mot de passe de surveillance de l'onduleur : 99JJUE2EZOAI2IZI10IIZ93I187UZ8 ;
- Adresse IP du réseau de l'esclave : 192.168.30.20 ;
- Masque de l'IP du réseau de l'esclave : 255.255.255.255.



Sur le serveur esclave :

- Nom de l'onduleur distant : eoleups ;
- Hôte gérant l'onduleur : 192.168.30.10 ;

- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

4.16. Onglet Eole sso : Configuration du service SSO pour l'authentification unique

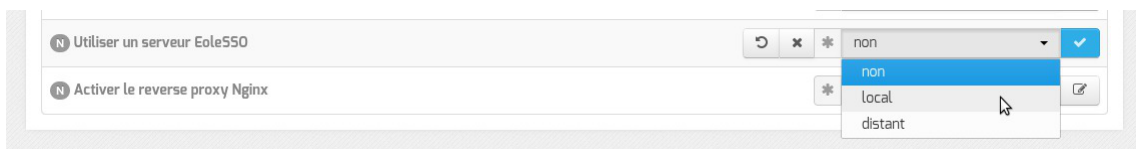
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

Il est cependant possible de l'utiliser dans un autre environnement en modifiant manuellement le fichier de configuration `/usr/share/sso/config.py`.

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les modules EOLE. Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur les modules EOLE.

Serveur local ou distant

L'activation du serveur EoleSSO s'effectue dans l'onglet `Services`.



La variable `Utiliser un serveur EoleSSO` permet :

- `non` : de ne pas utiliser de SSO sur le serveur ;
- `local` : d'utiliser et de configurer le serveur EoleSSO local ;
- `distant` : d'utiliser un serveur EoleSSO distant (configuration cliente).

Adresse et port d'écoute

L'onglet supplémentaire `Eole-sso` apparaît si l'on a choisi d'utiliser un serveur EoleSSO local ou distant.

Eole sso
Configuration

- Nom de domaine du serveur d'authentification SSO
- Port utilisé par le service EoleSSO: 8443
- Adresse du serveur LDAP utilisé par EoleSSO: localhost
 - Port du serveur LDAP utilisé par EoleSSO: 389
 - Chemin de recherche dans l'annuaire: o=gouv,c=fr
 - Libellé à présenter aux utilisateurs en cas d'homonymes: Annuaire de amon.monreseau.lar
 - Informations supplémentaire dans le cadre d'information sur les homonymes
 - Utilisateur de lecture des comptes LDAP (nécessaire pour la fédération): cn=reader,o=gouv,c=fr
 - Fichier de mot de passe de l'utilisateur de lecture: /root/.reader
 - Attribut de recherche des utilisateurs: uid
- Information LDAP supplémentaires (applications): non
- Adresse du serveur SSO parent
- Port du serveur SSO parent: 8443
- Nom d'entité SAML du serveur eole-ss0 (ou rien)
- Gestion de l'authentification OTP (RSA SecurID): non
- Chemin du certificat SSL (ou rien)
- Chemin de la clé privée liée au certificat SSL (ou rien)
- Chemin de l'autorité de certification (ou rien)
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200
- CSS par défaut du service SSO (sans le .css)
- Cacher le formulaire lors de l'envoi des informations de fédération: non

Configuration d'un serveur EoleSSO local

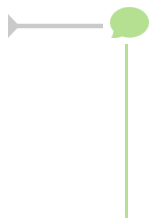
Dans le cas de l'utilisation d'un serveur EoleSSO distant, seuls les paramètres Nom de domaine du serveur d'authentification SSO et Port utilisé par le service EoleSSO sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.

Eole sso
Configuration

- Nom de domaine du serveur d'authentification SSO: etb1.ac-test.fr
- Port utilisé par le service EoleSSO: 8443
- Durée de vie d'une session sur le serveur SSO (en secondes): 7200

Configuration d'un serveur EoleSSO distant

Dans le cas de l'utilisation du serveur EoleSSO local, Nom de domaine du serveur d'authentification SSO doit être renseigné avec le nom DNS du serveur.



Par défaut le serveur communique sur le port 8443. Il est conseillé de laisser cette valeur par défaut en cas d'utilisation avec d'autres modules EOLE.

Si vous décidez de changer ce port, pensez à le changer également dans la configuration des autres machines l'utilisant.

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP pour authentifier les utilisateurs et récupérer leurs attributs.

Il est possible ici de modifier les paramètres d'accès à ceux-ci :

- l'adresse et le port d'écoute du serveur LDAP ;
- le chemin de recherche correspond à l'arborescence de base dans laquelle rechercher les utilisateurs ;
- un libellé à afficher dans le cas où un utilisateur aurait à choisir entre plusieurs annuaires/établissements pour s'authentifier (voir le chapitre Gestion des sources d'authentifications multiples) ;
- un fichier d'informations à afficher dans le cadre qui est présenté en cas d'homonymes. Ces informations apparaîtront si l'utilisateur existe dans l'annuaire correspondant. Les fichiers doivent être placés dans le répertoire /usr/share/sso/interface/info_homonymes ;
- DN et mot de passe d'un utilisateur en lecture pour cet annuaire ;
- attribut de recherche des utilisateurs : indique l'attribut à utiliser pour rechercher l'entrée de l'utilisateur dans l'annuaire (par défaut, uid)
- choix de la disponibilité ou non de l'authentification par clé OTP^[p.557] si disponible (*voir plus loin*).



Dans le cas où vous désirez fédérer EoleSSO avec d'autres fournisseurs de service ou d'identité (ou 2 serveurs EoleSSO entre eux), il est nécessaire de configurer un utilisateur ayant accès en lecture au serveur LDAP configuré.

Il sera utilisé pour récupérer les attributs des utilisateurs suite à réception d'une assertion d'un fournisseur d'identité (ou dans le cas d'une authentification par OTP).

Cet utilisateur est pré-configuré pour permettre un accès à l'annuaire local sur les serveurs EOLE.

Sur les modules EOLE, la configuration recommandée est la suivante :

- utilisateur : cn=reader,o=gouv,c=fr
- fichier de mot de passe : /root/.reader

Si vous connectez EoleSSO à un annuaire externe, vous devez définir vous même cet utilisateur :

- Utilisateur de lecture des comptes ldap : renseignez son *dn* complet dans l'annuaire

- fichier de mot de passe de l'utilisateur de lecture : entrez le chemin d'un fichier ou vous stockerez son mot de passe (modifiez les droits de ce fichier pour qu'il soit seulement accessible par l'utilisateur root)

Passer la variable Information LDAP supplémentaires (applications) à oui permet de configurer pour chaque annuaire LDAP déclaré des attributs supplémentaires qui seront utilisés par les applications web (DN racine de l'arbre utilisateurs, DN racine de l'arbre groupes, Champ 'nom d'affichage' de l'utilisateur, Champ 'mail' de l'utilisateur, Champ 'fonction' de l'utilisateur, Champ 'categorie' de l'utilisateur, Champ 'rne' de l'utilisateur, Champ 'fredurne' de l'utilisateur...).

Serveur SSO parent

Un autre serveur EoleSSO peut être déclaré comme serveur parent dans la configuration (adresse et port). Se reporter au chapitre traitant de la fédération pour plus de détails sur cette notion.

Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essaiera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs se fait par l'intermédiaire d'appels XML-RPC^[p.564] en HTTPS, sur le port défini pour le serveur EoleSSO).

Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).



Ce mode de fonctionnement n'est plus recommandé aujourd'hui. Il faut préférer à cette solution la mise en place d'une fédération par le protocole SAML.

Prise en compte de l'authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole securID^[p.560] de la société EMC (précédemment RSA).

Pour cela il faut :

- installer et configurer le client PAM/Linux proposé par EMC (voir annexes)
- Répondre oui à la question Gestion de l'authentification OTP (RSA SecurID)

Des champs supplémentaires apparaissent :

- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. 'inactifs' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec 'identiques', le login local (LDAP) de l'utilisateur sera également utilisé comme login OTP. La dernière option est 'configurables', et indique que les utilisateurs doivent renseigner eux même leur login OTP. Dans ce dernier cas, l'identifiant est conservé sur le serveur EoleSSO pour que l'utilisateur n'ait pas à le renseigner à chaque fois (fichier /usr/share/sso/securid_users/securid_users.ini).
- Le formulaire d'authentification détecte automatiquement si le mot de passe entré est un mot de passe OTP. Il est possible de modifier la reconnaissance si elle ne convient pas en réglant les tailles minimum et maximum du mot de passe et en donnant une expression régulière qui sera vérifiée si la taille correspond. Les options par défaut correspondent à un mot de passe de 10 à 12 caractères

uniquement numériques.

Certificats

Les communications de et vers le serveur EoleSSO sont chiffrées.

Sur les modules EOLE, des certificats auto-signés sont générés à l'instanciation^[p.550] du serveur et sont utilisés par défaut.

Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autres types de serveurs compatibles avec le protocole SAML^[p.560] (version 2).

Nom d'entité SAML du serveur eole-ssso (ou rien) : nom d'entité du serveur EoleSSO local à indiquer dans les messages SAML. Si le champ est laissé à vide, une valeur est calculée à partir du nom de l'académie et du nom de la machine.

Cacher le formulaire lors de l'envoi des informations de fédération : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant la fédération.

Autres options

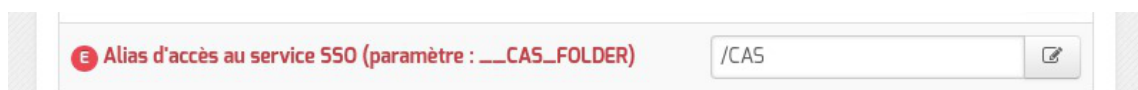
Durée de vie d'une session (en secondes) : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).

CSS par défaut du service SSO (sans le .css) : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/ssso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet.*

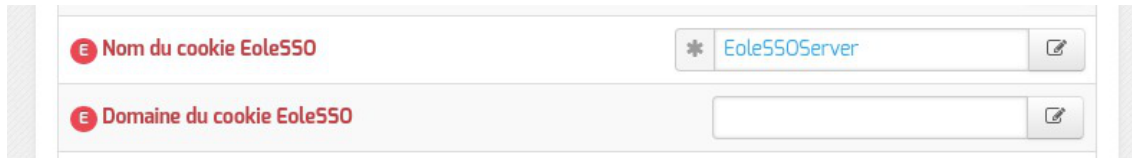
Configuration en mode expert

Options générales

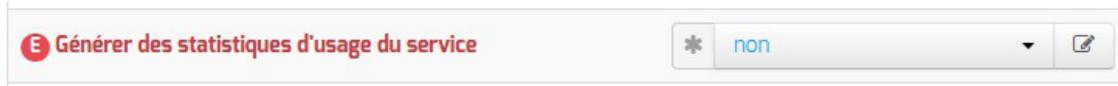
En mode expert plusieurs nouvelles variables sont disponibles :



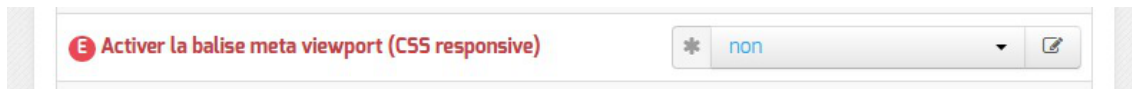
- Alias d'accès au service SSO (paramètre : CAS_FOLDER) permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP ou keycloak.



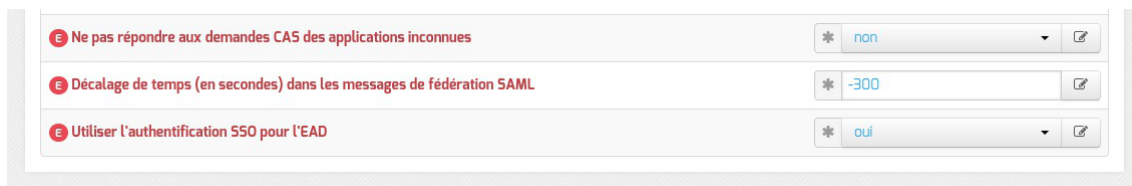
- Nom du cookie EoleSSO et Domaine du cookie EoleSSO permettent la gestion d'un cluster EoleSSO.



- Générer des statistiques d'usage du service est à non par défaut.
Si ce paramètre est à oui, eole-ss0 va générer des statistiques sur l'usage du service (consommation mémoire, nombre de session, ...). Ces statistiques sont générées par la librairie python prometheus-client. Elles peuvent être intégrées à un outil tel que Grafana, et sont disponible sur l'URL suivante : https://<adresse_serveur>:8443/metric [https://<adresse_serveur>:8443/metrics].



- Activer la balise meta viewport (CSS responsive) permet d'inclure la balise HTML meta viewport dans les pages de l'application (avec content="width=device-width, initial-scale=1"). Elle est à activer en cas d'utilisation d'une feuille de style CSS responsive.



- Ne pas répondre aux demandes CAS des applications inconnues est à non par défaut
Si ce paramètre est à oui, seules les applications renseignées dans les fichiers d'applications (`/usr/share/sso/app_filters/*_apps.ini`) sont autorisées à recevoir des réponses du serveur en mode CAS. Si il est à non, le filtre par défaut leur sera appliqué ;
- Décalage de temps (en secondes) dans les messages de fédération SAML est à -300 secondes par défaut
Ce décalage est appliqué aux dates dans les messages de fédération SAML. Cela permet d'éviter le rejet des messages lorsque le serveur partenaire n'est pas tout à fait synchrone (par défaut, on décale de 5 minutes dans le passé). Ce délai est aussi pris en compte pour la validation des messages reçus ;
- Utiliser l'authentification SSO pour l'EAD est à oui par défaut. Le passer à non permet de ne plus utiliser le serveur SSO pour l'authentification de l'EAD.

Configuration d'authentification OpenID Connect

- Autoriser l'authentification OpenID Connect est à non par défaut
Si ce paramètre est à oui, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- Référence du fournisseur d'identité OpenID : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
 - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;
 - `/usr/share/sso/interface/images/logo-<libelle>.png` : logo du fournisseur qui sera affiché sur la page d'association de comptes.
- Libellé du fournisseur d'identité OpenID : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- URL d'accès (issuer) : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- URL de demande d'autorisation (authorization endpoint) : URL permettant au client d'initier le processus d'authentification ;
- URL de récupération de jeton d'accès (token endpoint) : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- URL de déconnexion (logout endpoint) : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- URL de lecture des informations (userinfo endpoint) : URL permettant de

recupérer les informations de l'utilisateur à l'aide du jeton fourni ;

- URL de description des certificats de signature (jwks URI) : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

Définition de l'identifiant client (Client ID) et clé secrète (Client secret)



L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

Le nom_fournisseur doit correspondre au paramètre Référence du fournisseur d'identité OpenID renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose` .

Voir aussi...

Gestion des sources d'authentification multiples

Compatibilité OpenID Connect

4.17. Onglet Rvp : Mettre en place le réseau virtuel privé

The screenshot displays the 'Rvp' configuration page in the Amon 2.5.2 interface. The left sidebar lists various system services, with 'Rvp' highlighted. The main configuration area is organized into several sections:

- Paramètres strongSwan:**
 - Nombre d'essais de retransmission avant Dead Peer Detection: 11
 - Timeout pour le process stroke: 0
- Gestion des Routes VPN:**
 - Gestion des routes par strongSwan: non
 - Forcer l'adresse IP source de l'interface: eth1
- Gestion des threads:**
 - Nombre de threads disponibles pour strongSwan: 32
 - Nombre de threads à réserver pour les jobs HIGH priority: 2
 - Nombre de threads à réserver pour les jobs MEDIUM priority: 4
- Paramètres agent Zéphir RVP et diagnose:**
 - Agent RVP Zéphir en mode 'No action': non
 - Adresses IP à tester dans test-rvp: Pas de valeur
- Paramètres IPsec:**
 - Contrôle du status des certificats dans la CRL: oui
- Accès RVP par le proxy:**
 - Accès RVP par le proxy: non
- AGRIATES:**
 - Serveur membre du réseau AGRIATES: non

At the bottom of the interface, it states 'Powered By EOLE' and 'Onglet Rvp mode Expert'.

Le réseau virtuel privé^[p.559] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur des modules Amon déjà en exploitation.

Mise en place du RVP

L'onglet **Rvp** apparaît après activation du service dans l'onglet **Services**.

Activer le réseau virtuel privé RVP

* oui

Configuration des tunnels

- !** Le mode VPN database n'est plus supporté et n'est plus disponible à partir de la version 2.5.1 du module Amon. La configuration des tunnels s'effectue d'office en mode fichier plat.
- !** À l'occasion de la mise en place d'un nouveau tunnel avec un serveur Sphynx inférieur à la version EOLE 2.5, il faudra impérativement configurer ce serveur Sphynx en mode database à non.

Accès RVP par le proxy

Pour paramétrer l'accès RVP par le proxy, il faut passer la variable `Accès RVP par le proxy` à `oui`.

Accès RVP par le proxy

Accès RVP par le proxy

* oui

Adresse réseau de la zone RVP

Adresse réseau de la zone RVP

Masque de sous-réseau de la zone RVP

Autoriser d'autres zones que eth1 à accéder à ce réseau

Montrer/Cacher

+ Adresse réseau de la zone RVP

L'adresse réseau de la zone RVP permet la configuration du proxy Squid pour autoriser ou non, aux postes autres que sur l'interface eth1, l'accès via le VPN à un sous réseau.

Pour ajouter d'autres adresses réseau il faut cliquer sur le bouton `+Adresse réseau de la zone RVP`.

Paramètres agent Zéphir RVP et diagnose

Le champ `Adresses IP à tester dans test-rvp` permet de saisir une ou plusieurs adresses IP qui seront utilisées par le diagnose et par l'agent Zéphir pour tester des adresses IP à l'autre extrémité des tunnels.

Paramètres agent Zéphir RVP et diagnose

Adresses IP à tester dans test-rvp

Pas de valeur

AGRIATES

Si le serveur est membre d'AGRIATES il faut passer la variable `Serveur membre du réseau AGRIATES` à `oui`.

- Adresse du DNS permettant de résoudre les in.ac-acad.fr permet de spécifier l'adresse IP du serveur DNS permettant de résoudre les noms de zone AGRIATES (in.ac-académie.fr) ;
- Nom DNS de la zone résolue par le DNS AGRIATES : permet de spécifier d'autres noms de zones résolues par le DNS AGRIATES.

Paramètres propres au mode expert

Le mode Expert permet de personnaliser le fonctionnement de strongSwan.

Forcer l'encapsulation (Détection NAT), si la valeur est à oui, cela force la socket UDP/4500 pour l'établissement des connexions. Si la valeur est à non, le socket est fixé à UDP/500 sauf s'il y a détection de NAT (UDP/4500).

Autoriser le changement d'adresse IP d'une extrémité de connexion (MOBIKE IKEv2 extension - RFC 4555) permet à une extrémité de changer d'adresse IP pour une connexion donnée. Dans ce cas, la connexion se fera toujours sur UDP/4500.

Paramètres strongSwan

Nombre d'essais de retransmission avant Dead Peer Detection indique à strongSwan le nombre d'essais de reconnexion avant l'abandon.

Timeout pour le process stroke permet de fixer le nombre de millisecondes avant l'arrêt forcé de processus qui se seraient figés.

La variable Configuration des tunnels en mode database n'est plus disponible dans la version 2.5 d'EOLE, ce mode a été supprimé au profit du mode fichier plat.

Gestion des Routes VPN



Onglet Rvp mode Expert

Gestion des routes par strongSwan permet si la valeur est passée à non de faire gérer la mise en place des routes concernant les tunnels par un script.

Exemple, dans notre cas et sur le module Amon uniquement :

```
/etc/ipsec.d/ipsec_updown
```

Forcer l'adresse IP source de l'interface permet de forcer l'adresse IP que le serveur utilisera pour entrer dans les tunnels. Cette option est utilisée sur les serveur Amon afin d'éviter qu'ils utilisent aléatoirement l'adresse IP de l'une de ses interfaces lorsqu'ils passent dans un tunnel.

Gestion des threads



Nombre de threads disponibles pour strongSwan permet d'allouer un nombre de fils d'exécution maximum pour ses différentes tâches. Une valeur trop petite peut entraîner des mises en file d'attente importantes.

Nombre de threads à réserver pour les jobs HIGH priority réserve un nombre de fils d'exécution minimum pour les tâches HIGH priority (`ipsec stroke` et DPD). La valeur 1 ou 2 maximum est idéale.

Nombre de threads à réserver pour les jobs MEDIUM priority réserve un nombre de fils d'exécution minimum pour les tâches MEDIUM priority (Initialisation de connexion entre autres).

Paramètres agent Zéphir RVP et diagnose



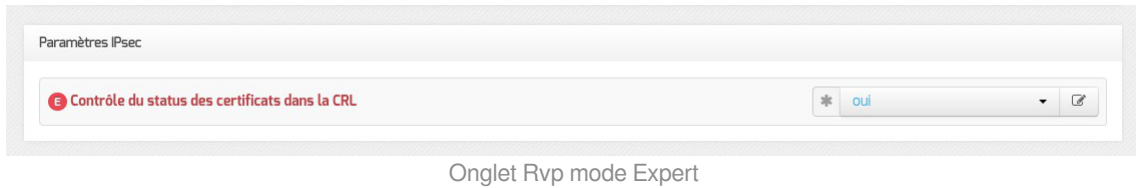
Onglet Rvp mode Expert

Agent rvp Zéphir en mode 'No action' permettait sur les versions strictement inférieures à EOLE 2.4.2 de paramétrer l'agent RVP pour ne rien faire en cas de détection de tunnels défectueux (pas de coupure/relance des tunnels).



Cette variable est sans effet depuis la version EOLE 2.4.2.

Paramètres IPsec



Onglet Rvp mode Expert

Active ou non la vérification de la validité d'un certificat dans la liste de révocation (CRL^[p.544]).

Application de la configuration et gestion du RVP

Activation du RVP au moment de l'instanciation du serveur Amon

Au lancement de l'instanciation, la question suivante vous est posée :

Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non]
[non] :

Vous devez répondre oui à cette question.

Deux choix sont alors proposés :

1. Manuel permet de prendre en compte la configuration RVP présente sur une clé USB ;
2. Zéphir active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le serveur est déjà enregistré sur Zéphir. Il sera demandé un compte Zéphir et son code secret ainsi que l'identifiant Zéphir du serveur Sphynx auquel associer le module Amon.

Dans les deux cas, le code secret de la clé privée est demandée. Si le code secret est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur root la commande `active_rvp init`.



Lors de cette phase de configuration du VPN sur Amon, les tunnels peuvent se couper dans les secondes qui suivent et dans certaines circonstances uniquement. Le problème est corrigé à partir de la version strongSwan 5.5.0 qui n'est pas disponible sur cette version d'EOLE.

Toutefois, le problème est très ponctuel et les tunnels seront relancés automatiquement par l'agent Zéphir assez rapidement.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur root la commande `active_rvp delete`.

4.18. Onglet Zones-dns : Configuration du DNS

EOLE propose un serveur DNS^[p.545] local qui a pour rôles principaux de servir de cache afin d'accélérer les requêtes et de résoudre certains noms de domaines locaux.

Dans le cadre du module Amon, il est en mesure de gérer les différentes zones du réseau établissement. La génération des différents fichiers de configuration (fichiers de zones) est effectuée par un programme appelé `h2n`.

Il est possible, depuis l'interface de configuration du module, d'activer ou non certaines fonctionnalités et d'ajouter des valeurs au niveau du DNS.

Configuration DNS sur l'interface-0

Sur une installation en mode une carte (exemple : EoleBase + `eole-dns`), le DNS est activable ou désactivable dans l'onglet `Interface-0` avec la variable : `Activer le serveur DNS sur cette zone`.

Sur le module Amon et ses variantes (AmonEcole, AmonEcole+), cette question est également présente dans l'onglet `Interface-0`.

Pour chacune des interfaces configurées, il est possible de préciser si le DNS est maître de la zone en passant la variable `Serveur master DNS sur cette zone` à `oui`.

 Au moins une des zones doit être configurée en maître de la zone.

Personnalisation des zones DNS

L'onglet expert `Zones-dns` comporte plusieurs variables directement liées au DNS.

L'onglet Zones-dns

Le champs `Nom de domaine local supplémentaire ou rien` permet au serveur DNS de résoudre les noms de ce domaine.

Si un nom d'hôte avec un suffixe DNS différent du nom de domaine privé du réseau local est déclaré, il est nécessaire de renseigner ce suffixe ici pour que le serveur DNS puisse résoudre ce nom.

Certaines zones nécessitent l'utilisation d'un serveur DNS particulier.

En passant la variable Déclarer des zones DNS à forwarder à oui, il est possible de saisir le nom d'une zone et l'adresse IP de son DNS de forward dans les champs Nom DNS de la zone et Adresse IP du serveur DNS de la zone.

La déclaration de serveurs locaux (Ajouts d'hôtes dans le DNS) ne se fait plus dans l'onglet Zones-dns mais dans l'onglet Réseau avancé.

DNS et RVP

Si le réseau privé virtuel (RVP^[p.559]) est activé et configuré sur le serveur et que le serveur est membre du réseau privé de l'Éducation nationale (AGRIATES^[p.540]), il devient possible de déclarer, dans l'onglet Rvp, le DNS interne à utiliser pour résoudre les noms de domaines.

L'onglet Rvp

Il est possible de renseigner un ou plusieurs serveurs DNS AGRIATES dans le champs Adresse du DNS permettant de résoudre les in.ac-acad.fr. Des relais de zones "AGRIATES" sont prédéfinis et correspondent aux zones *in* du domaine académique. D'autres relais de zone pour le DNS AGRIATES peuvent être ajoutés dans le champs Nom DNS de la zone résolue par le DNS AGRIATES.

La configuration des zones DNS AGRIATES est enregistrée dans le fichier templatisé :

`/etc/bind/agriates.zones.`

4.19. Onglet Ead-web : EAD et proxy inverse

Si l'interface web de l'EAD est activée sur le module (onglet **Services**), les paramètres de l'onglet **Ead-web** permettent de régler le port d'accès à l'interface EAD depuis l'extérieur si un proxy inverse est utilisé.

Par défaut l'utilisation d'un proxy inverse pour accéder à l'EAD est à non.

Si la variable est passée à oui, le port proposé pour accéder à l'EAD depuis l'extérieur est par défaut 4203.

Voir aussi...

Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur [p.259]

4.20. Onglet Messagerie

Même sur les modules ne fournissant aucun service directement lié à la messagerie, il est nécessaire de configurer une passerelle SMTP valide car de nombreux outils sont susceptibles de nécessiter l'envoi de mails.

La plupart des besoins concernent l'envoi d'alertes ou de rapports.

Exemples : rapports de sauvegarde, alertes système, ...

Serveur d'envoi/réception

Les paramètres communs à renseigner sont les suivants :

- Nom de domaine de la messagerie de l'établissement (ex : `monetab.ac-aca.fr`), saisir un nom de domaine valide, par défaut un domaine privé est automatiquement créé avec le préfixe `i-`;
- Adresse électronique recevant les courriers électroniques à destination

du compte `root`, permet de configurer une adresse pour recevoir les éventuels messages envoyés par le système.



Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécrits et envoyés à l'adresse électronique d'envoi du compte `root`.

Cette contrainte permet de faire en sorte que les courriers électroniques utilisant un domaine de type `@<NOM CONTENEUR>.*` soit considéré comme des courriers électroniques systèmes.

En mode normal il est possible de configurer le nom de l'émetteur des messages pour le compte `root`.



Certaines passerelles n'acceptent que des adresses de leur domaine.

Toujours en mode normal d'autres paramètres sont modifiables.

Passer `Gérer la distribution pour les comptes LDAP` à `oui` active les transports LDAP pour la distribution des courriers électroniques, la distribution des courriers locaux est forcée ainsi ils ne sont pas mis en queue et supprimés une semaine plus tard.

Il est également possible de changer la taille des quotas de boîtes aux lettres électroniques qui est fixé par défaut à 20 Mo.

En mode expert il est possible d'écraser l'entêtes des courriers électroniques.

La réécriture des adresses doit prendre en compte la distinction entre l'enveloppe SMTP (« MAIL FROM » et « RCPT TO ») et les en-têtes des messages (« From: », « Reply-To: », « To: », « Cc: », « Bcc: »).

Les adresses électroniques systèmes ont par défaut une des formes suivante :

- `user@%%domaine messagerie etab` si l'expéditeur ne précise pas le nom de domaine, par exemple :

```
root@internet:~# echo "Test" | mail -s "Test mail from shell" -r root root
```

- `user@%%nom machine.%%domaine messagerie etab` pour le maître si l'expéditeur utilise la

configuration définie dans `/etc/mailname`

- `user@%conteneur.%nom_machine.%domaine_messagerie_etab` pour les conteneurs^[p. 543] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

Si la valeur de `%nom_domaine_local` est différente de la valeur de `%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

- `user@%nom_machine.%domaine_messagerie_etab` pour le maître
- `user@%conteneur.%nom_machine.%domaine_messagerie_etab` pour les conteneurs

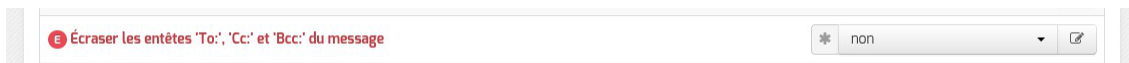
Les adresses destinataires `root@%nom_domaine_local` et `root@%domaine_messagerie_etab` sont remplacées par `%system_mail_to` si cette dernière est définie.

Les adresses expéditeurs et destinataires systèmes sont ensuite réécrites selon les tableaux suivants en fonction de variables expertes :

- `system_mail_from_for_headers` : écraser les en-têtes « From: », « Reply-To: » et « Sender: » du message, par défaut à `non`



- `system_mail_to_for_headers` : écraser les en-têtes « To: », « Cc: » et « Bcc: » du message, par défaut à `non`



Réécriture de l'expéditeur :

	<code>system_mail_from_for_headers = non</code>	<code>system_mail_from_for_headers = oui</code>
MAIL FROM	<code>system_mail_from</code>	<code>system_mail_from</code>
From :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_from</code>
Reply-To :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_from</code>
Sender :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_from</code>

Réécriture du destinataire :

	<code>system_mail_to_for_headers = non</code>	<code>system_mail_to_for_headers = oui</code>
RCPT TO	<code>system_mail_to</code>	<code>system_mail_to</code>
To :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_to</code>
Cc :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_to</code>
Bcc :	<code>user@conteneur.machine.domaine</code>	<code>system_mail_to</code>

Par défaut la distribution des messages se fait en local, ce qui permet d'avoir un domaine local et un domaine privé.

E Gérer la distribution locale

Dans ce cas il est possible d'agir sur le quota des boîtes et sur le pourcentage d'occupation, qui entraîne un message électronique d'avertissement.

E Pourcentage d'utilisation des boîtes entraînant un warning

Relai des messages

Relai des messages

B Router les courriels par une passerelle SMTP

B Passerelle SMTP

La variable `Passerelle SMTP`, permet de saisir l'adresse IP ou le nom DNS de la passerelle SMTP à utiliser.



Afin d'envoyer directement des courriers électroniques sur Internet il est possible de désactiver l'utilisation d'une passerelle en passant `Router les courriels par une passerelle SMTP` à `non`.

Sur les modules possédant un serveur SMTP (Scribe, AmonEcole), ces paramètres sont légèrement différents et des services supplémentaires sont configurables.

N Utilisation du TLS (SSL) par la passerelle SMTP

`Utilisation du TLS (SSL) par la passerelle SMTP` permet d'activer le support du TLS^[p.563] pour l'envoi de message. Si la passerelle SMTP^[p.560] accepte le TLS, il faut choisir le port en fonction du support de la commande STARTTLS^[p.561] (port 25) ou non (port 465).

Par défaut le relai des messages n'est pas activé sur les modules sauf sur le module Seshat. Si la variable est passée à oui, elle active les listes d'adresses IP autorisées à utiliser ce serveur comme relai de messagerie et la liste des noms de domaines autorisés à être relayés par ce serveur.

E Activer le relai des messages

E Activer le TLS pour les clients

E Relayer les courriers électroniques pour des plages d'adresses IPv4

E Relayer les courriers électroniques pour des nom de domaines

Le TLS est activé par défaut pour les clients.

Dans la rubrique Configuration experte plusieurs paramètres peuvent être modifiés.



• FQDN utilisé par Exim

Personnalisation du nom de domaine complètement qualifié utilisé par Exim dans le protocole SMTP. C'est utile pour les vérifications anti-spam des MX externes

Les valeurs possibles sont :

- automatique : laisser Exim décider ;
- nom_machine.domaine_messagerie_etab : utiliser le nom de la machine complété par le nom de domaine de la messagerie établissement ;
- nom_machine.nom_domaine_local : utiliser le nom de la machine complété par le nom de domaine local.

• Domaine utilisé pour qualifier les adresses

Nom de domaine ajouté aux adresses :

- nom de domaine local ;
- domaine privé de messagerie établissement ;
- domaine public de messagerie établissement.

• Envoyer les logs à rsyslog

Permet de désactiver l'envoi des logs.

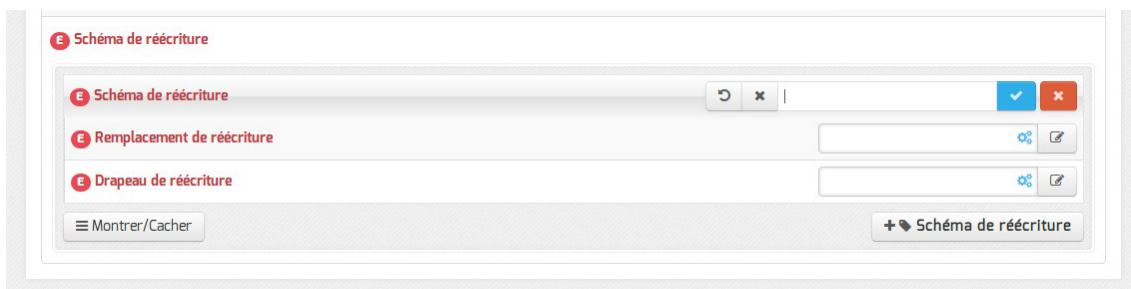
• Dupliquer les logs dans des fichiers

Dupliquer les logs dans des fichiers gérés directement par Exim. Si vous envoyez les logs à syslog, vous pouvez conserver la gestion des fichiers traditionnelle d'Exim. Ces fichiers étant gérés directement par Exim, ils se trouveront dans le conteneur du service.

• Activer les règles de réécriture étendue

Permettre de définir des règles de réécriture personnalisées. Si non, seuls les courriers électroniques en localhost sont réécrits avec le nom_domaine_local.

http://exim.org/exim-html-current/doc/html/spec_html/ch31.html.



Les trois variables à saisir sont :

- Modèle de correspondance des adresses courriers électroniques à réécrire : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID151

- Valeur de remplacement des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID152
- Drapeau contrôlant la réécriture des adresses électroniques : http://exim.org/exim-html-current/doc/html/spec_html/ch31.html#SECID153

4.21. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS

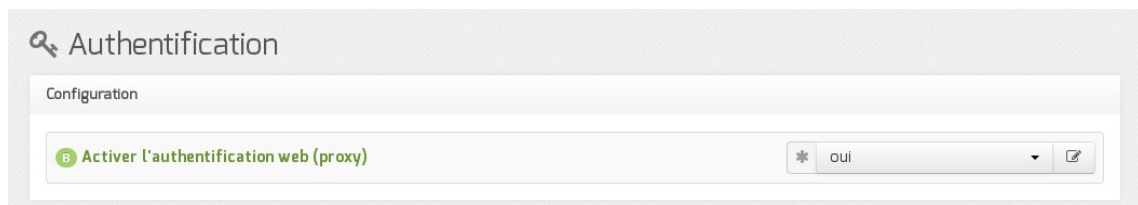
EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet **Authentification** : Activer l'authentification web (proxy).



Cinq méthodes d'authentification sont alors disponibles dans l'onglet **Proxy authentifié**.

Activer une deuxième instance de Squid

Activer une deuxième instance de Squid permet une double authentification, c'est à dire la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Pour profiter de cette fonctionnalité, il faut passer Activer une deuxième instance de Squid à oui.



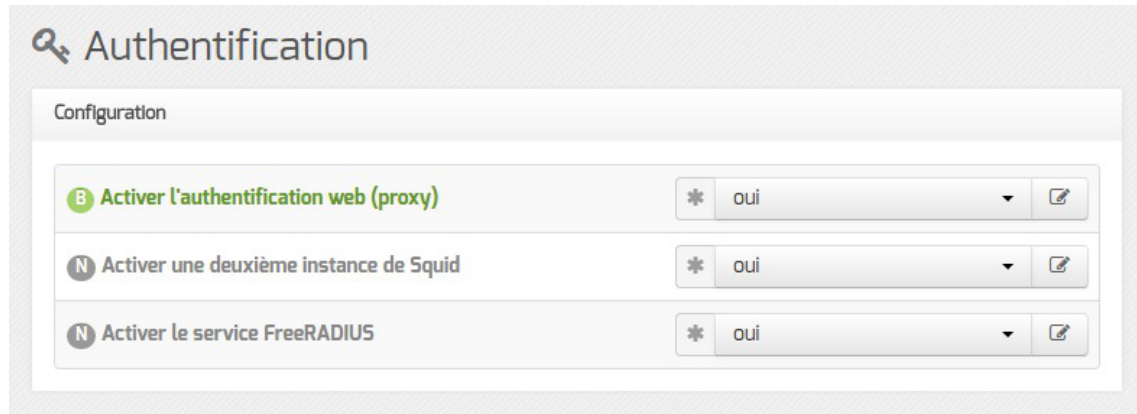
Cela fera apparaître l'onglet **Proxy authentifié 2**.

En mode expert cela fera apparaître également l'onglet **Squid2**.

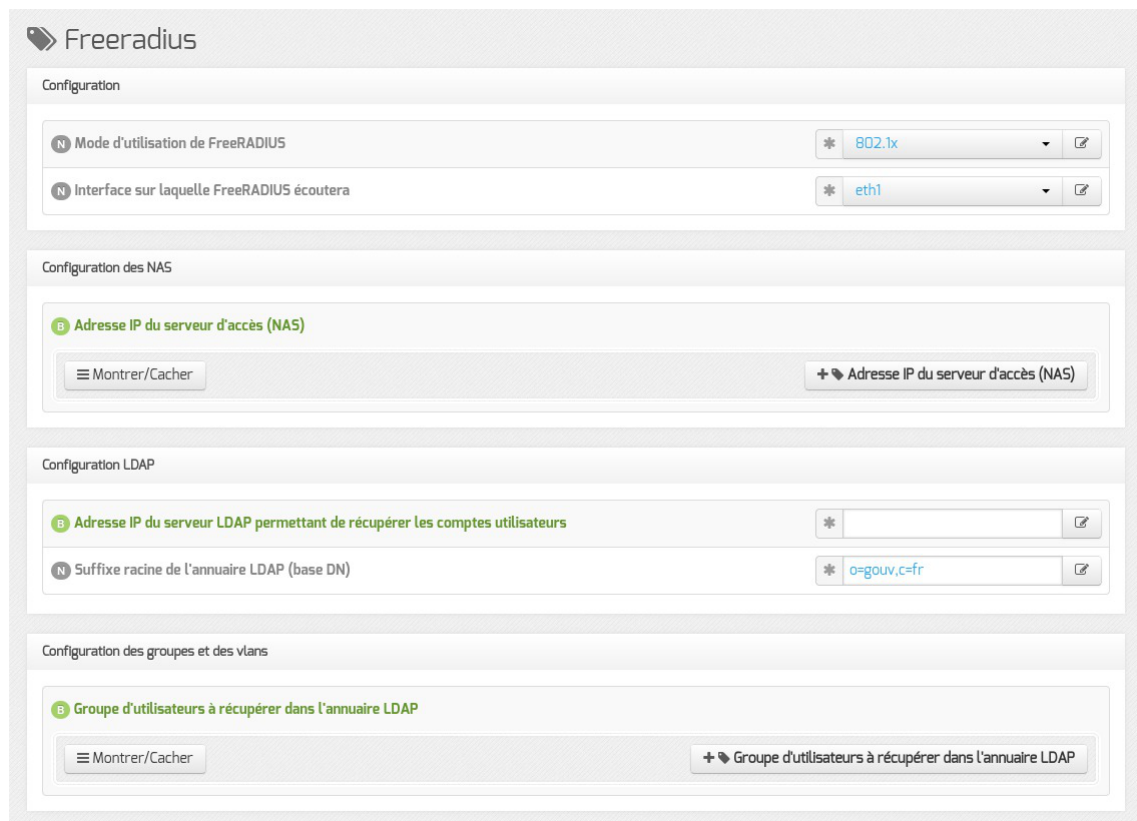
Activer le service FreeRADIUS

EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS^[p.559].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant Activer le service FreeRADIUS à oui.



Cela fera apparaître l'onglet **Freeradius**.



Vue de l'onglet Freeradius de l'interface de configuration du module

Voir aussi...

- ▶ Onglet Proxy authentifié : 5 méthodes d'authentification [p.142]
- ▶ Onglets Squid2 et Proxy authentifié 2 : Double authentification [p.241]
- ▶ Onglet Freeradius : Configuration de l'authentification Radius [p.153]

4.22. Onglet Filtrage web : Configuration du filtrage web

EOLE permet de différencier les zones suivant l'interface (administration ou pédagogie).

La différenciation se fait en modifiant la valeur choisie pour Filtre Web à appliquer à cette interface dans la configuration de l'interface (onglets : **Interface-1** , **Interface-2** , ...).

Les filtres web 1 et 2 correspondent chacun à une instance du logiciel de filtrage.

Le module Amon intègre le logiciel libre e2guardian^[p.545] pour réaliser le filtrage web.

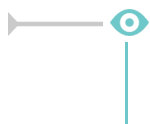
Le paramétrage par défaut de e2guardian convient à un établissement de taille moyenne sans modification particulière.

Il peut être néanmoins intéressant de modifier ce paramétrage pour satisfaire les besoins de l'établissement (notamment dans le cas où le serveur ne peut plus répondre aux requêtes, la fenêtre d'authentification apparaît de façon intempestive, ...).

Sur un petit établissement, il sera possible d'économiser des ressources.

Sur un gros établissement, il pourra répondre à un plus grand nombre de requêtes.

Un certain nombre de paramétrages sont proposés pour contrôler les ressources de e2guardian.



Il est possible d'affecter une politique spécifique aux machines du foyer (politique plus laxiste) et une autre aux machines du CDI (politique moins permissive).

Politiques de filtrage optionnelles

Une politique de filtrage correspond à un ensemble d'autorisations ou interdictions d'accès à des sites, suivant différents critères.

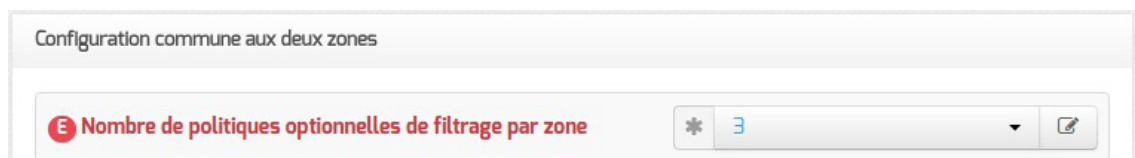
Il existe par défaut 4 politiques obligatoires :

- une politique de filtrage par défaut ;
- une politique « modérateur » (permet d'outrepasser les interdictions) ;
- une politique « interdits » (permet d'interdire toute navigation) ;
- une politique « liste blanche » (navigation limitée aux sites de cette même liste).

Seule la politique de filtrage par défaut est modifiable via l'EAD.

En plus de ces politiques, il est possible d'ajouter de 1 à 4 autres politiques de filtrage optionnelles (il y en a 3 par défaut).

Ces politiques de filtrage optionnelles seront alors paramétrables dans l'EAD.



Pour modifier le nombre de politiques de filtrage par zone, il faut utiliser le paramètre :

Nombre de politiques optionnelles de filtrage par zone.

La valeur 0 revient à n'utiliser que les 4 politiques par défaut proposées ci-dessus.

L'ajout de politiques optionnelles (valeur 1,2,3,4) permet d'ajouter des filtres supplémentaires, associables à des groupes de machines ou des comptes utilisateur.



Plus vous définissez de politiques, plus e2guardian utilisera de ressources.
Adaptez le nombre de politiques activées en fonction de vos besoins.

L'observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian^[p.545].



La question Autoriser la consultation des logs liés au filtrage web dans l'EAD propose plusieurs options :

- oui : accès autorisé pour les utilisateurs EAD possédant les actions navigation visit admin et/ou navigation visit pedago ;
- non : accès interdit pour tout le monde, personne ne voit le lien Visites des sites (configuration par défaut) ;
- admin seulement : accès autorisé uniquement pour le rôle admin.



La consultation des visites de sites se fait au travers de l'EAD, menu : Filtre web X/visites des sites.

Paramétrage de e2guardian

Le logiciel e2guardian offre de nombreuses options de configuration.

Plusieurs sont paramétrables dans l'interface de configuration du module.

Seule l'expérience «à tâtons»^[p.551] permet de définir les valeurs adéquates à votre installation.

L'objectif est d'utiliser le plus de mémoire possible sans que le serveur n'utilise la partition d'échange (swap^[p.562]).



La commande top en console permet d'observer l'évolution de l'utilisation de la partition d'échange de façon dynamique.

Les options de configuration proposées dans la première partie de l'interface de configuration sont communes aux deux zones configurables :

Filtrage web

Configuration commune aux deux zones

E Nombre de politiques optionnelles de filtrage par zone	*	3	
E Proxy Timeout (ex: Doc Body Timeout)	*	20	
E Proxy header exchange (ex: Doc Header Timeout)	*	20	
E Pconn timeout (ex: Header Timeout)	*	55	
E Autoriser la consultation des logs liés au filtrage web dans l'EAD	*	non	

Proxy Timeout (ex: Doc Body Timeout)

Délai d'attente TCP entre le proxy et e2guardian (en secondes).

Proxy header exchange (ex: Doc Header Timeout)

Délai d'attente entre le proxy et e2guardian (en secondes).

Pconn timeout (ex: Header Timeout)

Délai pendant lequel une connexion persistante attend de nouvelles requêtes (en secondes).

Les options de configuration proposées dans les sections suivantes permettent de personnaliser la configuration de chacune des zones configurables.

Filtre web 1

E Libellé du filtre web 1 dans l'EAD	*	Filtre web 1	
E Nombre maximum de processus	*	256	
E Nombre minimum de processus	*	8	
E Nombre minimum de processus en attente	*	4	
E Nombre maximum de processus en attente	*	32	
E Nombre de processus démarré s'il en manque	*	6	
E Durée de vie maximum d'un processus avant de se terminer	*	500	
E Répertoire de cache	*	/tmp	
E Taille maximum de fichier conservé en mémoire	*	5000	
E Taille maximum de fichier conservé sur le disque	*	5000	

Nombre maximum de processus

Nombre maximum de processus disponibles pour traiter les nouvelles connexions (paramètre maxchildren).

Sa valeur par défaut est fixée à 256. Elle peut être modifiée en respectant les contraintes suivantes :

- sa valeur minimum est de 80 ;
- sa valeur maximum théorique est de 8192 mais, dans les faits, elle est proche de 8192 moins deux fois la valeur du paramètre `preforkchildren` (Nombre de processus démarré s'il en manque) qui est de 6 par défaut.



Si la valeur maximum est dépassée, le service refusera de démarrer.

Nombre minimum de processus

Le nombre de processus minimal pour traiter les nouvelles connexions.

Nombre minimum de processus en attente

Le nombre minimum de processus prêts à recevoir de nouvelles connexions.

Nombre maximum de processus en attente

Le nombre maximum de processus attendant de nouvelles connexions.

Nombre de processus démarré s'il en manque

Le nombre minimum de processus disponibles lorsqu'ils viennent à manquer.

Durée de vie maximum d'un processus avant de se terminer

Les processus enfant, comme tout processus, peuvent succomber à des variables parasites. Ce paramètre définit l'âge maximal de connexions qu'un processus enfant traite avant de quitter. La valeur par défaut est de traiter 500 demandes de connexion avant de quitter.

Augmenter ce paramètre peut aider à soulager les problèmes de performance liés à la rotation des processus, mais peut créer un problème de performance si un processus s'emballe pour une raison quelconque.

Sur les grands sites vous pourriez vouloir essayer de passer cette valeur à 10000.

Répertoire de cache

Permet de choisir le chemin du répertoire de cache, par défaut `/tmp`.

La taille maximum de fichier conservé en mémoire

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

C'est la taille maximale des fichiers en kibibytes^[p.558] que e2guardian va télécharger et mettre en cache dans la RAM. Après que cette limite soit atteinte, e2guardian met en cache sur le disque.

Cette valeur doit être inférieure ou égale à la valeur de La taille maximum de fichier conservé sur le disque.

Utiliser la valeur 0 permet de définir le même réglage que La taille maximum de fichier conservé sur le disque.

La taille maximum de fichier conservé sur le disque

Cette variable n'est utilisée que si vous utilisez un greffon d'anti-virus.

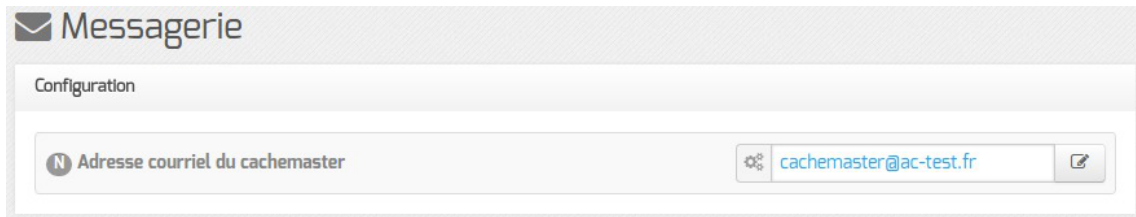
C'est la taille maximale des fichiers en kibibytes^[p.558] que e2guardian va télécharger de sorte qu'ils soient vérifiés par l'anti-virus.

Cette valeur doit être supérieure ou égale à La taille maximum de fichier conservé en mémoire.

Adresse électronique à utiliser en cas de réclamation

Lorsque la consultation d'une page est refusée à l'utilisateur, une page d'erreur affichant les détails de l'interdiction apparaît.

Celle-ci propose également une adresse électronique à utiliser pour signaler les interdictions injustifiées.



Cette adresse se configure par l'intermédiaire de la variable Adresse courriel du cachemaster disponible dans l'onglet Messagerie.

Désactivation du filtrage web

Dans certaines configurations (utilisation d'un proxy académique, ...), il peut s'avérer utile de désactiver complètement le filtrage web.



Cela est possible en allant dans l'interface de configuration du module en mode expert et en répondant non à la question de l'onglet Services, Activer le filtrage sur le proxy.

⚠ Dans cette configuration, le proxy Squid écoute sur le **port 3128** en lieu et place du logiciel de filtrage e2guardian.

Voir aussi...

Observatoire des navigations ^[p.376]

4.23. Onglet Squid : Configuration du proxy

Le service proxy Squid n'étant pas désactivable, l'onglet Squid est toujours accessible en mode expert. L'onglet expert Squid permet de modifier et de fixer une sélection des principaux paramètres du fichier de configuration : /etc/squid3/squid.conf.

Les paramètres de ce fichier de configuration se retrouvent explicitement dans le nom des variables Creole (mode Debug de l'interface de configuration du module).

The screenshot shows the Squid configuration interface with the following settings:

- Générer les statistiques Squid automatiquement**: * non
- Port d'écoute du CGI LightSquid**: * 8062
- Méthode d'anonymisation des rapports LightSquid**: * aucune
- Port d'écoute HTTPS de Squid**: (empty field)
- "SSL_ports" supplémentaire**: Pas de valeur
- "Safe_ports" supplémentaire**: Pas de valeur
- Nombre de processus associés au module d'authentification basique**: * 20
- Nombre de processus associés au module d'authentification NTLM**: * 20

Paramétrer l'analyse de logs LightSquid

Les options Générer les statistiques Squid automatiquement, Port d'écoute du CGI LightSquid et Méthode d'anonymisation des rapports LightSquid servent à configurer l'outil d'analyse de logs LightSquid permettant d'afficher sous forme de pages web l'utilisation du proxy. Sa configuration fait l'objet d'une section dédiée.

Paramétrer les ports de Squid

Ports d'écoute

Si le filtrage web est activé, le service Squid écoute sur le port 8080 de la boucle locale.

Si le filtrage web est désactivé, le service Squid écoute sur le port par défaut de e2guardian : 3128.

Il est possible de paramétrer Squid pour qu'il écoute les requêtes HTTPS des clients.

Ceci est particulièrement utile dans les situations où Squid est utilisé comme accélérateur des requêtes.

Il faut alors saisir le numéro de port choisi dans le champ Port d'écoute HTTPS de Squid.

SSL_ports

Par défaut, seuls les ports de destination (sortants) des connexions SSL 443, 563, 631, 4000-5000, 6080, 8062, 8070, 8090, 8443, 8753 et 7070 sont autorisés.

Il est possible d'en ajouter autant que souhaité dans le champ "SSL_ports" supplémentaire.

Safe_ports

De même, seuls les ports de destination (sortants) non SSL 80, 21, 443, 563, 70, 210, 631 et 1025-65535 sont autorisés.

Il est possible d'en ajouter autant que souhaité dans le champ "Safe_ports" supplémentaire.

Personnaliser la durée des caches

L'option Personnaliser sélectivement la durée des caches, présente à partir de la version 2.5.2 d'EOLE, permet de personnaliser l'algorithme de gestion du rafraîchissement du cache par

site.

La gestion du cache de Squid peut ne pas correspondre à tous les sites. Par exemple, pour les sites antiviraux, il vaut mieux augmenter la durée de conservation du cache des fichiers téléchargés par les postes clients.

Voici un exemple la configuration à mettre en place pour conserver en cache les signatures de l'anti-virus Trend :



L'expression rationnelle décrit la chaîne de caractères et les règles qui permettent de construire l'URL :

- ^ marque le début d'une chaîne ;
- \$ marque la fin d'une chaîne ;
- | marque l'alternative ;
- . indique n'importe quel caractère ;
- * aucune, une ou plusieurs occurrences du caractère.

Les variables qui permettent de régler le comportement du cache de Squid sont :

- Temps maximum de cache ;
- Rapport entre l'âge de l'objet dans le cache et son âge sur le site ;
- Temps minimum de cache.



Cette configuration générera la ligne de configuration suivante :

- `refresh_pattern -i <url regexp> "Temps maximum de cache" "Rapport entre l'âge de l'objet dans le cache et son âge sur le site" "Temps minimum de cache" <options>`
- `refresh_pattern -i /*.*\trendmicro\.com/.* 180 100% 300 reload-into-ims ignore-reload`

L'option `-i` permet de ne pas tenir compte de la casse des caractères dans l'expression régulière.



La personnalisation sélective de la durée du cache est basée sur la directive `refresh_pattern` de Squid. Cette directive permet un contrôle très fin de la validité des objets mis en cache.

Lors d'une requête, Squid décide du comportement à adopter en fonction de l'état de l'objet dans son cache :

- si l'objet n'est pas dans le cache, Squid le demande au serveur qui héberge l'objet, le met en cache et le fournit au client ;
- si l'objet est dans le cache et qu'il est considéré comme étant encore à jour, Squid le fournit directement au client ;
- s'il n'est plus considéré comme à jour, alors une requête `If-modified-since` est envoyée au serveur qui héberge l'objet.

Pour déterminer si un objet est à jour, Squid utilise plusieurs paramètres :

- la valeur liée à l'objet enregistré :
 - **age** correspond au temps en seconde écoulé depuis l'entrée de l'objet dans le cache (`objet_age = maintenant - objet_date`)
 - **Im_age** correspond à l'âge de l'objet au moment de l'entrée dans le cache, temps, en secondes, écoulé entre la dernière modification de l'objet sur le serveur hébergeur et son entrée dans le cache. (`Im_age = objet_date - objet_lastmod`)
 - **expires** est la date d'expiration de l'objet éventuellement fournie par le serveur hébergeur au moment de l'entrée de l'objet dans le cache. Si elle est renseignée, la valeur de `Temps minimum de cache` prend le pas sur cette valeur.
- la valeur fournie par le client ;

Squid tient compte de la variable **client_max_age** éventuellement fournie par le client, elle indique l'âge maximal de l'objet accepté par le client. Si cette valeur est fournie par le client elle prend le pas sur la valeur `Temps maximum de cache` du fichier de configuration de Squid.

- les valeurs du fichier de configuration de Squid :
 - temps écoulé depuis le téléchargement (**age**), temps maximum et minimum de cache :
 - si `Temps maximum de cache` est défini et que le temps écoulé depuis le téléchargement est supérieur, l'objet est périmé et devra être mis à jour ;
 - si le temps écoulé depuis le téléchargement est inférieur ou égal au `Temps minimum de cache`, l'objet est considéré comme étant à jour.
 - date d'expiration de l'objet fournie par le serveur hébergeur :
 - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur et qu'elle est dépassée, l'objet est périmé et devra être mis à jour ;
 - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur mais qu'elle n'est pas encore dépassée, l'objet est considéré comme étant à jour.
 - rapport (**Im_factor**) entre le temps, en secondes, écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache :

Plus le score du rapport entre le temps écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache (**age/Im_age**) est élevé plus l'objet risque

d'être périmé :

- peu de temps écoulé (10) / objet vieux (1000) = rapport faible (0.01) → objet probablement à jour
- beaucoup de temps écoulé (1000) / objet vieux (1000) = rapport élevé (1) → objet probablement périmé
- peu de temps écoulé (10) / objet jeune (10) = rapport élevé (1) → objet probablement périmé
- beaucoup de temps écoulé (1000) / objet jeune (10) = ce cas de figure n'arrive pas car géré par des règles en amont.

Si le rapport est inférieur au pourcentage (**percent**) saisi dans Rapport entre l'âge de l'objet dans le cache et son âge sur le site, l'objet est considéré comme à jour. Diminuer la valeur du pourcentage diminue la probabilité (rapport faible) qu'un objet soit périmé.

Enfin, si aucune règle n'aboutit à considérer l'objet comme étant à jour, celui-ci est considéré comme périmé et devra être mis à jour.

Augmenter le nombre de redirections

Certains sites ont besoin de faire un grand nombre de redirections avant de fournir le contenu souhaité à l'utilisateur.

Par défaut, Squid n'accepte que 10 redirections (variable forward_max_tries du fichier de configuration de Squid) ce qui peut entraîner l'abandon des redirections et donc bloquer l'accès au site.

Il est possible à partir de la version 2.5.2 d'EOLE d'augmenter cette valeur en modifiant la variable Nombre maximum de redirections testées de l'onglet.

Paramètre Half_closed_clients

Certains clients peuvent arrêter leur connexion TCP d'envoi tout en laissant leur connexion de réception ouverte. Parfois, Squid ne peut pas faire la différence entre une connexion à demi-fermée et une connexion entièrement fermée :

- si le paramètre Half closed clients est à On, les connexions demi-fermée sont maintenues ouvertes jusqu'à ce qu'une erreur de lecture ou d'écriture apparaisse ;
- si le paramètre Half closed clients est à Off, les connexions sont fermées dès qu'il n'y a plus de données à lire (valeur recommandée sur Squid >= 3.0).

Historiquement paramétrée à On sur les modules EOLE, sa valeur par défaut a été passée à Off sur les versions d'EOLE >= 2.5.1 depuis avril 2016.

Autres paramètres

L'onglet expert Squid permet de modifier et de fixer un nombre conséquent de paramètres optionnels du fichier de configuration : `/etc/squid3/squid.conf`.

Pour plus d'informations sur la modification de ces paramètres, vous pouvez consulter :

- les exemples de configuration dans le fichier de documentation de Squid :

`/usr/share/doc/squid3-common/squid.conf.documented.gz`

- la documentation en ligne des différents paramètres : <http://www.squid-cache.org/Doc/config/>

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.226]

Outil d'analyse de logs LightSquid [p.377]

4.24. Onglet Proxy authentifié : 5 méthodes d'authentification

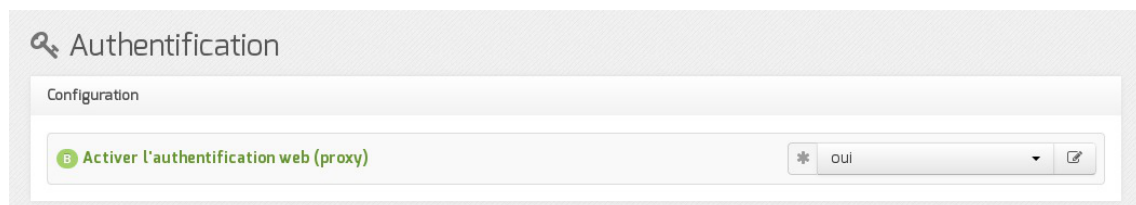
EOLE propose un mécanisme d'authentification web via un proxy.

Tous les accès web (HTTP et HTTPS) nécessiteront alors une phase d'authentification.

Cette fonctionnalité offre deux avantages :

- il sera possible de savoir quel utilisateur a accédé à une ressource particulière ;
- il sera possible d'appliquer des politiques de filtrage pour chaque utilisateur.

Pour profiter de cette fonctionnalité, il faut activer l'authentification du proxy dans l'onglet **Authentification** : Activer l'authentification web (proxy).



Cinq méthodes d'authentification sont alors disponibles dans l'onglet **Proxy authentifié**.

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba.



Il est possible de configurer plusieurs contrôleurs de domaine dans le cadre de l'authentification NTLM/SMB.

C'est la configuration à choisir si vous disposez d'un serveur pédagogique Scribe et/ou d'un serveur administratif Horus.

La syntaxe pour utiliser le proxy authentifié avec une machine hors domaine est `domaine\login` mais elle ne fonctionne pas avec toutes les versions de navigateurs.

L'authentification NTLM/SMB nécessite l'application de la clé de registre suivante sur les clients Windows Vista et Windows Seven :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
```

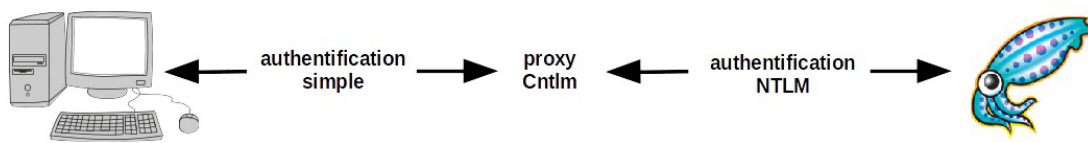
```
"LMCompatibilityLevel"=dword:00000001
```

Pour plus d'informations, consulter : <http://technet.microsoft.com/en-us/library/cc960646>

Authentification NTLM/SMB poste hors domaine

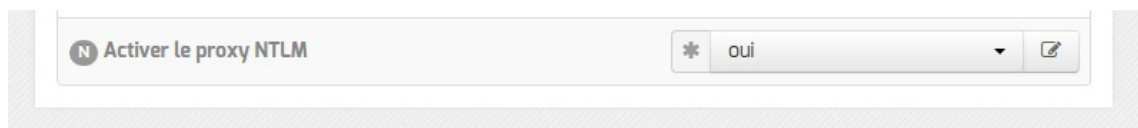
En mode normal, l'authentification NTLM^[p.555] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm^[p.543].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.



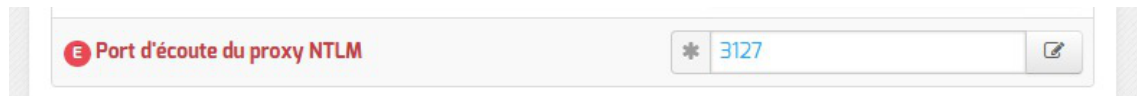
Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert. Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

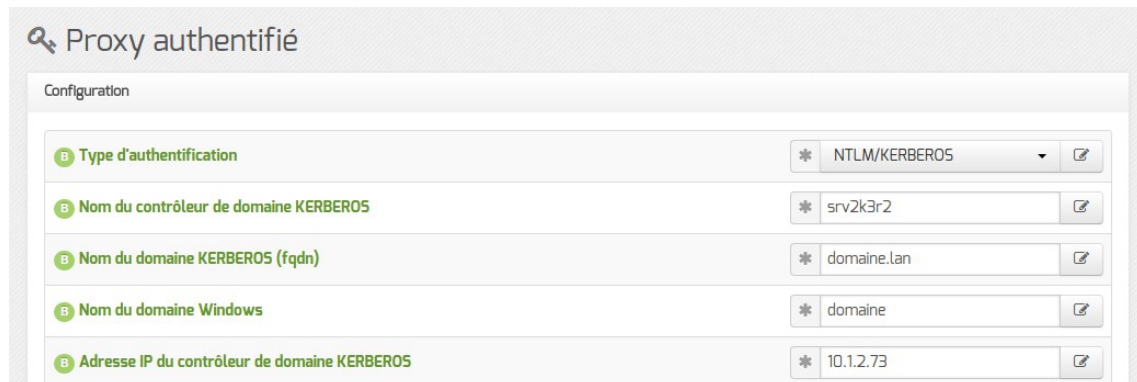
C'est le premier domaine spécifié qui sera utilisé par Cntlm.

En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.



Une fois activé, le choix peut être fait de désactiver le proxy NTLM sur une interface donnée, pour cela il faut se rendre en mode expert dans l'onglet de l'interface à paramétrer.

Authentification NTLM/KERBEROS



Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory.

Cette méthode d'authentification nécessite l'intégration du serveur au royaume Kerberos.

L'intégration peut être réalisée lors de l'instanciation du module en répondant **oui** à la question suivante :

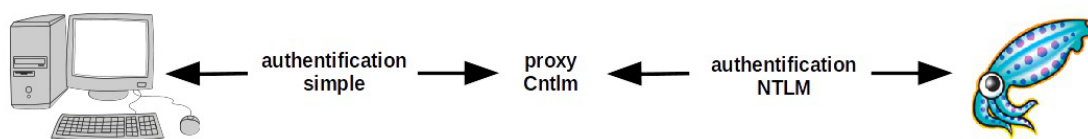
Voulez-vous (ré)intégrer le serveur au domaine maintenant ?

Si la configuration de l'authentification NTLM/KERBEROS est réalisée après l'instanciation, il est possible de relancer l'intégration du serveur à tout moment à l'aide du script `enregistrement_domaine.sh`.

Authentification NTLM/KERBEROS poste hors domaine

En mode normal, l'authentification NTLM^[p.555] peut être facilitée par l'utilisation d'un proxy. Le proxy NTLM proposé par EOLE utilise le logiciel libre Cntlm^[p.543].

Le proxy NTLM Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.



Cette méthode permet d'utiliser l'authentification NTLM sur des machines qui ne savent pas le gérer. Ce qui est le cas des machines hors domaine.

Pour activer le proxy NTLM Cntlm il faut passer la variable `Activer le proxy NTLM` à `oui`.

The screenshot shows a configuration field with a red 'N' icon on the left. The text 'Activer le proxy NTLM' is displayed. To the right, there is a dropdown menu with an asterisk icon and the value 'oui' selected. A small edit icon is visible on the far right.

Le port utilisé par défaut par Cntlm est `3127`, il est modifiable en mode expert.

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Les postes intégrés au domaine doivent donc utiliser le port `3128` pour passer par le proxy et les postes nomades (hors domaine) doivent utiliser le port `3127` pour passer par Cntlm.

Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm (`3127` par défaut).

En mode expert il est possible de changer le port d'écoute par défaut du proxy NTLM.

The screenshot shows a configuration field with a red 'E' icon on the left. The text 'Port d'écoute du proxy NTLM' is displayed. To the right, there is a text input field containing the value '3127' and an asterisk icon. A small edit icon is visible on the far right.

Une fois activé, le choix peut être fait de désactiver le proxy NTLM sur une interface donnée, pour cela il faut se rendre en mode expert dans l'onglet de l'interface à paramétrer.

Authentification LDAP

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type OpenLDAP.

The screenshot shows a configuration window titled 'Proxy authentifié'. Under the 'Configuration' section, there are three fields:

- 'Type d'authentification' with a dropdown menu set to 'Ldap' and an asterisk icon.
- 'Adresse du premier serveur LDAP' with a text input field containing '10.1.1.10' and an asterisk icon.
- 'Suffixe racine de l'annuaire LDAP (base DN)' with a text input field containing 'o=gouv,c=fr' and an asterisk icon.

Ce type d'authentification est recommandé pour les postes hors domaine.

En mode normal, il est possible de déclarer un annuaire de secours.

The screenshot shows a configuration field with a red 'N' icon on the left. The text 'Adresse du second serveur LDAP (si le 1er ne répond pas)' is displayed. To the right, there is an empty text input field and a small edit icon on the far right.

Cet annuaire est interrogé uniquement si le premier ne répond pas.

Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

Authentification LDAP (Active Directory)

The screenshot shows the 'Proxy authentifié' configuration window. Under the 'Configuration' tab, the 'Type d'authentification' is set to 'Ldap (Active Directory)'. Other fields include: 'Adresse IP du serveur LDAP (Active Directory)' set to '10.1.2.73', 'Suffixe racine de l'annuaire LDAP (base DN Active Directory)' set to 'DC=domaine,DC=lan', 'Nom du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'Administrateur', and 'Mot de passe du compte nécessaire pour l'interrogation LDAP (Active Directory)' set to 'P@sswOrd'.

Il s'agit d'une authentification non transparente s'appuyant sur un annuaire de type Active Directory. Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification sur Fichier local

The screenshot shows the 'Proxy authentifié' configuration window. Under the 'Configuration' tab, the 'Type d'authentification' is set to 'Fichier local'.

Il s'agit d'une authentification non transparente s'appuyant sur un fichier de comptes locaux. Ce type d'authentification peut être utilisé dans une petite structure, comme une école, qui ne disposerait pas vraiment d'un réseau local.

Pour cette authentification, le fichier utilisé par défaut est : `/etc/squid3/users`

Il doit être au format `htpasswd` et il peut être peuplé en utilisant la commande suivante :

```
# htpasswd -c /etc/squid3/users <compte>
```

⚠ En mode conteneur (module AmonEcole par exemple), le fichier `/etc/squid3/users` se trouve dans le conteneur `proxy` :

```
# ssh proxy
```

```
# htpasswd -c /etc/squid3/users <compte>
```

ou

```
# CreoleRun "htpasswd -c /etc/squid3/users <compte>" proxy
```

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors `eth0` si plusieurs interfaces sont configurées), il est possible d'activer/désactiver l'authentification proxy.

Par exemple, pour désactiver l'authentification proxy uniquement sur le réseau `eth2`, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette`

interface (s'applique aussi aux VLAN).

4.25. Onglets Squid2 et Proxy authentifié 2 : Double authentification

Par double authentification, nous entendons la possibilité de pouvoir configurer deux types distincts d'authentification proxy.

Par exemple, pouvoir utiliser à la fois une authentification NTLM/SMB et une authentification LDAP.

L'implémentation retenue est d'utiliser une instance du logiciel Squid par type d'authentification.

Configuration pas à pas

1. Activation de la deuxième instance de Squid dans l'onglet **Authentification** :

The screenshot shows a configuration field for 'Activer une deuxième instance de Squid'. The field is a dropdown menu with a star icon on the left and a pencil icon on the right. The selected value is 'oui'.

2. Configuration du type d'authentification dans l'onglet **Proxy authentifié 2** :

The screenshot shows the 'Proxy authentifié 2' configuration page. It has a search icon and the title 'Proxy authentifié 2'. Below the title is a 'Configuration' section with four rows of settings:

- 'Type d'authentification': dropdown menu set to 'Ldap'.
- 'Adresse du premier serveur LDAP': text input field containing '10.21.11.5'.
- 'Adresse du second serveur LDAP (si le 1er ne répond pas)': empty text input field.
- 'Suffixe racine de l'annuaire LDAP (base DN)': text input field containing 'o=gouv,c=fr'.

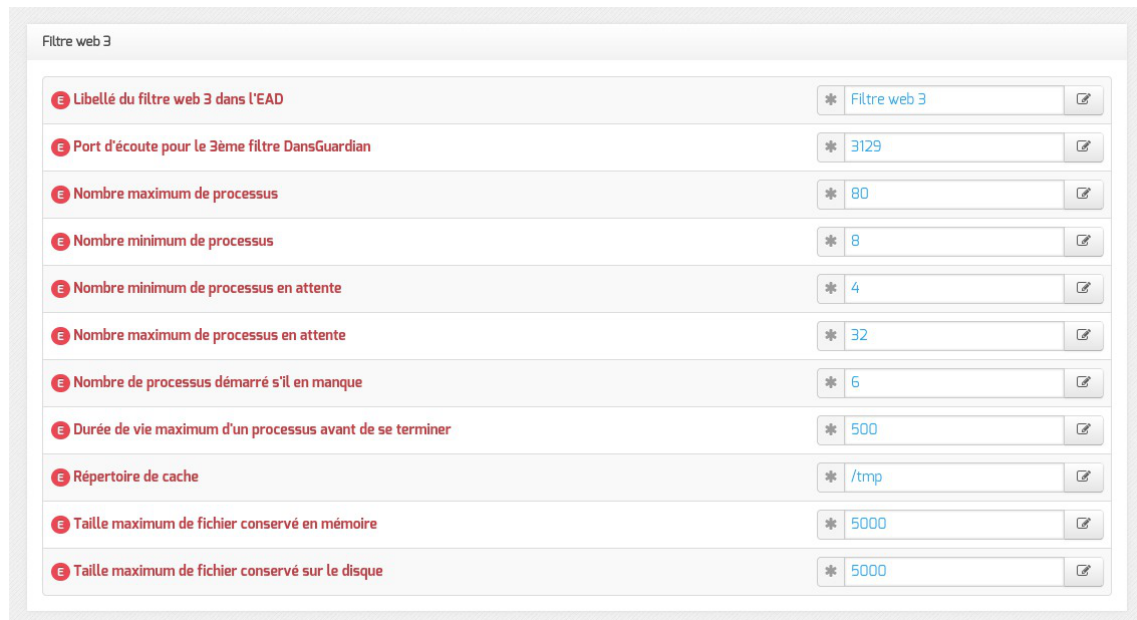
3. Paramétrage de la seconde instance de Squid dans l'onglet expert **Squid2** :

The screenshot shows the 'Squid2' expert configuration page. It has a search icon and the title 'Squid2'. Below the title is a 'Configuration' section with five rows of settings, all marked with a red error icon:

- 'Emplacement du cache': text input field containing '/var/spool/squid2'.
- 'Type de stockage utilisé': dropdown menu set to 'ufs'.
- 'Taille du cache (en MBytes)': text input field containing '1000'.
- 'Nombre maximum de répertoires de niveau 1': text input field containing '16'.
- 'Nombre maximum de répertoires de niveau 2': text input field containing '256'.

At the bottom left is a 'Montrer/Cacher' button, and at the bottom right is a '+ Emplacement du cache' button.

4. Paramétrage du filtrage web associé dans l'onglet expert **Filtrage web** (section Filtre web 3)



Notes techniques

Les fichiers de logs spécifiques au second type d'authentifications sont les suivants :

- `/var/log/rsyslog/local/squid/squid2.info.log`
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log`

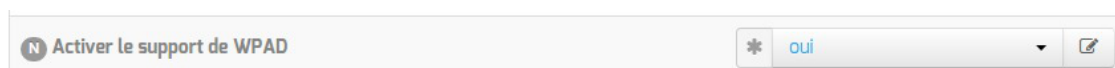
Dans l'état actuel, ces logs ne sont pas consultables au travers de l'interface EAD et seule la première configuration proxy est distribuée par WPAD (voir partie dédiée).

4.26. Onglet Wpad : découverte automatique du proxy

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

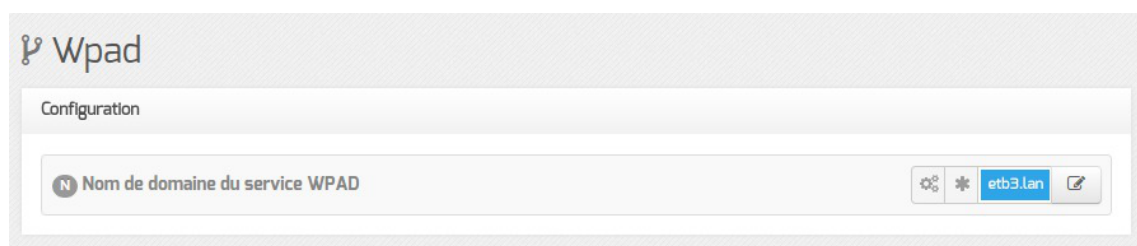
Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` corresponde à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet **Services** de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet **Wpad** au sein duquel le **Nom de domaine du service WPAD** doit être rempli avec la même valeur que le **Nom de domaine privé du réseau local** présent dans l'onglet **Général**.

⚠ Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au **Nom de domaine privé du réseau local** de l'onglet **Général**, il faut le déclarer dans le champ **Nom domaine local supplémentaire ou rien** de l'onglet **Zones-dns**.

⚠ Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande **reconfigure** sur le module.

💡 WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.
En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.267]

4.27. Onglet Exceptions proxy

Dans l'onglet **Exceptions proxy** de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton **Exceptions de type réseau pour eth-n** permet d'ajouter plusieurs exceptions sur une même

interface.

Exception sur un nom de domaine

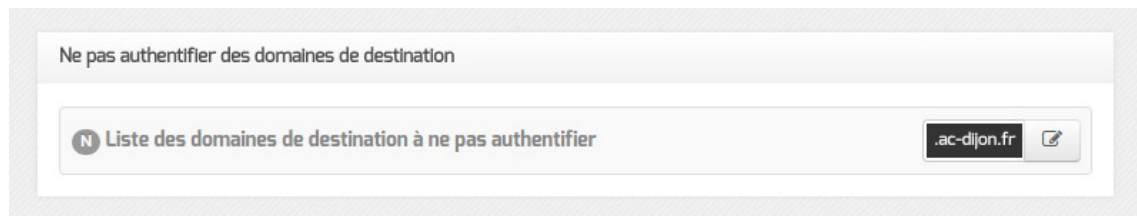
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour laquelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.

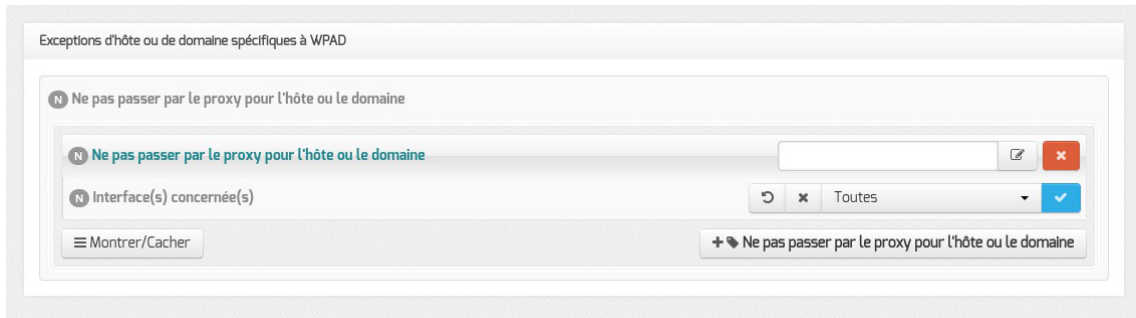
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton **+ Ne pas passer par le proxy pour l'hôte ou le domaine** permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.



Si le champ **Ne pas passer par le proxy pour l'hôte ou le domaine** a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.



Compléments sur **Ne pas passer par le proxy pour le domaine** (dnsDomainIs) :

<http://findproxyforurl.com/netscape-documentation/#dnsDomainIs>

Compléments sur **Ne pas passer par le proxy pour l'hôte ou le domaine** (localHostOrDomainIs) :

<http://findproxyforurl.com/netscape-documentation/#localHostOrDomainIs>

4.28. Onglet Proxy parent : Chaînage du proxy

L'onglet expert **Proxy parent** permet de déclarer un ou plusieurs serveurs proxy à utiliser en amont de celui activé sur le module EOLE.

Cette fonctionnalité est à utiliser dans le cas de la mise en place d'un proxy centralisé au niveau d'une académie ou d'un groupe d'établissements.

Proxy parent

Proxy parent global

E Utiliser un proxy web parent global * non

Proxy parent par zone

E Utiliser un proxy web parent par zone * non

Coopération des caches

E Activer la coopération des cache * non

Si plusieurs proxy parents sont déclarés, un mécanisme de type round-robin^[p.560] est utilisé afin de répartir la charge sur les différents serveurs.



Les proxy déclarés ici ne seront pas utilisés par le serveur lui-même.

La déclaration d'un proxy à utiliser par le module EOLE s'effectue dans l'onglet **Général** en passant la variable : Utiliser un serveur mandataire (proxy) pour accéder à Internet à oui.

Proxy parent global

Le ou les proxy parents peuvent être déclarés de façon globale en passant la variable Utiliser un proxy web parent global à oui.

Proxy parent global

E Utiliser un proxy web parent global * oui

E Adresse du proxy web parent

E Adresse du proxy web parent * proxy.ac-test.fr

E Port du serveur proxy web parent * 3128

E Port ICP du serveur proxy web parent * 3130

E Option du proxy web parent * no-query

Montrer/Cacher

+ Adresse du proxy web parent

Proxy parent par zone

Pour des besoins spécifiques, des proxy parents peuvent être déclarés pour des zones DNS particulières en passant la variable Utiliser un proxy web parent par zone à oui.

Les zones DNS de destination peuvent être :

- soit renseignées directement dans la variable Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent si la Méthode d'utilisation de la zone accessible via ce serveur web parent est DNS;
- soit renseignées dans un fichier texte dont le chemin est à indiquer dans la variable Nom DNS ou nom de fichier de la zone accessible via ce serveur web parent si la Méthode d'utilisation de la zone accessible via ce serveur web parent est nom fichier;



Pour que ces sous-domaines soient également pris en compte, le nom DNS du domaine doit impérativement être précédé d'un point.

Il est possible de renseigner directement plusieurs zones DNS en les séparant par des espaces, exemple : .domain1 .domain2 .domain3.

Coopération des caches

Si on a plusieurs proxy cache, il peut être intéressant de les faire collaborer pour partager le cache. Cela se fait via le mécanisme de proxy sibling^[p.558].

4.29. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx^[p.555].

Le proxy inverse est un type de serveur proxy, habituellement placé en frontal de serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes (situés en DMZ^[p.545] par exemple). Cela le différencie grandement d'un proxy classique comme Squid^[p.561].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situés "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables*^[p.550]/*DNAT*.

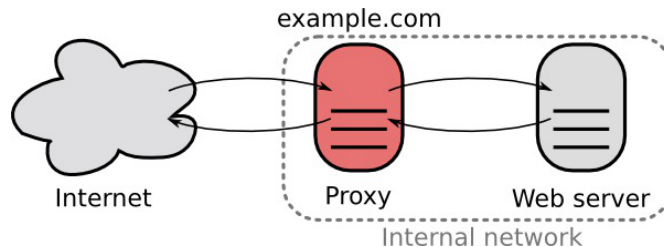
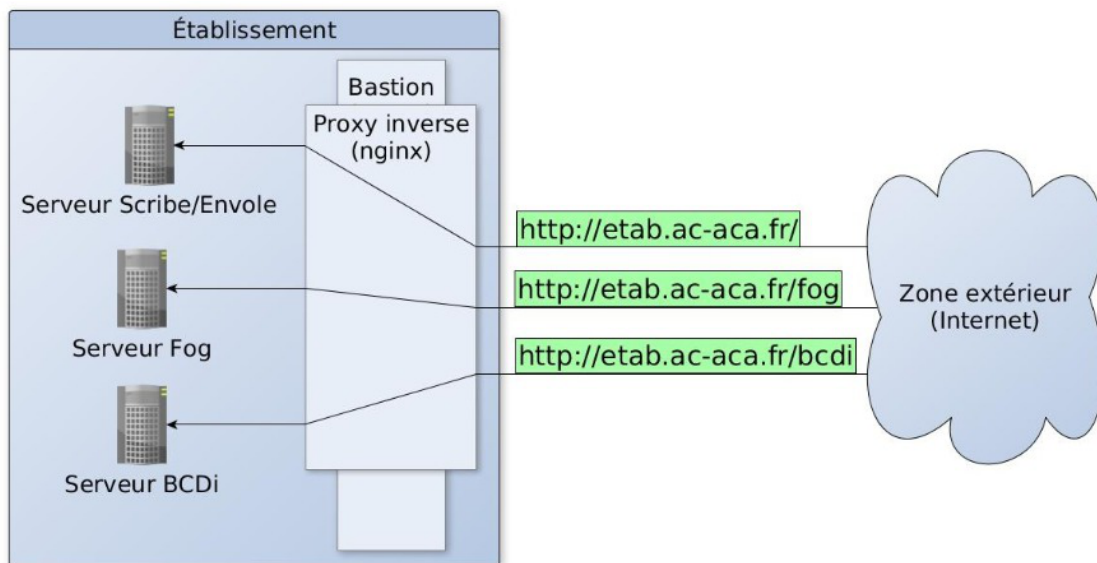


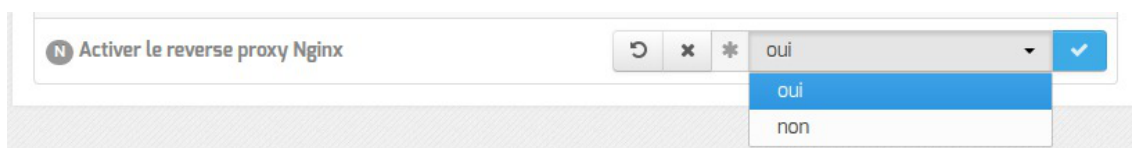
Diagramme d'un proxy inverse - Licence CC0

Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD^[p.545] ;
- application EOP ;
- protocole HTTP^[p.549] ;
- protocole HTTPS^[p.549].



Avant toute chose, le proxy inverse doit être activé dans l'onglet **Services** en passant Activer le reverse proxy Nginx à oui.

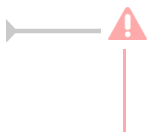


L'activation du service fait apparaître un nouvel onglet.

Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.



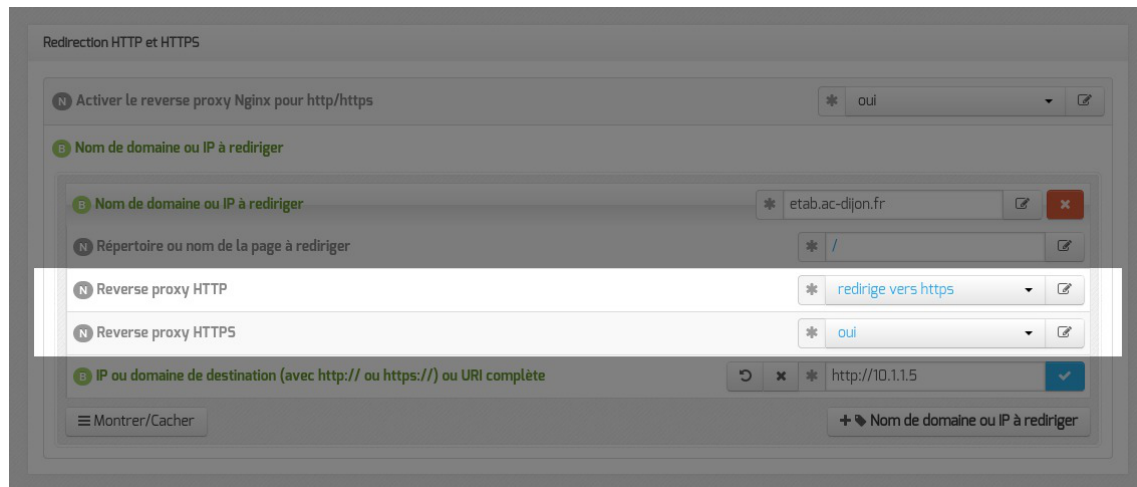
Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS

Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable Activer le reverse proxy Nginx pour le http/https à oui et de renseigner plus d'informations :

- le Nom de domaine ou IP à rediriger : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- le Répertoire ou nom de la page à rediriger permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est / ;

- l'IP ou domaine de destination (avec http:// ou https://) ou URI complète permet de saisir l'adresse IP (exemple : http://192.168.10.1), le nom de domaine (exemple : http://scribe.monetab.fr) ou l'URI^[p.563] (exemple : http://scribe.monetab.fr/webmail/) du serveur de destination hébergeant la ou les applications.

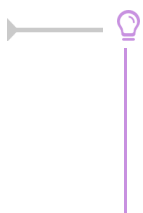


Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse http://monetab.fr sera automatiquement redirigé vers https://monetab.fr

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs Reverse proxy HTTP à non et Reverse proxy HTTPS à oui.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton Nom de domaine ou IP à rediriger.



Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote^[p.558], https://monetab.fr/pronote/ peut être redirigé vers http://pronote.monetab.fr/ (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

En mode expert il est possible :

- d'Activer la réécriture d'URL ;
- d'augmenter ou de diminuer la Longueur maximum pour un nom de domaine ;
- de choisir la Taille maximale des données reçues par la méthode POST (en Mo).



L'activation de la réécriture d'URL permet d'ajouter une expression rationnelle et une valeur de remplacement.

Il n'y a pas de lien automatique entre une "redirection" Nginx renseignée et une réécriture d'URL.

Pour que la réécriture d'URL s'applique à une règle il faut que le nom de domaine, le protocole et le répertoire de la réécriture correspondent aux paramètres saisis dans la règle de "redirection" renseignée.

Sur une installation recevant de très nombreuses connexions, diminuer la valeur de la Longueur maximum pour un nom de domaine (`server_names_hash_bucket_size`) pourra améliorer les performances du proxy inverse. La valeur optimale varie d'une installation à l'autre.

Avec une valeur trop basse, le service Nginx refusera de démarrer et affichera un message d'erreur ressemblant à :

```
could not build the server names hash, you should increase
server names hash bucket size: 32
```

Nginx Optimization : http://nginx.org/en/docs/http/server_names.html#optimization

L'option du mode expert Taille maximale des données reçues par la méthode POST (en Mo) permet de spécifier la taille des données HTTP au delà de laquelle Nginx renverra une erreur (message : Request Entity Too Large).

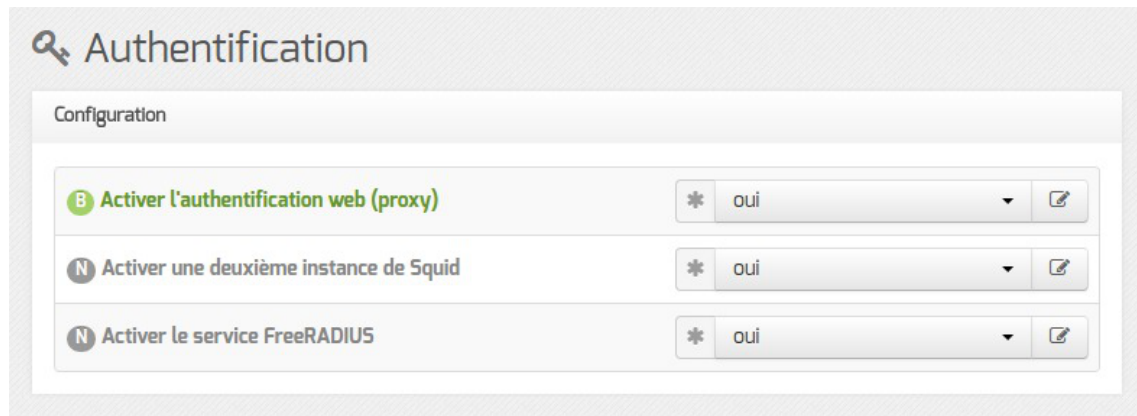
⚠ Dans le cas où, sur un module, le service `eole-web` est installé en plus du service `eole-reverseproxy` (ce qui est le cas sur le module AmonEcole et ses dérivés), le paramétrage de cette option est déplacée dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

4.30. Onglet Freeradius : Configuration de l'authentification Radius

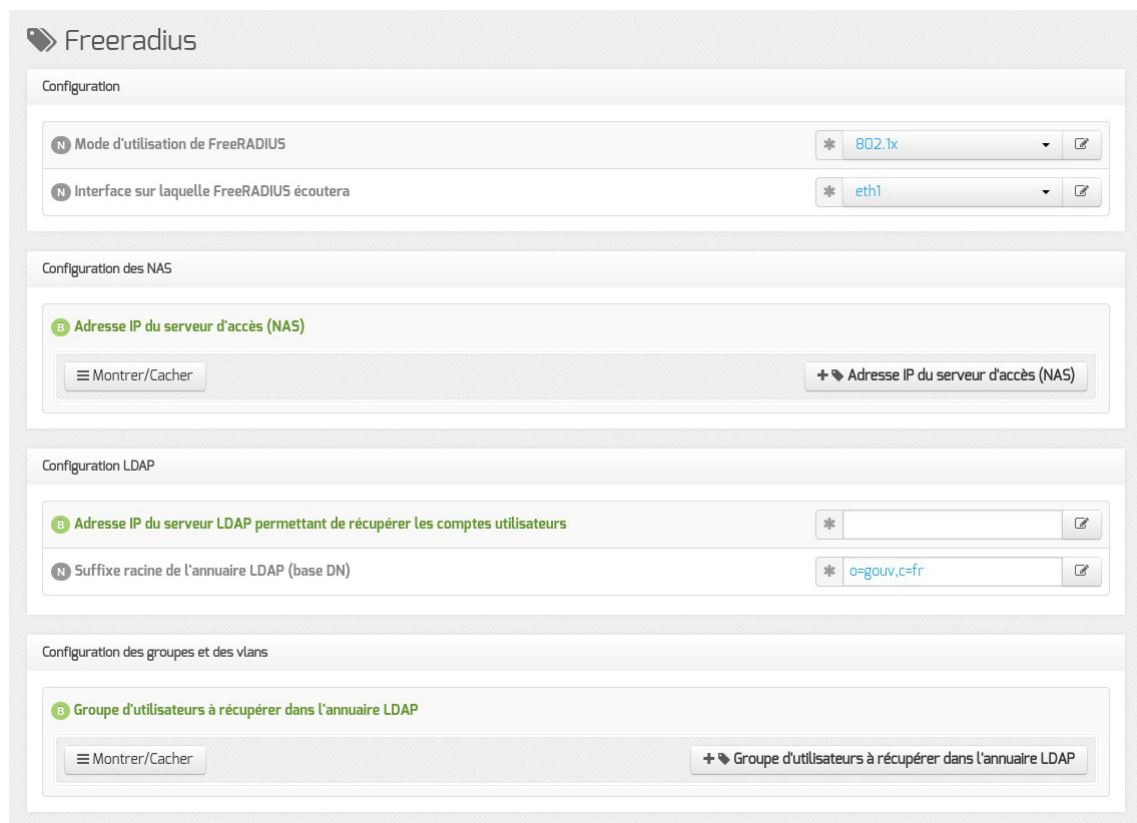
EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS^[p.559].

Pour profiter de cette fonctionnalité, il faut activer le service d'authentification RADIUS en passant

Activer le service FreeRADIUS à oui dans l'onglet Authentification .



Cela fera apparaître l'onglet **Freeradius** .



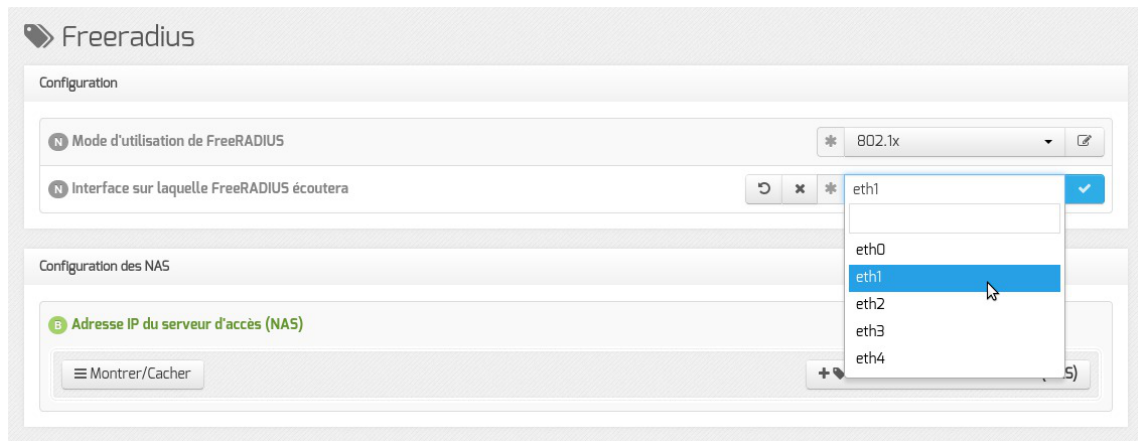
Vue de l'onglet Freeradius de l'interface de configuration du module

Il est possible de choisir entre 2 modes d'utilisation de FreeRADIUS :

- 802.1x ;
- accounting.

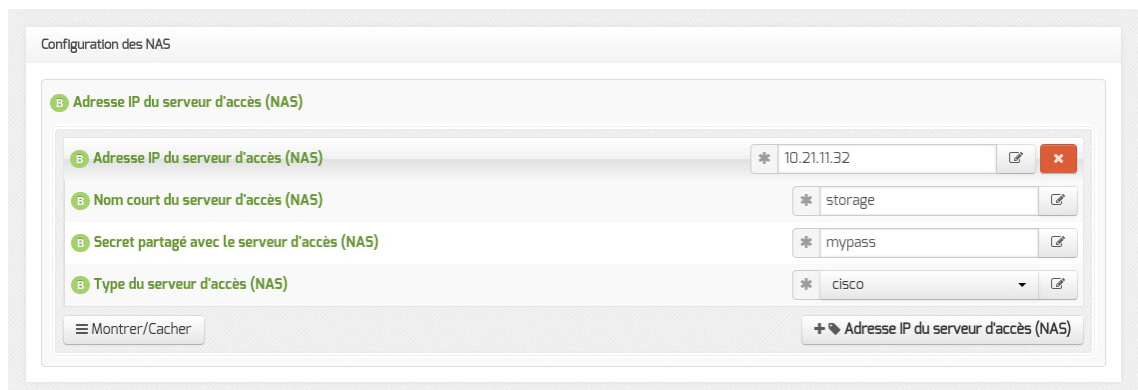
Le mode 802.1x

Le mode 802.1x permet de taguer dynamiquement des ports d'un switch (NAS^[p.554]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



Interface sur laquelle FreeRADIUS écoutera : définition de l'interface d'écoute de FreeRADIUS.

Configuration des NAS



Adresse IP du serveur d'accès (NAS) : adresse IP du switch.

Nom court du serveur d'accès (NAS) : libellé du switch.

Secret partagé avec le serveur d'accès (NAS) : secret partagé entre FreeRADIUS et le switch.

Type du serveur d'accès (NAS) : type de switch.

Configuration LDAP



Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs : adresse IP LDAP.

Suffixe racine de l'annuaire LDAP (base DN) : *ou=education,o=gouv,c=fr* par exemple.

Configuration des groupes et des VLAN

Groupe d'utilisateurs à récupérer dans l'annuaire LDAP : saisir ou choisir un groupe existant dans l'annuaire.

Numéro de VLAN à attribuer à ce groupe : les machines se connectant avec un utilisateur appartenant au groupe indiqué ci-dessus verra son port tagué sur ce numéro de VLAN.

Le mode accounting

Le mode accounting permet de créer un réseau Wi-Fi WPA entreprise sur une borne Wi-Fi (NAS) ayant pour identifiants autorisés les compte/motDePasse de l'annuaire LDAP déclaré.

Onglet Freeradius - mode accounting

Adresse IP sur laquelle FreeRADIUS écoutera : l'adresse IP d'une des interfaces du serveur.

Configuration des NAS

Onglet Freeradius - mode accounting

Adresse IP du serveur d'accès (NAS) : adresse IP de la borne Wi-Fi.

Masque de sous réseau (notation CIDR) du serveur d'accès (NAS) : 24 (en notation

CIDR^[p.543]) si le réseau est de classe C.

Nom court du serveur d'accès (NAS) : libellé de la borne Wi-Fi.

Secret partagé avec le serveur d'accès (NAS) : secret partagé entre FreeRADIUS et la borne Wi-Fi.

Type du serveur d'accès (NAS) : type de borne (other en général).

Configuration LDAP

Onglet Freeradius - mode accounting

Adresse IP du serveur LDAP permettant de récupérer les comptes utilisateurs : adresse IP ldap.

Suffixe racine de l'annuaire LDAP (base DN) : *ou=education,o=gouv,c=fr* par exemple.

Clé d'accès reader à la base ldap sur Scribe (/root/.reader) : à récupérer sur le serveur LDAP.

4.31. Onglet Eoleflask

Dans cet onglet se trouvent les options concernant le service Eoleflask et les options des applications reposant sur ce service.

Passer la variable En écoute depuis l'extérieur à oui permet d'accéder à l'interface de configuration du module depuis un poste client.

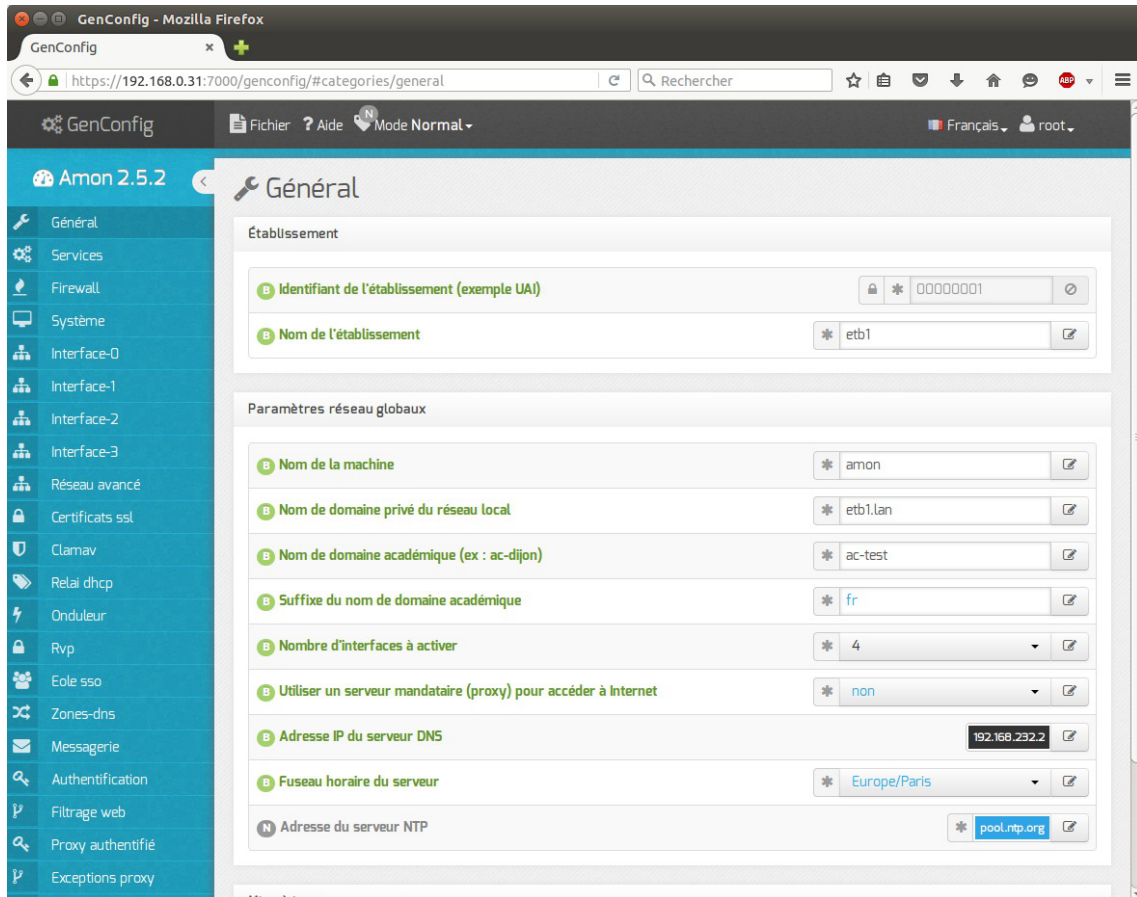
Accès distant

Après instance ou reconfigure, si votre adresse IP est autorisée pour l'administration du serveur, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

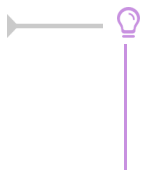
`https://<adresse_serveur>:7000/genconfig/`

Ne pas oublier d'utiliser le protocole HTTPS et de préciser le numéro de port 7000.

Il faut ensuite valider les certificats pour pouvoir accéder à l'interface.



Vue de l'interface de configuration au travers d'un navigateur web



Pour autoriser l'accès distant à une ou plusieurs adresses IP il faut le déclarer explicitement dans l'onglet `Interface-n` de l'interface de configuration du module en passant la variable `Autoriser les connexions SSH` à `oui`.

5. Configuration du module Amon avec le module Scribe en DMZ

L'installation d'un module Scribe et plus généralement de serveurs pédagogiques dans une DMZ^[p.545] permet de les isoler d'attaques provenant de l'intérieur (par exemple des services saturés par un virus utilisant le broadcast^[p.542]) et de les placer dans une zone où l'accès aux autres réseaux de l'établissement doit être explicitement autorisé.

L'utilisation d'une DMZ vise également à faciliter l'ouverture de services sur Internet, et notamment les services web (portail de l'établissement, messagerie, logiciels de vie scolaire, ...) et l'accès FTP.

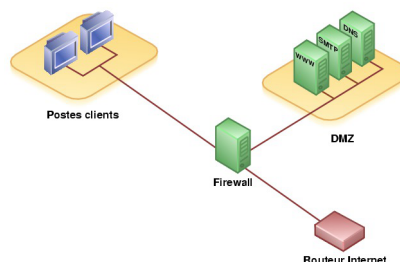


Diagramme d'une DMZ

Ports à ouvrir

Pour permettre un bon fonctionnement du serveur Scribe dans une DMZ, certains ports demandent à être ouverts.

Ces ports servent à la communication entre le serveur et les stations clientes, notamment pour le protocole Samba et pour le service Scribe (client Scribe) :

- 137-139 (TCP/UDP) : Samba ;
- 445 (TCP) : Samba ;
- 8788 (TCP) : service Scribe (client Scribe) ;
- 5800/5900 (TCP) : VNC.

Par défaut, sur le module Amon, une DMZ peut se connecter sur Internet.

Il faut cependant faire de la traduction d'adresse réseau (NAT^[p.554]) pour assurer le trafic.

Si la communication entre la DMZ et l'extérieur est fermée, les ports à ouvrir sont :

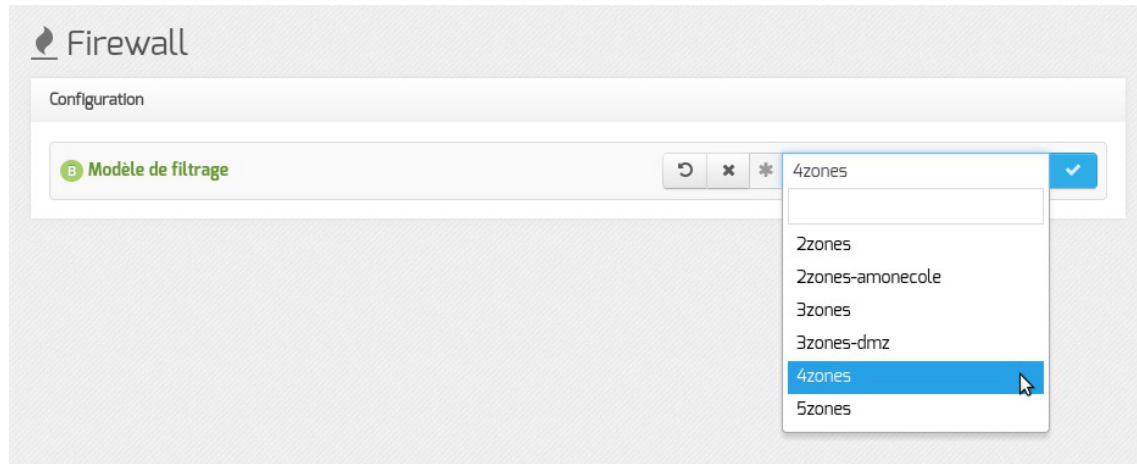
- pour le serveur Zéphir : 22 (TCP), 7080 (TCP) et 8090 (TCP) ;
- pour les serveurs mises à jour : 80 (TCP) ;
- pour les bases de données antivirales : tous les ports vers les adresses database.clamav.net et cvd.clamav.net

Pour pouvoir accéder au serveur Scribe depuis l'extérieur par le web et par le FTP, il faut rediriger la connexion effectuée sur les ports 21 et 443 (HTTP sécurisé) depuis l'extérieur sur le serveur Amon vers le serveur Scribe.

Configuration automatique

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet **Firewall**, choisir un Modèle de filtrage compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.



Le modèle de zones proposées correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

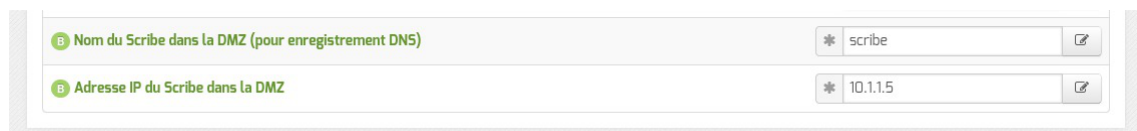
Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Ces modèles requièrent que le serveur Scribe soit déclaré au niveau du module Amon.

Pour se faire, dans l'onglet **Firewall** en mode normal ou expert, il faut répondre oui à la question Activer la gestion d'un Scribe dans la DMZ.



Cela entraîne l'apparition de nouvelles variables permettant de déclarer le nom et l'adresse IP du module Scribe.



Si le module Scribe offre un service DHCP pour le réseau pédagogique, il faudra activer et configurer le relai du DHCP entre ce serveur et le réseau pédagogique.

Voir aussi...

Onglet Relai DHCP [p.125]

ERA, éditeur de règles pour le module Amon [p.380]

6. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur

Le serveur Scribe étant derrière un serveur Amon, la configuration des deux modules permet de faire écouter l'EAD du serveur Scribe sur le port 4203 et donc d'y accéder depuis l'extérieur grâce à une redirection Nginx.

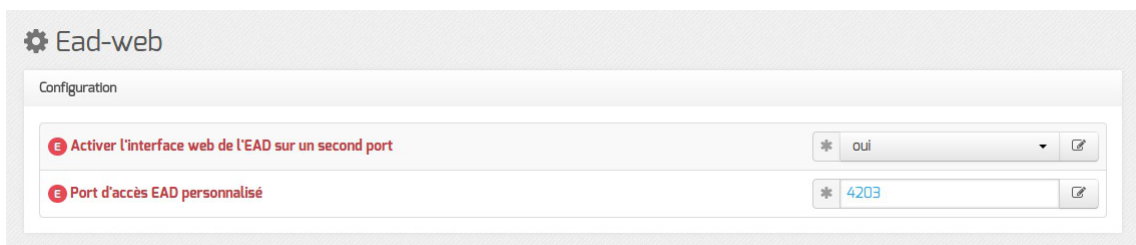
Avantages

Cette configuration présente plusieurs avantages par rapport à la méthode consistant à ajouter le serveurs de commandes du module Scribe dans l'interface EAD du serveur Amon :

- elle ne nécessite pas de déclarer le serveur SSO du serveur Scribe comme source d'authentification de l'EAD du serveur Amon ;
- il n'y a pas de problème d'incompatibilité (templates, protocoles obsolètes, ...) dans le cas où les versions des EAD des deux modules sont différentes ;
- elle simplifie la gestion des certificats.

Configuration côté Scribe

Dans l'interface de configuration du module Scribe, en mode expert, aller dans l'onglet **Ead-web** et passer la variable Activer l'interface web de l'EAD sur un second port à oui et vérifier que le port personnalisé est bien le 4203.



Ead-web	
Configuration	
Activer l'interface web de l'EAD sur un second port	* oui
Port d'accès EAD personnalisé	* 4203

Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande `reconfigure` est nécessaire afin que l'EAD écoute sur le port 4203.

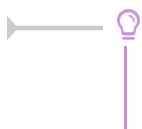
Configuration côté Amon

Dans l'interface de configuration du module Amon, aller dans l'onglet **Reverse proxy**, passer la variable Activer la redirection de l'EAD d'un Scribe à oui puis renseigner l'adresse IP du module Scribe et vérifier que le port renseigné est le 4203.



Activer la redirection de l'EAD Scribe	* oui
IP du Scribe pour la redirection EAD	* 10.1.3.5
Port de l'EAD sur le Scribe	* 4203

Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande `reconfigure` est nécessaire afin que la redirection soit appliquée.



L'autorisation d'accès au port configuré est gérée par ERA via la directive optionnelle cachée [p.544] : `ead_scribe`.

Voir aussi...

Onglet Ead-web : EAD et proxy inverse

Onglet Reverse proxy : Configuration du proxy inverse

7. Configurer le module Amon pour Envole

Pour un fonctionnement optimal des applications web hébergées sur le module Scribe derrière un serveur Amon ou hébergées sur module AmonEcole, il est impératif d'utiliser un nom de domaine^[p.555] (exemple : `monetab.ac-acad.fr`). Celui-ci doit être résolvable depuis Internet et il faut le renseigner partout où cela est nécessaire.

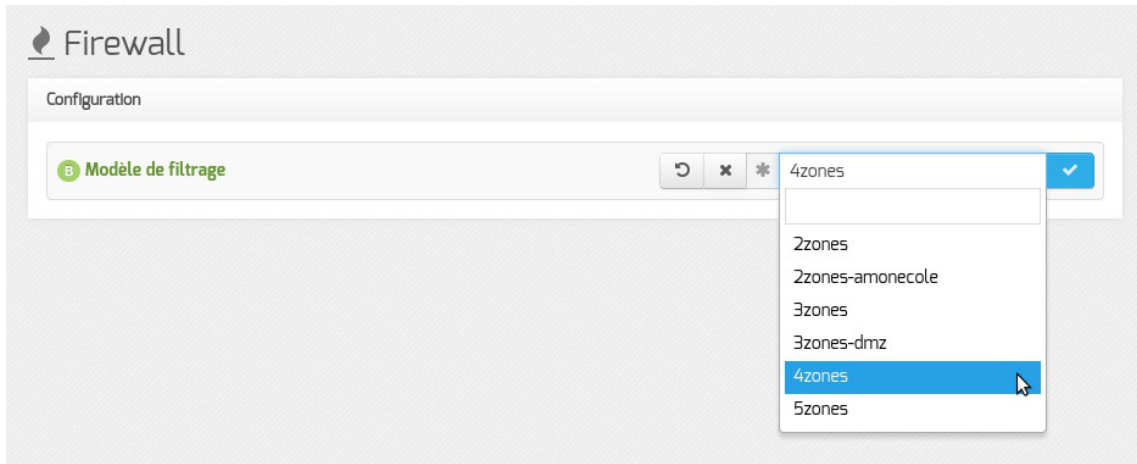
Ce nom de domaine sera à utiliser tant depuis l'extérieur de l'établissement que depuis l'intérieur.

Pour rendre accessible Envole ou certaines applications web hébergées sur le module Scribe depuis l'extérieur, il faut activer et configurer le pare-feu et le proxy inverse.

Configurer le pare-feu

Par défaut, le module Amon propose des modèles de pare-feu facilitant la mise en place d'un serveur Scribe en DMZ. Pour configurer le pare-feu, il faut dans l'onglet `Firewall`, choisir un `Modèle de filtrage` compatible :

- **3zones-dmz** : gestion d'une zone pedago sur eth1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth2 ;
- **4zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 ;
- **5zones** : gestion d'une zone admin sur eth1, d'une zone pedago sur eth2, d'une zone DMZ publique pouvant accueillir un module Scribe sur eth3 et d'une zone DMZ privée sur eth4.

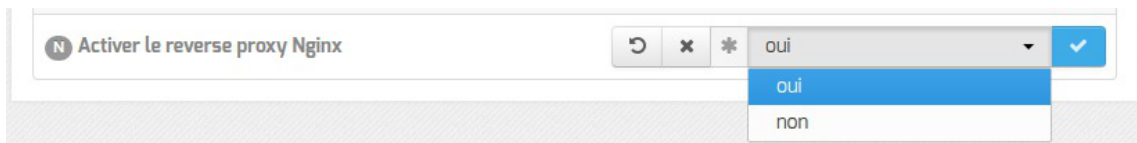


Le modèle de zones proposées correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

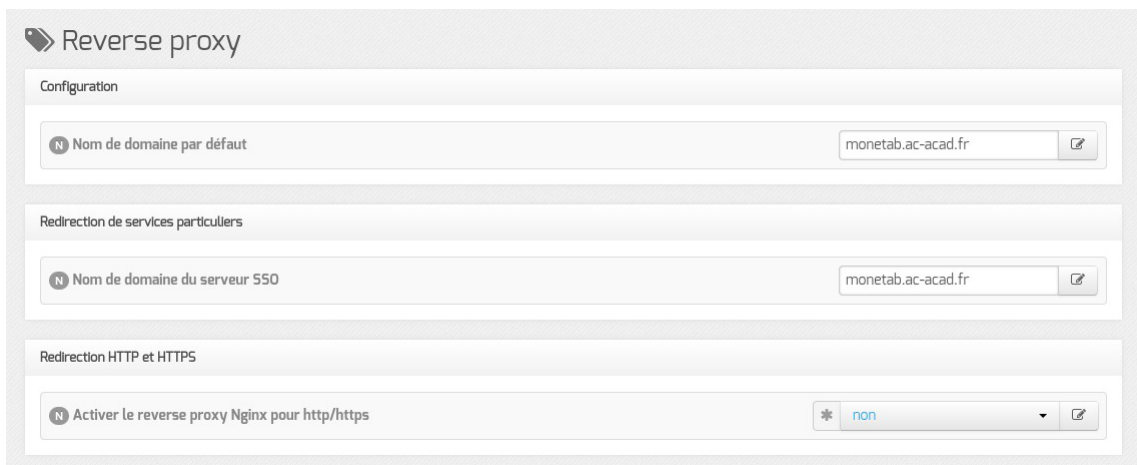
Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

Configuration du proxy inverse

Pour activer le proxy inverse, dans `Services`, passer `Activer le reverse proxy Nginx` à `oui`.

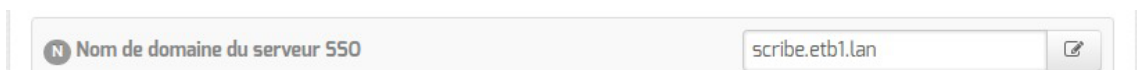


L'activation du service fait apparaître un nouvel onglet nommé `Reverse proxy`.

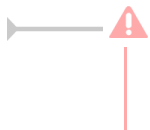


Vue de l'onglet Reverse proxy de l'interface de configuration du module

Redirection de services particuliers

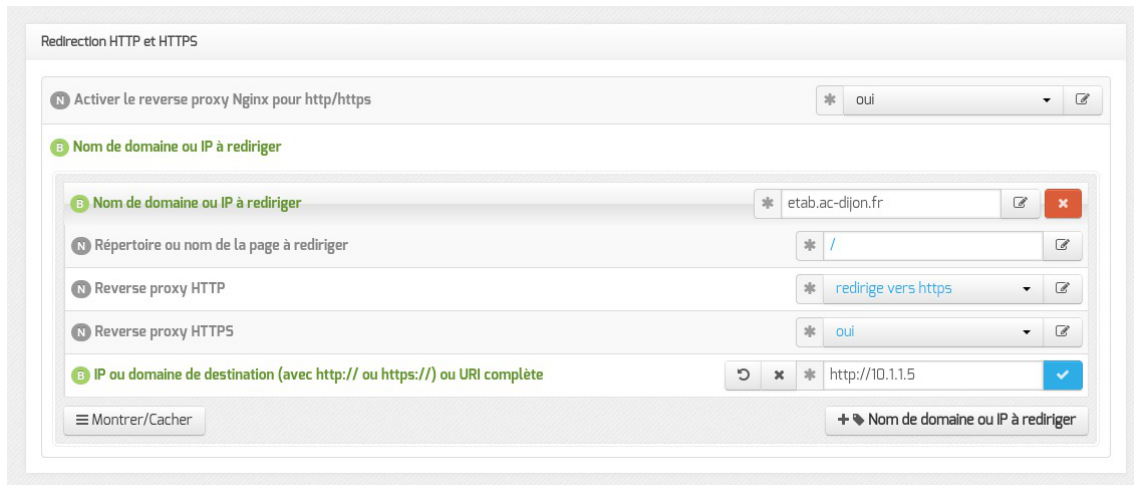


Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.



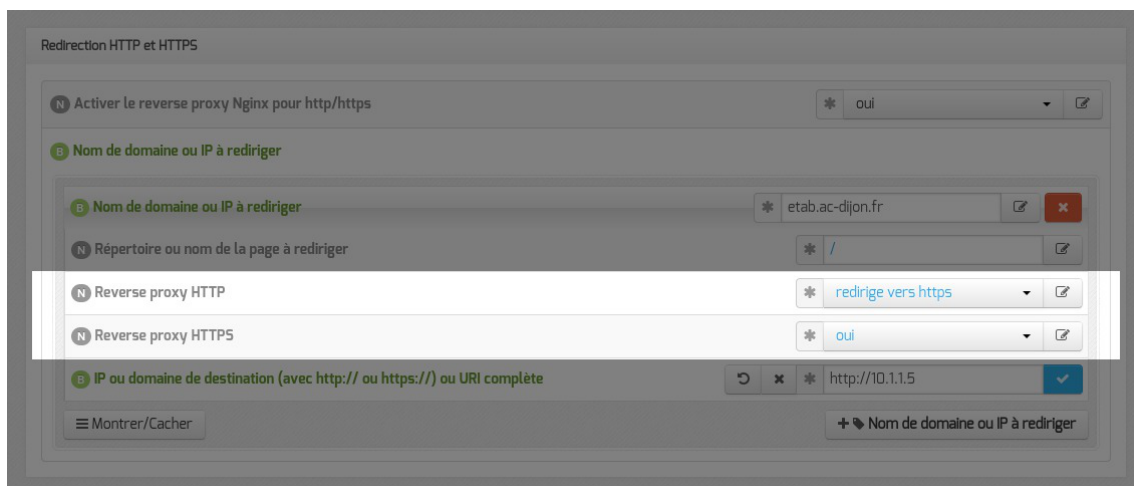
Le service SSO local du module Amon ne devra pas être activé si vous renseignez l'adresse d'un service SSO distant au niveau du proxy inverse.

Redirection HTTP et HTTPS



Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable Activer le reverse proxy Nginx pour le http/https à oui et de renseigner plus d'informations :

- le Nom de domaine ou IP à rediriger : le nom de domaine diffusé auprès des utilisateurs. Ce nom de domaine est celui qui permet d'accéder au module Amon ou AmonEcole ;
- le Répertoire ou nom de la page à rediriger permet de rediriger un sous-répertoire vers une machine. La valeur par défaut est / ;
- l'IP ou domaine de destination (avec http:// ou https://) ou URI complète permet de saisir l'adresse IP (exemple : http://192.168.10.1), le nom de domaine (exemple : http://scribe.monetab.fr) ou l'URI^[p.563] (exemple : http://scribe.monetab.fr/webmail/) du serveur de destination hébergeant la ou les applications.



Il est possible de forcer l'utilisation du protocole HTTPS pour les requêtes utilisant le protocole HTTP de façon transparente. De cette manière, un utilisateur web se connectant à l'adresse <http://monetab.fr> sera automatiquement redirigé vers <https://monetab.fr>

Ainsi les communications sont automatiquement chiffrées protégeant la transmission de données sensibles (nom d'utilisateur, mot de passe, etc.).

Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs Reverse proxy HTTP à non et Reverse proxy HTTPS à oui.

Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton Nom de domaine ou IP à rediriger.



Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote^[p.558], <https://monetab.fr/pronote/> peut être redirigé vers <http://pronote.monetab.fr/> (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Activation de l'authentification unique

Si vous voulez activer le service EoleSSO sur le module Amon, Utiliser un serveur EoleSSO à distant dans l'onglet Services, dans l'onglet Eole sso, seuls les paramètres Nom de domaine du serveur d'authentification SSO et Port utilisé par le service EoleSSO sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.

Configuration d'un serveur EoleSSO distant

L'option Nom de domaine du serveur d'authentification SSO doit être configurée avec le nom de domaine public utilisé dans Envole (typiquement : *monetab.ac-monacad.fr*).

Dans ce cas l'utilisateur admin du module Scribe sera administrateur du module Amon.

Dans le cas de l'utilisation du serveur EoleSSO local, Nom de domaine du serveur d'authentification SSO doit être renseigné avec le nom DNS du serveur.

Nom de domaine et récapitulatif de la configuration

Le nom de domaine doit être renseigné à de multiples endroits de la configuration.

- onglet **Général** : choisir le modèle de filtrage ;
- onglet **Services** :
 - Activer le proxy inverse Nginx : oui ;
- onglet **Eole sso** :
 - Nom de domaine du serveur d'authentification SSO : etab.ac-acad.fr ;
- onglet **Applications web** si module AmonEcole :
 - Nom de domaine des applications web (sans http://) : etab.ac-acad.fr ;
- onglet **Reverse proxy** :
 - Nom de domaine par défaut : etab.ac-acad.fr ;
 - Nom de domaine du serveur SSO : etab.ac-acad.fr ;
 - Activer la configuration automatique pour les applications locales à oui.
- onglet **Certificats ssl** uniquement en mode expert :
 - Nom DNS/IP alternatif du serveur : etab.ac-acad.fr (*ré-générer les certificats si nécessaire*).

Voir aussi...

Onglet Firewall [p.105]

Onglet Reverse proxy : Configuration du proxy inverse [p.150]

Onglet Eole sso : Configuration du service SSO pour l'authentification unique [p.133]

ERA, éditeur de règles pour le module Amon [p.380]

8. Configuration DNS pour chaque interface

Configuration des alias sur l'interface

EOLE supporte les alias sur les cartes réseau. Définir des alias IP consiste à affecter plus d'une adresse IP à une interface.

Pour cela, il faut activer son support (Ajouter des IP alias sur l'interface à oui) et configurer l'adresse IP et le masque de sous réseau.

Autoriser cet alias à utiliser les DNS de zones forward additionnelles permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.



Si le support du RVP est activé une option supplémentaire est disponible :

- Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES : Si le service RVP est activé (onglet Services) et que le serveur est membre du réseau AGRIATES (onglet Rvp) la variable est disponible pour autoriser ou non cet alias à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN (réseau local virtuel) sur une interface déterminée du module.

Pour cela, il faut activer son support (Activer le support des VLAN sur l'interface à oui et ajout d'un numéro identifiant du VLAN avec le bouton + Numéro d'identifiant du VLAN) et configurer l'ensemble des paramètres utiles (l'ID, l'adresse IP, ...).

Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.

Si le support du RVP est activé une option supplémentaire est disponible :

- Autoriser ce VLAN à utiliser les DNS de Forward RVP/AGRIATES : Si le service RVP est activé (onglet Services) et que le serveur est membre du réseau AGRIATES (onglet Rvp) la variable est disponible pour autoriser ou non ce VLAN à utiliser les DNS noms d'hôte de la zone AGRIATES.

Configuration DNS sur l'interface

Il est possible d'ajuster les paramètres du serveur DNS pour chaque interface réseau sauf pour l'interface 0.

- Serveur master DNS de cette zone : sert à activer le DNS sur l'interface.
- Autoriser le réseau ethX à utiliser les DNS des zones forward additionnelles : permet d'autoriser le réseau ethX à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet Zones-dns.

- **Nom à donner à l'interface (pour résolution DNS)** : entrée DNS correspondant à l'adresse IP de l'interface ethX. Le nom par défaut (admin pour l'interface eth1) est différent et doit rester pour chaque interface.

Si le support du RVP est activé une option supplémentaire est disponible :

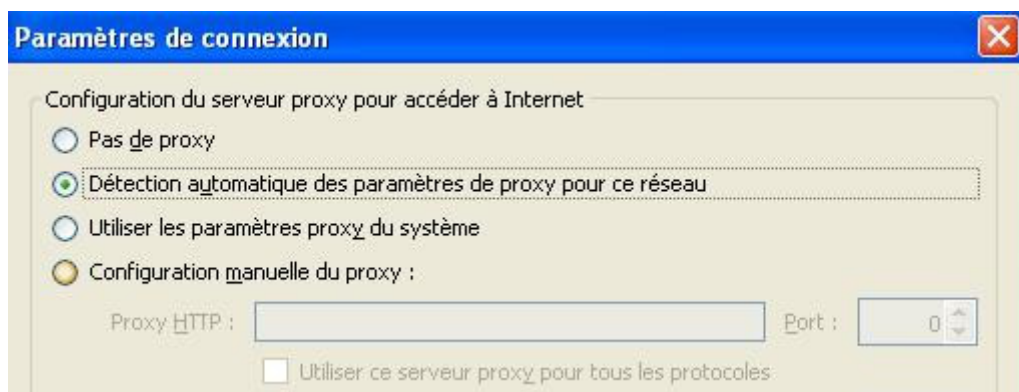
- **Autoriser le réseau ethX à utiliser les DNS de forward RVP/AGRIATES** : Si le service RVP est activé (onglet Services) et que le serveur est membre du réseau AGRIATES (onglet Rvp) la variable est disponible pour autoriser ou non le réseau ethX à résoudre les noms d'hôte de la zone AGRIATES.

9. Configurer la découverte automatique du proxy avec WPAD

WPAD^[p.564] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essaiera de télécharger le fichier : `wpad.<domaine local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.



La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm^[p.543] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx^[p.555] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom_domain_local>` qui pointe vers le serveur web ;
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.

⚠ Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.

💡 Pour les postes de travail Windows c'est la valeur du champ `Nom de domaine du serveur WPAD` qui sera utiliser pour accéder au fichier WPAD tandis que pour des postes de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.

Configuration interface showing the field "Nom de domaine du serveur WPAD" with the value "etb1.lan".

Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.

⚠ Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet `eole-wpad` mais n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom_domain_local>` corresponde à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.

Configuration interface showing the field "Activer le support de WPAD" with the value "oui".

Activation de WPAD dans l'onglet Services

Dans l'onglet **Services** de l'interface de configuration du module Activer le support de WPAD doit être placé à oui.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet **Wpad** au sein duquel le Nom de domaine du service WPAD doit être rempli avec la même valeur que le Nom de domaine privé du réseau local présent dans l'onglet **Général**.

⚠ Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au Nom de domaine privé du réseau local de l'onglet **Général**, il faut le déclarer dans le champ Nom domaine local supplémentaire ou rien de l'onglet **Zones-dns**.

⚠ Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande **reconfigure** sur le module.

💡 WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.
En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

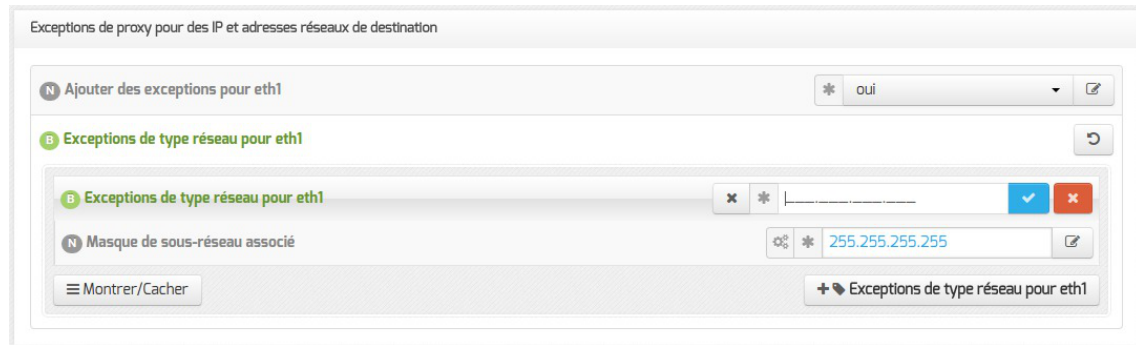
Ajouter des exclusions dans la configuration automatique du proxy

Dans l'onglet **Exceptions proxy** de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton **Exceptions de type réseau pour eth-n** permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

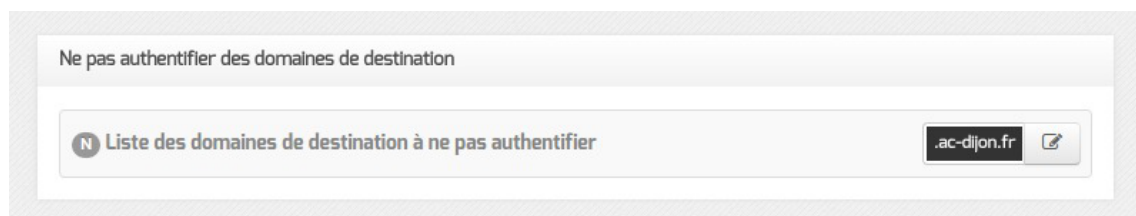
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour laquelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.



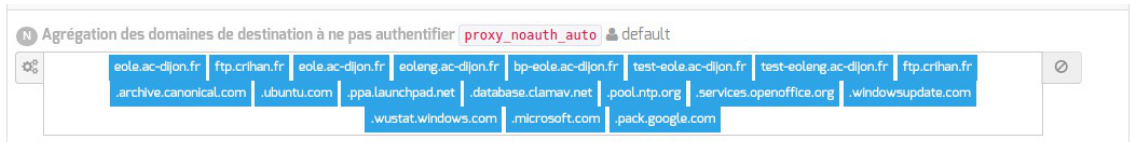
Si cNTLM et WPAD sur activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`.
Il est possible de l'afficher dans l'onglet **Exceptions proxy** de l'interface de configuration du

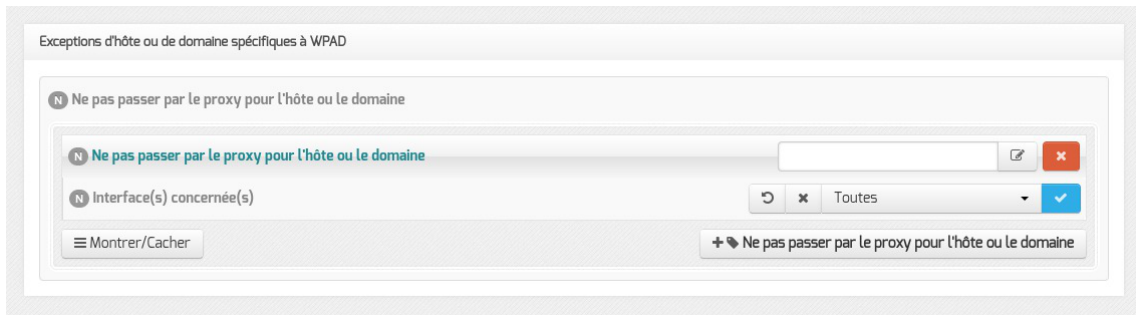
module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier `WPAD.dat` généré contiendra la ligne `!! localhostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le domaine` (`dnsDomainIs`) : <http://findproxyforurl.com/netscape-documentation/#dnsDomainIs>
 Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (`localhostOrDomainIs`) : <http://findproxyforurl.com/netscape-documentation/#localhostOrDomainIs>

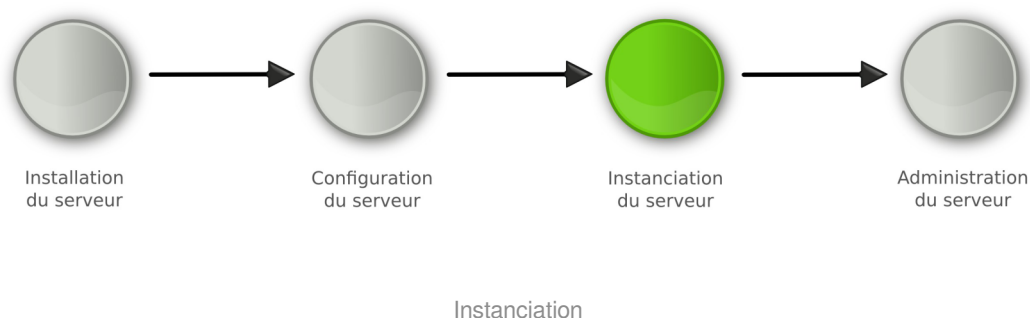
Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP

Chapitre 7

Instanciation du module

La troisième des quatre phases



- La **phase d'instanciation** s'effectue au moyen de la commande `instance` .

L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.

À l'issue de cette phase, le serveur est utilisable en exploitation.

Cette phase doit être complétée par un diagnostic complet du module à l'aide de la commande `diagnose -L` .

1. Principes de l'instanciation

Les modules EOLE sont livrés avec un ensemble de **templates**.

Les templates^[p.562] sont les fichiers de configuration de chacun des logiciels utilisés. Ils sont pré-paramétrés et contiennent des variables.

Parallèlement les modules fournissent des dictionnaires décrivant l'ensemble de ces variables, comme expliqué dans la phase de configuration.

L'instanciation consiste à remplacer les variables par les valeurs renseignées dans le fichier `/etc/eole/config.eol` et à copier les fichiers vers leur emplacement cible.

Si des patches EOLE^[p.558] ont été créés pour personnaliser le serveur, ils seront pris en compte durant cette phase.

Voir aussi...

Personnalisation du serveur à l'aide de Creole ^[p.426]

2. Lancement de l'instanciation

Pour lancer l'instanciation, il faut utiliser la commande `instance`.

Le compte rendu d'exécution est dans le fichier `/var/log/creole.log`.

En plus de remplacer les variables par les valeurs renseignées dans le fichier `/etc/eole/config.eol` et de copier les fichiers vers leur emplacement cible, l'instanciation :

- arrête et redémarre des services ;
- lance des commandes ;
- effectue certaines tâches en fonction des réponses aux dialogues proposés.

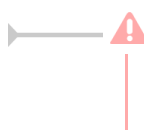
Un fichier `config.eol.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation du serveur. Celui-ci permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.


 La commande `instance` utilise le fichier `/etc/eole/config.eol`. Il n'est plus nécessaire de spécifier le nom du fichier à utiliser.

2.1. Les mots de passe

À l'installation le mot de passe du compte `root` a été généré aléatoirement selon les critères suivants :

- 12 caractères ;
- au moins une majuscule ;
- au moins un chiffre ;
- au moins un caractère spécial ;
- pas de caractères ambigus (l ou 1, 0 ou O, ...).

 Le mot de passe aléatoire de l'utilisateur `root` est affiché uniquement sur la console, il faut donc avoir un accès physique à la machine.

 La connexion SSH par mot de passe pour l'utilisateur `root` est permise.

Au lancement de l'instanciation, la modification des mots de passe est demandée pour le compte :

- de l'utilisateur `root` ;
- du ou des utilisateurs à droits restreints (`eole`, `eole2`, ...)
- de l'utilisateur `admin` sur les modules Scribe, Horus et AmonEcole ;
- de l'utilisateur `admin_zephir` sur le module Zéphir.



Sur un module Amon, en cas d'utilisation d'un réseau pédagogique et d'un réseau administratif, le second administrateur (`eole2`) permet d'administrer le réseau pédagogique.

Par défaut, le système vérifie la pertinence des mots de passe. Pour cela, il utilise un système de classes de caractères :

- les lettres en minuscule [a-z] ;
- les lettres en majuscule [A-Z] ;
- les chiffres [0-9] ;
- les caractères spéciaux (exemple : \$*ùµ%£, ; : !\$/ . ?).

Il faut utiliser différentes classes de caractères pour que le mot de passe soit considéré comme valide. Il n'est pas possible de réutiliser le mot de passe par défaut fourni à l'installation.

Par défaut, voici les restrictions :

- une seule classe de caractères : impossible ;
- deux classes de caractères : 9 caractères ;
- trois et quatre classes : 8 caractères.

Cette configuration est modifiable durant l'étape de configuration, en mode expert (onglet `Systeme`).



Il s'agit de comptes d'administration donc sensibles sur le plan de la sécurité. Il est important de renseigner des mots de passe forts.

Cet article du CERTA donne une explication détaillée sur la stratégie des mots de passe.

<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>

2.2. Activation automatique de la mise à jour hebdomadaire

À la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée.

La mise à jour permet de maintenir votre serveur avec le niveau de fonctionnalité le plus récent et surtout de bénéficier des dernières corrections. Certaines corrections peuvent combler des failles de sécurité importantes, il est donc important de les appliquer aussitôt qu'elles sont publiées.

Il est conseillé d'effectuer la mise à jour immédiatement, comme proposé à la fin de l'instance.

Une mise à jour est recommandée

Voulez-vous effectuer une mise à jour via le réseau maintenant ? [oui/non]

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.

Voir aussi...

Gestion des tâches planifiées eole-schedule [p.474]

2.3. Le redémarrage

Il est possible qu'un redémarrage soit proposé à la fin de l'instanciation.

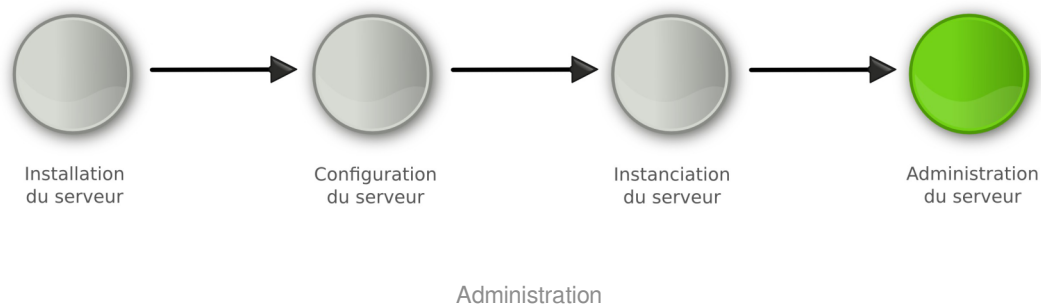
Si le noyau (kernel) a été mis à jour, le serveur doit redémarrer pour pouvoir l'utiliser. Dans ce cas, la question suivante apparaîtra :

Un redémarrage est nécessaire

Faut-il l'effectuer maintenant ? [oui/non]

Chapitre 8

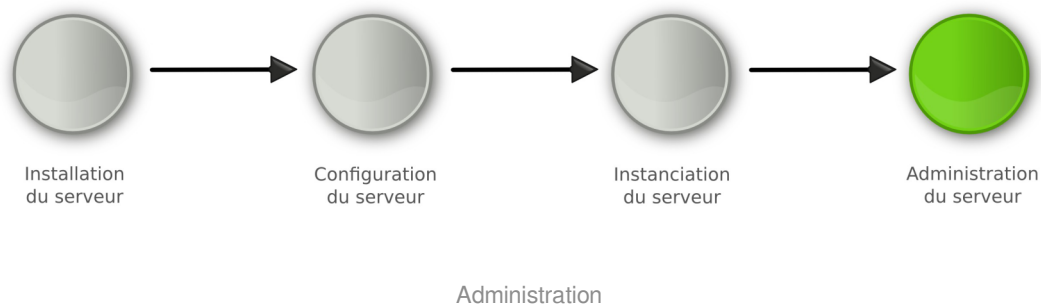
Administration du module Amon



- La **phase d'administration** correspond à l'exploitation du serveur.
Chaque module possède des fonctionnalités propres, souvent complémentaires.
Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

1. Administration généralités

La dernière des quatre phases



- La **phase d'administration** correspond à l'exploitation du serveur.
Chaque module possède des fonctionnalités propres, souvent complémentaires.
Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

1.1. Principes de l'administration

L'administration d'un module est facilitée par plusieurs outils mis à disposition :

- l'interface d'administration web : [EAD](#) ;

- l'interface d'administration semi-graphique : `manage-eole` ;
- l'interface d'administration du module Zéphir : `Zéphir-Web` ;
- des outils spécifiques à certains modules : `ARV`, `frontend_horus`, ...
- des interfaces fournies par les logiciels utilisés : Cups, Sympa, ...
- la procédure de mise à jour ;
- les sauvegardes.

Il est également possible d'utiliser la **ligne de commande**.

Le choix de l'outil à utiliser s'effectue en fonction du type de module, de l'emplacement de ce module dans l'architecture (serveur en établissement ou serveur académique) et du profil de l'administrateur (administrateur académique, relai académique, personne ressource en établissement...).

1.2. Découverte de GNU/Linux



1.2.1. Les Bases

Descriptif sommaire

Une distribution

- un kernel = Linux [p.551]
- des outils périphériques = GNU [p.548]
- un environnement console ou graphique
- un système de fichiers éprouvé, hérité d'UNIX

1.2.1.a. L'arborescence GNU/Linux

L'arborescence GNU/Linux

Pour l'utilisateur, un système de fichiers est vu comme une arborescence : les fichiers sont regroupés dans des répertoires (concept utilisé par la plupart des systèmes d'exploitation). Ces répertoires contiennent soit des fichiers, soit récursivement d'autres répertoires. Il y a donc un répertoire racine et des sous-répertoires. Une telle organisation génère une hiérarchie de répertoires et de fichiers organisés en arbre.

Racine de l'arbre

`/` (appelé slash ou root) : racine de l'arborescence sur laquelle sont raccrochés tous les sous-répertoires et fichiers.

Arborescence 1er niveau

- `bin/` : commandes liées au système, exécutables par tous ;
- `boot/` : noyau et initrd nécessaires au démarrage (ou boot) du système ;
- `dev/` : fichiers spéciaux effectuant le lien noyau / périphériques ;
- `etc/` : fichiers de configuration ;
- `home/` : répertoires de connexion (ou home directory) des utilisateurs ;
- `lib/` : bibliothèques essentielles au démarrage et modules du noyau ;
- `mnt/` : contient les sous-répertoires de montage des partitions des autres périphériques ;
- `opt/` : installation des applications autres ;
- `proc/` : pseudo système de fichier représentant le noyau à un instant T ;
- `root/` : répertoire de connexion de root ;
- `sbin/` : commandes réservées à root et utilisées dans les niveaux de démarrage bas ;
- `sys/` : pseudo système de fichier représentant les processus ;
- `tmp/` : répertoire temporaire accessible à tous ;
- `usr/` : commandes utilisées par les utilisateurs (bin), l'administrateur (sbin), mais aussi ensemble du système graphique ;
- `var/` : ensemble des données variables du système (spools, logs, web, bases de données, ...).

Filesystem Hierarchy Standard (« norme de la hiérarchie des systèmes de fichiers », abrégé en **FHS**) définit l'arborescence et le contenu des principaux répertoires des systèmes de fichiers des systèmes d'exploitation GNU/Linux et de la plupart des systèmes Unix.

Fichiers et répertoires

Sous Unix, tout est fichier

Les différents types :

- **fichiers ordinaires** : fichiers éditables
- **fichiers programmes** : fichiers contenant des données compilées
- **répertoires** : fichier contenant les infos sur les fichiers et sous-répertoires contenus (index)
- **fichiers spéciaux** : fichier associé à un périphérique. Ne contient qu'une description relative au driver et type d'interface.

Adresse absolue / adresse relative

Un fichier ou un répertoire peut être défini :

- soit par un chemin relatif à l'endroit où vous vous positionnez au moment T.
- soit par un chemin absolu à partir de la racine de l'arborescence.

1.2.1.b. La gestion des droits

Droits de base UNIX

Les droits détaillés ci-après s'appliquent à l'ensemble des composantes de l'arborescence GNU/Linux, à savoir les fichiers et les répertoires.

Droits essentiels :

- lecture
- écriture
- exécution

Autres droits :

- sticky bit
- setuid et setgid bits

Description d'un fichier

```
$ ls -li fic
309790 -rw-r--r-- 1 user1 group1 64 avr 20 14:59 fic
```

1. numéro d'inode
2. type & droits sur le fichier (ou répertoire)
3. compteur de liens physiques
4. propriétaire
5. groupe
6. taille
7. date de dernière modification
8. nom du fichier (répertoire)

Représentation du type et des droits des fichiers

Le schéma précédent montre, dans le second bloc, comment sont affichés les droits associés à un fichier (ou répertoire).

Ce bloc se décompose en 4 sous-parties :

- La première, codée sur un caractère, représente le type du fichier
- On trouve ensuite 3 groupes de 3 caractères indiquant les droits de lecture/écriture/exécution.

Le type du fichier peut être un des éléments suivants :

- **d** : répertoire
- **l** : lien symbolique

- `c` : périphérique de type caractère
- `b` : périphérique de type bloc
- `p` : pile fifo
- `s` : socket
- `-` : fichier classique



- Fichiers de périphériques :
 - `brw-rw----` 1 root disk 8, 0 nov 12 08:17 /dev/sda
 - `brw-rw----` 1 root cdrom 3, 0 nov 12 08:17 /dev/hda
 - `crw-r-----` 1 root kmem 1, 1 nov 12 08:17 mem
 - `crw-rw----` 1 root root 4, 0 nov 12 08:17 tty0
- Répertoires :
 - `drwxr-xr-x` 13 root root 4096 oct 20 10:22 /usr
 - `drwxr-xr-x` 17 user1 group1 4096 oct 31 09:18 /home/user1
- Fichiers standards :
 - `-rw-r--r--` 1 root root 2008 oct 17 19:36 /etc/inittab
 - `-rw-r--r--` 1 root root 724 déc 20 2006 /etc/crontab
 - `-rwxr-x--1` root root 1024 oct 29 /home/user1/monScript
- Lien symbolique :
 - `lrwxrwxrwx` 1 root root 31 oct 27 15:00 /var/lib/postgresql/8.3/main/root.crt -> /etc/postgresql-common/root.crt
- Socket :
 - `srw-rw-rw-` 1 root root 0 nov 12 08:18 /var/run/gdm_socket

Détail des droits standards

Comme énoncé précédemment, les droits sont codés sur 3 jeux de 3 droits.

Cet ensemble de 3 droits sur 3 entités se représente généralement de la façon suivante : on écrit côte à côte les droits **r** (*R*ead/lecture), **w** (*W*rite/écriture) puis **x** (*eX*ecute/exécution) respectivement pour le propriétaire (**u**), le groupe (**g**) et les autres utilisateurs (**o**). Les codes u, g et o (u comme user, g comme group et o comme others) sont utilisés par les commandes UNIX qui permettent d'attribuer les droits et l'appartenance des fichiers.

Lorsqu'un droit est attribué à une entité, on écrit ce droit (r, w ou x), et lorsqu'il n'est pas attribué, on écrit un '-'. Par exemple : `rwxr-xr--`

Droits Spécifiques

SUID Bit

Ce droit s'applique aux fichiers exécutables, il permet d'allouer temporairement à un utilisateur les droits du propriétaire du fichier, durant son exécution.

En effet, lorsqu'un programme est exécuté par un utilisateur, les tâches qu'il accomplira seront restreintes par ses propres droits, qui s'appliquent donc au programme.

Lorsque le droit SUID est appliqué à un exécutable et qu'un utilisateur quelconque l'exécute, le programme détiendra alors les droits du propriétaire du fichier durant son exécution.

Bien sûr, un utilisateur ne peut jouir du droit SUID que s'il détient par ailleurs les droits d'exécution du programme. Ce droit est utilisé lorsqu'une tâche, bien que légitime pour un utilisateur classique, nécessite des droits supplémentaires (généralement ceux de root). Il est donc à utiliser avec précaution.

- `-r-s--x--x 1 root root 15540 jun 20 2004 /usr/bin/passwd`

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci :
`---s-----` ou `---S-----`

SGUID Bit

Ce droit fonctionne comme le droit SUID, mais appliqué aux groupes. Il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire.

De plus, ce droit a une tout autre utilisation s'il est appliqué à un répertoire. Normalement, lorsqu'un fichier est créé par un utilisateur, il en est propriétaire, et un groupe par défaut lui est appliqué (généralement users si le fichier a été créé par un utilisateur, et root s'il a été créé par root). Cependant, lorsqu'un fichier est créé dans un répertoire portant le droit SGID, alors ce fichier se verra attribuer par défaut le groupe du répertoire. De plus, si c'est un autre répertoire qui est créé dans le répertoire portant le droit SGID, ce sous-répertoire portera également ce droit.

- `-rwxr-sr-x 1 root utmp 319344 avr 21 2008 /usr/bin/xterm`

C'est un **s** si le droit d'exécution du propriétaire est présent, ou un **S** sinon. Il se place donc comme ceci :
`---s-----` ou `---S-----`

Sticky Bit

Lorsque ce droit est positionné sur un répertoire, il interdit la suppression des fichiers qu'il contient à tout utilisateur autre que le propriétaire. Néanmoins, il est toujours possible pour un utilisateur possédant les droits d'écriture sur ce fichier de le modifier (par exemple de le transformer en un fichier vide).

Notation : il est représenté par la lettre `t` ou `T`, qui vient remplacer le droit d'exécution `x` des autres utilisateurs que le propriétaire et ceux appartenant au groupe du fichier, de la même façon que les droits SUID et SGID. La majuscule fonctionne aussi de la même façon, elle est présente si le droit d'exécution `x` caché n'est pas présent : `-----t` ou `-----T`

Exemple : le répertoire /tmp

- `drwxrwxrwt 23 root root 4096 oct 20 14:27 /tmp/`

Listes de contrôle d'accès

Une liste de contrôle d'accès ou ACL, permet de définir une liste de permission sur un fichier ou répertoire.

Aux habituels utilisateur, groupe et autre, il est possible d'étendre le nombre d'utilisateurs et de groupes ayant des droits sur un même fichier

Les ACLs s'ajoutent aux droits standards. Lorsqu'on liste les droits d'un fichier, les ACLs sont symbolisées par un "+".

```
-rwxrwx---+ 1 root professeurs 26 2009-05-27 16:37 fic
```

Les droits étendus apparaissent de la façon suivante :

```
user::rwx
```

```
user:p.nom:rwx
```

```
group::---
```

```
mask::rwx
```

```
other::---
```

Les ACLs d'un dossier père ne sont pas automatiquement repris pour le fichier fils.

Il est possible de modifier ce comportement, à associer des droits par défaut (grâce à l'attribut *default*).

Par exemple :

```
user::rwx
```

```
user:p.nom:rwx
```

```
group::rwx
```

```
mask::rwx
```

```
other::--x
```

```
default:user::rwx
```

```
default:user:p.nom:rwx
```

```
default:group::---
```

```
default:mask::rwx
```

```
default:other::---
```

1.2.1.c. La gestion des processus

Définition d'un processus

Un processus est un programme qui s'exécute en mémoire.

Tout processus lancé :

- se voit attribuer un numéro appelé **PID** (Process Identifier).
- est fils du processus qui l'a lancé. Le fils connaît le PID de son père, et en garde une trace sous la forme d'un numéro appelé **PPID** (Parent Process Identifier).
- appartient à un propriétaire (**UID** - celui qui a lancé le programme et qui pourra interagir avec ce processus)
- détermine son activité par un état : Actif, Exécutable, Endormi, Zombi.

Si un processus disparaît, tous les processus fils disparaissent également, sauf quand un processus est rattaché à `init`. Ainsi donc, à l'instar des fichiers, les processus sont organisés en arbre.

Enfin GNU/Linux est un système multi-tâche, c'est à dire que plusieurs processus peuvent être exécutés en même temps, en réalité, un seul utilise le processeur à la fois, ce dernier ne sachant effectuer qu'une seule instruction à la fois.

Etat d'un processus

Comme évoqué précédemment, un processus peut avoir un état : Actif, Exécutable, Endormi, Zombi.

- **Actif** : le processus utilise le processeur, et est donc en train de réaliser des actions pour lequel il a été conçu.

- **Exécutable** : le processus est en exécution mais il est en attente de libération du processus qui est utilisé par un processus actif. Pour l'utilisateur, ceci est invisible car l'opération est très rapide.
- **Endormi** : comme son nom l'indique, le processus est endormi, il ne fait rien. Par exemple, un processus peut attendre un événement pour redevenir *Actif*, comme par exemple, que l'on appuie sur une touche lors de l'affichage d'un message.
- **Zombie** : un processus zombie est un processus terminé, mais le système ou le processus parent n'en a pas été informé. L'état d'un processus peut être modifié par un autre processus, par lui-même ou par l'utilisateur.

1.2.2. Quelques Commandes

Actions sur les fichiers et répertoires

Se déplacer dans l'arborescence :

- savoir où je me situe : `pwd` ;
- aller vers : `cd [répertoire]`.

Lister les fichiers et les droits : `ls [-la] [fichier...] [répertoire...]`.

Lister les ACLs : `getfacl [fichier...] [répertoire...]`.

Créer/supprimer un répertoire :

- créer un répertoire : `mkdir [-p] <répertoire...>` ;
- supprimer un répertoire (déjà vide) : `rmdir <répertoire...>`.

Copier, renommer, déplacer :

- copier : `cp [-fr] <source1>... <destination>` ;
- renommer : `mv <source> <destination>` ;
- déplacer : `mv <source1>... <destination>`.

Liens physiques, liens symboliques : `ln [-s] <origine> <destination>`.

Manipuler les droits & les propriétaires :

changer les droits : `chmod [-R] [MODE|MODE-OCTAL] <fichier...> <répertoire...>` ;

changer le propriétaire : `chown [-R] <user>[.<group>] <fichier...> <répertoire...>` ;

changer le groupe : `chgrp [-R] <group> <fichier...> <répertoire...>` ;

changer les ACLs : `setfacl [-R] -m <u|g|o>:<utilisateur|group>:<droit> <répertoire...>`.

Gestion des processus

Voir l'état des processus :

- à un instant T : `ps [auxef...]` ;
- visualisation dynamique : `top`.

Arrêt d'un processus : `kill [-Num_Sig] <PID...>`.

Autres commandes diverses

passwd : permet de changer le mot de passe d'un utilisateur système (il ne permet pas de changer les mots de passe des utilisateurs dans un annuaire LDAP)

`passwd` sans option modifie le mot de passe de l'utilisateur courant.

`passwd nom_d_utilisateur` permet de changer le mot de passe d'un autre utilisateur.

Si la commande est exécuté par un utilisateur autre que "root" le mot de passe actuel sera demandé.

sort : trier des lignes en fonction d'une ou plusieurs clés : `sort [-ndtX] [-k num_champs] fichier...`.

grep : rechercher des chaînes de caractère dans un ou plusieurs fichiers : `grep [-vni] chaîne fichier...`.

cut : extraire des colonnes d'un ou plusieurs fichiers : `cut -f <nombre> [options] fichier...`.

wc : déterminer le nombre de lignes, mots ou caractères dans un ou plusieurs fichiers : `wc [-lwc] fichier...`.

tail et head : visualiser les dernières ou les premières lignes d'un fichier :

- `tail [-n] fichier` ;
- `head [-n] fichier` .

screen : multiplexeur de terminaux en mode texte. Il permet de détacher un terminal et de le récupérer en cas de déconnexion. Ce logiciel est particulièrement adapté aux travaux à distance, en cas de coupure réseau il est possible de reprendre la main dessus le serveur. Voici le fonctionnement de base :

- lancer un nouveau terminal : `screen` ;
- détacher ce terminal : `ctrl a d` ;
- re-attacher le terminal : `screen -rd` .

1.2.3. Les conteneurs

Pour gérer les conteneurs, différentes commandes sont disponibles :

- installation d'un paquet dans un conteneur : `apt-eole install-conteneur (nom_du_conteneur) paquet`
- statut de tous les conteneurs : `lxc-status` ;
- arrêt de tous les conteneurs : `service lxc stop` ;
- démarrage de tous les conteneurs : `service lxc start` ;
- arrêt d'un conteneur : `lxc-halt -n (nom_du_conteneur)` ;
- forcer l'arrêt d'un conteneur : `lxc-stop -n (nom_du_conteneur)` ;
- démarrage d'un conteneur : `lxc-start -n (nom_du_conteneur) -d`
- entrer dans un conteneur : `ssh (nom_du_conteneur)` .

Les conteneurs seront installés dans le répertoire `/opt/lxc/`, mais, normalement, il n'est pas nécessaire de modifier les fichiers directement dans ce répertoire.

1.2.4. La gestion des onduleurs

Quelques commandes utiles :

- test d'une installation sans démarrer le service upsd : `upsdrcvtl start` ;
- test de l'arrêt du serveur sans avoir à attendre que la batterie soit vide : `upsmon -c fsd` ;
- lister la configuration : `upsc eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur) ;

- modifier la configuration : `upsw eoleups@localhost` (où "eoleups" est un nom choisi arbitrairement pour la configuration de l'onduleur).

1.2.5. Les manuels

L'organisation du man

L'ensemble du man est organisé en sections numérotées de 1 à 9 pour les plus courantes :

1. commandes utilisateurs pouvant être exécutées quelque soit l'utilisateur
2. appels systèmes, c'est-à-dire les fonctions fournies par le noyau
3. fonctions des bibliothèques
4. périphériques, c'est-à-dire les fichiers spéciaux que l'on trouve dans le répertoire /dev
5. descriptions des formats de fichiers de configuration (comme par exemple /etc/passwd)
6. jeux
7. divers (macros, conventions particulières, ...)
8. outils d'administration exécutables uniquement par le super utilisateur (root)
9. autre section (spécifique à GNU/Linux) destinée à la documentation des services offerts par le noyau

Lorsque la documentation est interrogée à propos d'un terme présent dans plusieurs sections (ex : `passwd`), à la fois commande et fichier de configuration), si le numéro de section n'est pas précisé, c'est toujours la section de numérotation la moins élevée qui sera affichée.

Contenu d'une page

Chaque page de man est structurée en paragraphes contenant des éléments particuliers.

Intitulé de la commande ou du fichier et section du manuel

Vérifier qu'il s'agit de la documentation attendue.

Exemple :

- `CP(1) Manuel de l'utilisateur Linux CP(1)`

documentation pour la commande cp, section 1

- `PASSWD(5) Manuel de l'administrateur Linux PASSWD(5)`

documentation pour le fichier passwd, section 5

Nom

comme son nom l'indique, il s'agit du nom de la commande ou du fichier ainsi que d'une description synthétique.

Exemple :

- `NOM`
`cp - Copier des fichiers.`

Synopsis

Dans ce paragraphe, on retrouve la syntaxe d'une commande, c'est-à-dire l'ensemble des options et

arguments disponibles.

Quelques précisions pour bien lire cette syntaxe : si à première vue elle peut paraître rébarbative, elle dit tout au sujet de la manipulation d'une commande.

Exemple :

- `cp [options] fichier chemin`
Options GNU (forme courte) : `[-abdfilprsvxPR]`

la commande `cp` accepte des options (introduites par un "-") et des arguments (sans "-").

Les éléments spécifiés entre crochets sont facultatifs pour le fonctionnement de la commande.

Au contraire, les éléments indiqués sans crochets sont obligatoires et, s'ils sont omis, provoqueront une erreur.

Lorsque les options sont indiquées dans les mêmes crochets, elles peuvent être combinées. Dans le cas contraire, elles sont incompatibles et devront être utilisées séparément.

Enfin les options peuvent être abrégées (ex : `-f`) ou complètes (ex : `--force`), la signification est la même et elle est développée dans le paragraphe [description](#).

Description

Cette section du man détaille la totalité des options et arguments d'une commande, ou les éléments d'un fichiers de configuration.

Fichiers

Dans ce paragraphe, vous trouverez une liste de fichiers intéressants à consulter, en complément d'information pour une commande ou un fichier de configuration.

Voir aussi

(ou "See also")

Comme son nom l'indique, il s'agit d'une liste de commandes, fichiers, appels système... auquel on renvoie le lecteur pour compléter son information

Exemple :

- `VOIR AUSSI`
`passwd(1), login(1), group(5), shadow(5).`

Cette page propose ici de consulter les commandes `passwd` et `login` dans la section 1 et les fichiers `group` et `shadow` dans la section 5 de la documentation.

Environnement

ici sont spécifiées les variables d'environnement qu'il est possible de configurer pour le fonctionnement de la commande ou du fichier.

1.2.6. L'éditeur de texte Vim

Qu'est ce que Vim ?

Vim est un éditeur de texte libre. Il est à la fois simple est puissant.

Il est néanmoins nécessaire de passer par un temps d'apprentissage pour maîtriser l'outil.

Pourquoi Vim ?

L'éditeur est généralement installé de base sur la plupart des distributions. C'est un logiciel stable et éprouvé.

L'éditeur peut être lancé directement sans interface graphique. Il est ainsi possible d'exécuter depuis le serveur.

De plus, Vim est pré-configuré par l'équipe EOLE. Il n'y aura pas de problème de balise de fin de ligne, de nombre d'espace lors de l'indentation, ... Problème qu'il est possible de rencontrer avec d'autres éditeurs.

1.2.6.a. Les modes Vim

Introduction

Vim utilise un système de "modes". Ce concept de base est indispensable pour comprendre le fonctionnement du logiciel.

Vim est un éditeur entièrement accessible au clavier. Un ensemble de commande permet d'accéder à un ensemble de fonctionnalité. Pour que l'éditeur distingue la saisie de commande (le mode "normal") et la saisie de texte (le mode "insertion"), différents modes sont utilisés.

Il existe également le mode "visuel" permettant de sélectionner une zone de texte où sera appliquée un ensemble de commande.

Cette distinction n'existe pas, généralement, dans les autres éditeurs. Ils utilisent alors des entrées dans un menu graphique ou des raccourcis clavier à la place du mode "normal".

Comparé au mode graphique, le mode commande ne nécessite pas l'usage de la souris pour rechercher le bon menu. Par rapport aux raccourcis clavier, le mode commande est souvent plus facile à se rappeler (write pour écrire).

Passage d'un mode à l'autre

Pour passe au mode "normal", il suffit de taper la touche **Echap** ou **Esc**.

Pour passer au mode "insertion" (depuis le mode "normal") :

- insérer avant le curseur : **i** (ou la touche **Inser** du clavier) ;
- insérer après le curseur : **a** ;
- insérer en début de ligne : **I** ;
- insérer en fin de ligne : **A** ;
- insérer une ligne après : **o** ;
- insérer une ligne avant : **O** ;
- supprime pour remplacer un (et un seul) caractère : **s** ;
- supprime pour remplacer la ligne complète : **S** ;
- remplacer un caractère : **r** ;
- remplacer plusieurs caractères : **R** ;

Pour passer au mode "visuel" (depuis le mode "normal") :

- sélection caractère par caractère : **v** ;
- sélection ligne par ligne : **V** ;

- sélection colonne par colonne : `ctrl v` .

1.2.6.b. Première prise en main

Exécuter Vim

Pour exécuter Vim, il suffit de taper `vim` dans l'interpréteur de commande. Il est aussi possible d'ouvrir directement un fichier en faisant `vim fichier.txt` .

Ouvrir un fichier

En mode normal, taper : `:edit fichier.txt` (ou `:e fichier.txt`).

Insérer du texte

Passer en mode insertion : `i` et taper votre texte.

Enregistrer le texte

Quitter le mode insertion : `esc` .

Enregistrer le texte : `:write` (ou `:w`).

Quitter l'éditeur

Pour quitter l'éditeur : `:quit` (ou `:q`).

Vim créé un "buffer" lorsque l'on édite un fichier. Cela signifie que l'on ne modifie pas directement le fichier. Il faut sauvegarder les changements sous peine de perdre les modifications.

Le buffer est sauvegardé de façon fréquente dans un fichier "swap" (généralement `.fichier.txt.swp`). Ce fichier est supprimé lorsqu'on enregistre ou ferme le document.

1.2.6.c. Les déplacements

- se déplacer d'un caractère vers la gauche : `h` ;
- se déplacer de 20 caractères vers la gauche : `20h` ;
- se déplacer d'une ligne vers le bas : `j` ;
- se déplacer de 20 lignes vers le bas : `20j` ;
- se déplacer d'une ligne vers le haut : `k` ;
- se déplacer d'un caractère vers la droite : `l` ;
- se déplacer au début du prochain mot : `w` ;
- se déplacer au début de deux mots : `2w` ;
- revenir au début du mot précédent : `b` ;
- se déplacer à la fin du prochain mot : `e` ;
- se déplacer à la prochaine phrase : `)` ;
- revenir à la phrase précédente : `(` ;

- se déplacer au prochain paragraphe : `}` ;
- revenir au paragraphe précédent: `{` ;
- revenir au début de la ligne : `^` ;
- aller à la fin de la ligne : `$` ;
- remonter d'un écran : `pgup` ;
- descendre d'un écran : `pgdown` ;
- descendre à la fin du fichier : `G` ;
- aller à la ligne 20 : `20G` ;
- aller au début de la page courante : `H` ;
- aller au milieu de la page courante : `M` ;
- aller à la fin de la page courante : `L` ;
- revenir à l'emplacement précédent : `ctrl o` ;
- aller à l'emplacement suivant : `ctrl i` ;
- la troisième occurrence de la lettre "e" : `3fe` ;

Il est possible de "marquer" des positions dans le texte. Cela permet de revenir très facilement à cet emplacement plus tard.

Pour cela, il faut utiliser la commande `m` suivi du nom de la marque (c'est à dire une lettre). Par exemple : `ma`. Pour revenir à la marque, il suffira de taper : `'a`.

1.2.6.d. Recherche et remplacement de texte

Rechercher

- chercher les occurrences EOLE : `/EOLE` ;
- chercher les mots EOLE : `^<EOLE>` ;
- chercher l'occurrence suivante : `n` ;
- chercher l'occurrence précédente : `N` ;
- chercher les autres occurrences du mot sous le curseur : `*` ;
- chercher en arrière les autres occurrences du mot sous le curseur : `ctrl #` ;

Remplacement

- remplacer le mot EOLE par Scribe : `:%s/EOLE/Scribe/g`
- remplacer le mot EOLE par Scribe en demande confirmation : `:%s/EOLE/Scribe/gc`
- remplacer le mot EOLE par Scribe sur les 20 première ligne d'un fichier : `:0,20s/EOLE/Scribe/g`

1.2.6.e. Couper, copier et coller

- couper un texte sélectionné : `d` ;
- couper le caractère sélectionné : `x` ;

- couper les deux caractères suivants : `d2l` ;
- couper un mot : `dw` ;
- couper la ligne courante : `dd` ;
- couper 2 lignes : `d2` ;
- couper le paragraphe : `d}` ;
- copier un texte sélectionné : `y` ;
- coller le texte après : `p` .
- coller le texte avant : `P` ;

1.2.6.f. Le mode fenêtre

Ouvrir plusieurs fenêtres

Il est possible d'ouvrir plusieurs fichiers en même temps.

Pour cela, il suffit de lancer plusieurs fois la commande `:e nomdufichier` .

Pour passer d'un buffer à un autre, il suffit de taper `:bn` (n étant le numéro du buffer).

Ouvrir plusieurs tabulations

Pour ouvrir le fichier dans une nouvelle tabulation : `:tabedit fichier.txt` .

Pour se déplacer de tabulation en tabulation, il suffit d'utiliser `ctrl alt pgup` et `ctrl alt pgdown` .

Voir plusieurs fichiers

Il est possible de voir plusieurs fichiers dans la même interface.

Pour cela, il faut créer un nouveau buffer en tapant `:new` et ensuite ouvrir le nouveau fichier : `:e fichier.txt` .

Pour se déplacer dans les buffers, il faut utiliser le raccourci `ctrl w` et les touches de déplacement `hjkl` .


Pour se déplacer de buffer en buffer, il est possible également de taper deux fois `ctrl w` .

Il est ensuite possible de déplacer les fenêtres horizontalement et verticalement avec `ctrl w` et les touches de déplacement en majuscule `HJKL` .

Pour fermer une fenêtre, il suffit de faire `:q` .

Voir plusieurs fois le même fichier

Il est possible d'ouvrir plusieurs fois le même buffer en faisant `ctrl w s` . Cela permet de voir simultanément plusieurs parties du même texte.

 Dans ce cas, il s'agit du même buffer. Une modification dans une vue sera automatiquement reporter dans les autres vues.

Système de fichiers

Il est possible d'ouvrir une fenêtre de système de fichiers en faisant : `:Sex` ou `:Vex` .

1.2.6.g. Autres

Complétion automatique

La complétion permet de compléter un mot automatiquement à partir d'une liste de mot présent dans le texte en court d'écriture. Il est souvent utile pour ne pas faire d'erreur dans le nom des fonctions.

Pour l'utiliser, il suffit de commencer a écrire le début du mot et faire `ctrl n` ou `ctrl p`.

Annuler et refaire

Pour annuler la dernière action : `u` ;

Pour revenir sur l'annulation : `ctrl r`.

Passer un texte en majuscule

Pour passer un texte en majuscule, il suffit de taper `~` ou `maj u`.

Voir la différence entre les fichiers

Vim permet également de voir la différence entre deux textes. Pour cela, il suffit de lancer en ligne de commande :

```
vimdiff nomdufichieroriginal.txt nomdufichiermodifier.txt
```

1.2.6.h. Liens connexes

<http://www.vim.org/>

http://www.swaroopch.com/notes/Vim_fr:Table_des_Mati%C3%A8res

https://svn.timetombs.org/svn/doc-keymap/doc-keymap-cheat_sheet-vim-azerty_fr.pdf [https://svn.timetombs.org/svn/doc-keymap/doc-keymap-cheat_sheet-vim-azerty_fr.pdf]

1.2.7. Les commandes à distance avec SSH

1.2.7.a. Le protocole SSH

SSH^[p.561] (Secure Shell) est un protocole de communication sécurisé. Il permet différentes actions comme l'authentification à distance, l'exécution de commande à distance ou le transfert de fichier.

Le protocole est chiffré par un mécanisme d'échange de clés de chiffrement effectué au début de la connexion.

Le transfert de fichier d'une machine à une autre se fait par un protocole proche de FTP^[p.548]. La différence étant que les transferts du client et du serveur se font par un tunnel chiffré.

1.2.7.b. SSH sous GNU/Linux

Connexion à distance

Le client SSH est installé par défaut sur la plupart des distributions. Si ce n'est pas le cas, il faut installer un paquet dont le nom est généralement "openssh-client".

Une fois installé, il est possible d'ouvrir une session à distance de la manière suivante :

```
ssh utilisateur@ip_serveur
```

Si vous ne spécifiez pas de nom d'utilisateur, c'est l'utilisateur courant de votre session GNU/Linux qui sera utilisé.

Pour lancer des applications graphiques, il faudra le préciser dans la commande ssh en rajoutant l'option -X :

```
ssh -X utilisateur@ip_serveur.
```

A la première connexion, le message suivant apparaît :

```
Warning: Permanently added 'xxxxx' (RSA) to the list of known hosts.
```

Cela signifie qu'on ne s'est jamais connecté sur cette station et qu'un identifiant est ajouté à la liste des hôtes connus.

Il peut arriver que le certificat du serveur change (par exemple en cas de réinstallation).

Le message suivant apparaîtra :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
```

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

```
It is also possible that the RSA host key has just been changed.
```

```
The fingerprint for the RSA key sent by the remote host is
```

```
65:6d:9d:c0:78:f7:60:bf:13:86:59:16:53:07:3b:a4.
```

```
Please contact your system administrator.
```

Add correct host key in /home/xxx/.ssh/known_hosts to get rid of this message.

```
Offending key in /home/xxx/.ssh/known_hosts:12
```

```
Password authentication is disabled to avoid man-in-the-middle attacks.
```

Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.

X11 forwarding is disabled to avoid man-in-the-middle attacks. Permission denied (publickey,password).

Ce message nous apprend plusieurs choses :

- le serveur ssh a une clef différente de celle de notre dernier passage ;
- le fichier contenant les hôtes connus est `/home/xxx/.ssh/known_hosts` ;
- l'identifiant de l'hôte est spécifié à la ligne 12 (Offending key in /home/xxx/.ssh/known_hosts:12).

Si vous êtes sûr que l'hôte est le bon, il vous suffira de supprimer la ligne 12 du fichier known_hosts et de relancer une connexion.

Il faudra spécifier le mot de passe de l'utilisateur pour se connecter.

Ssh propose également la connexion par échange de clef. Cela permet de se connecter à distance sans connaître le mot de passe de l'utilisateur.

L'échange de clef peut être réalisé par l'intermédiaire d'un serveur Zéphir. Pour plus d'informations, consulter la documentation spécifique à ce module.

Exécution de commande à distance

Une fois connecté à distance, vous pouvez lancer n'importe quelle action comme si vous étiez en local.

Transfert de fichier à distance

Pour envoyer un fichier sur un serveur, il faut faire :

```
scp nom_du_fichier utilisateur@ip_serveur:/repertoire/de/destination/
```

Pour récupérer un fichier d'un serveur :

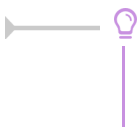
```
scp utilisateur@ip_serveur:/repertoire/source/nom_du_fichier
/repertoire/de/destination/
```

Pour récupérer un répertoire d'un serveur :

```
scp -r utilisateur@ip_serveur:/repertoire/ /repertoire/de/destination/
```

Enfin, il est possible d'avoir un shell proche de la commande FTP en faisant :

```
sftp utilisateur@ip_serveur
```



Sur la plupart des gestionnaires de fichier disponibles sous GNU/Linux, il est possible de faire des transferts de fichier avec SSH graphiquement (logiciel Filezilla par exemple).

1.2.7.c. SSH sous Windows

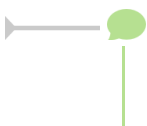
Exécution de commande à distance

Putty est un logiciel libre implémentant un client Telnet^[p.562] et SSH^[p.561] pour Unix et Windows.

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Dans l'environnement EOLE, il permet de se connecter à un serveur à distance depuis un poste Windows et, ainsi, pouvoir exécuter des commandes.

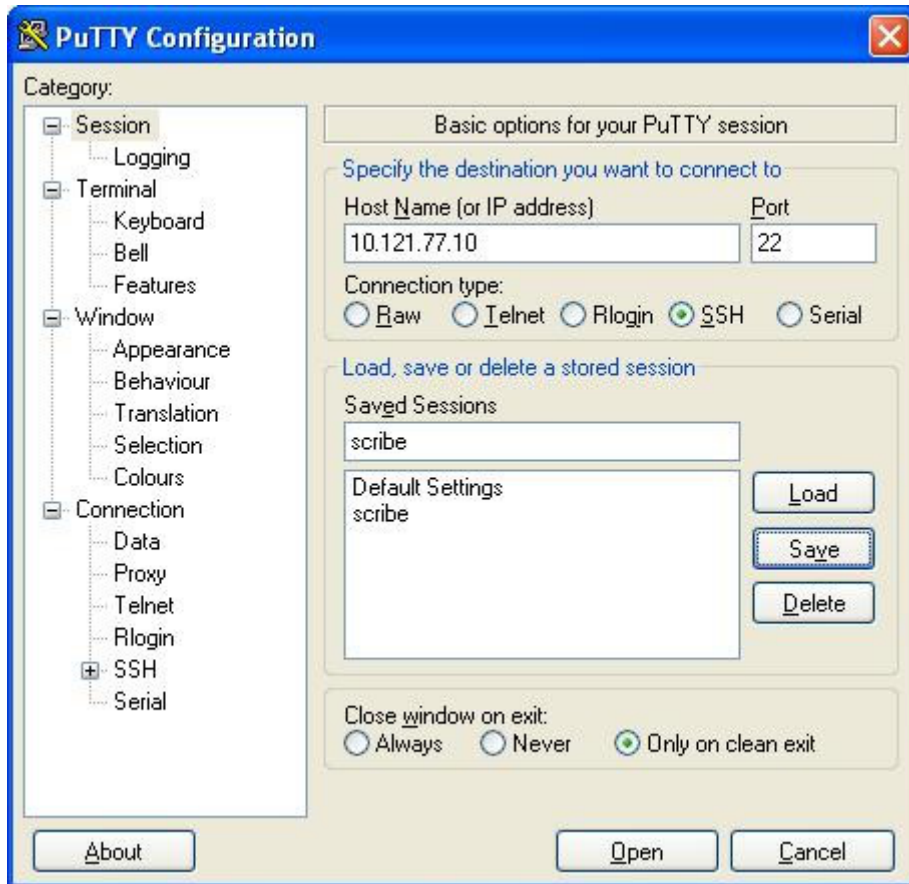
La connexion avec Putty au serveur se fait en utilisant le protocole SSH.



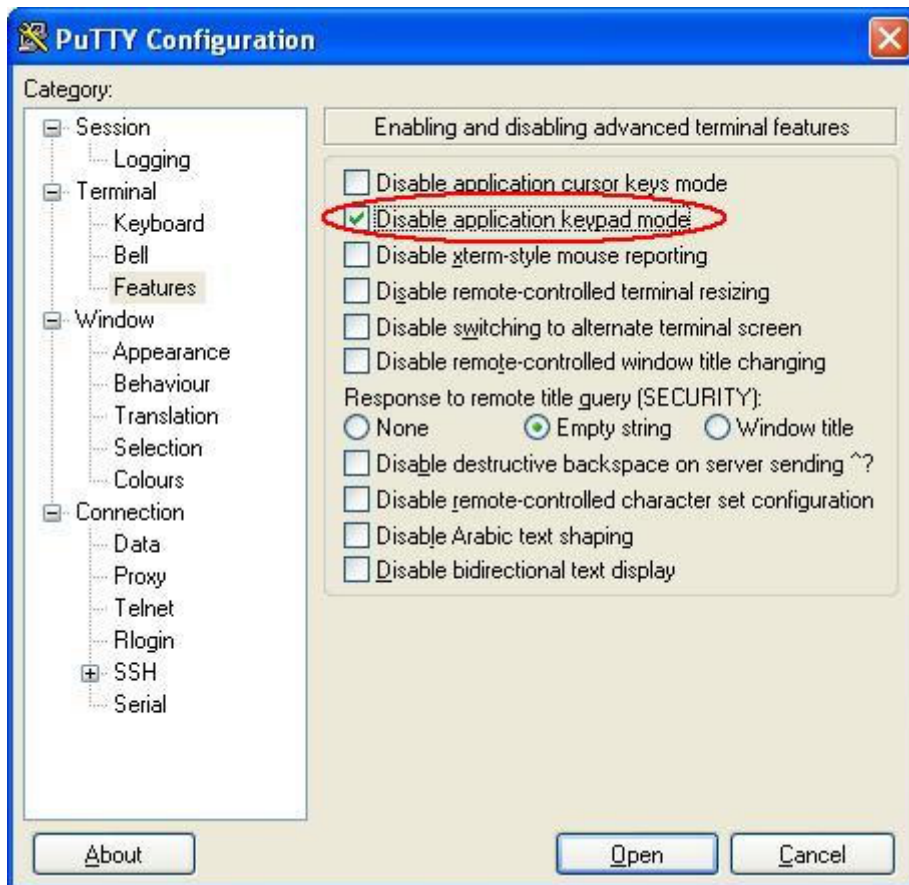
Sur le module Scribe, Putty est pré-installé dans le répertoire personnel d'*admin* (U:\client\putty.exe).

Configuration pour les serveurs EOLE

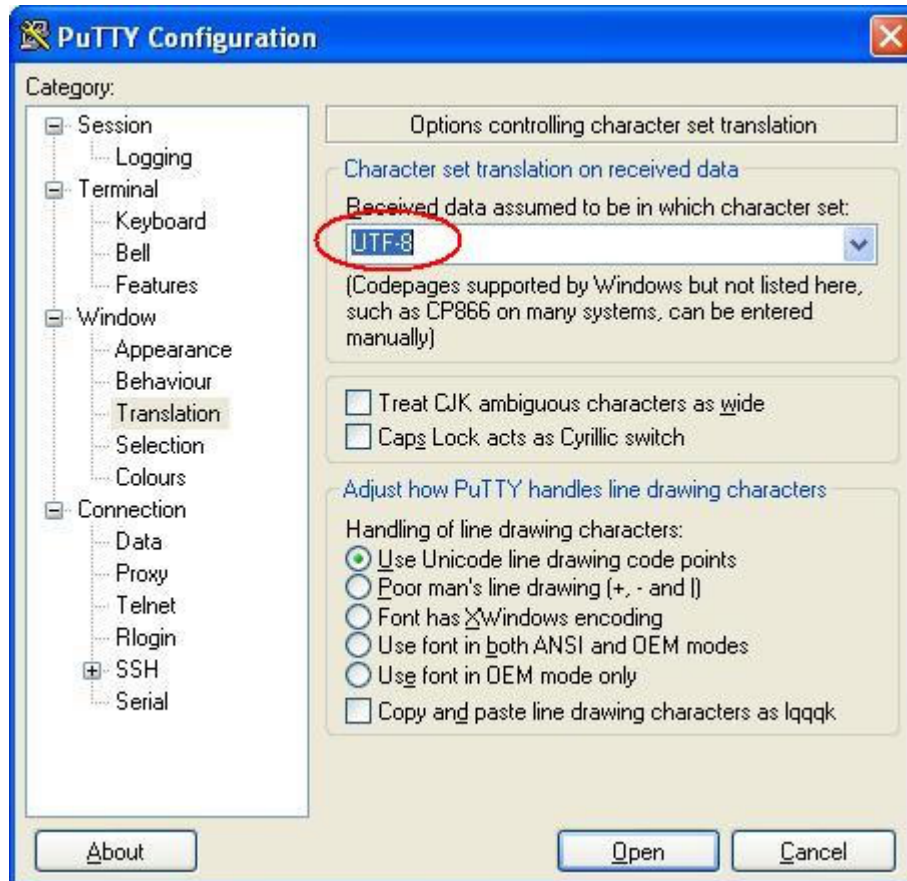
Pour obtenir un meilleur environnement de travail, la configuration par défaut de Putty doit être modifiée.



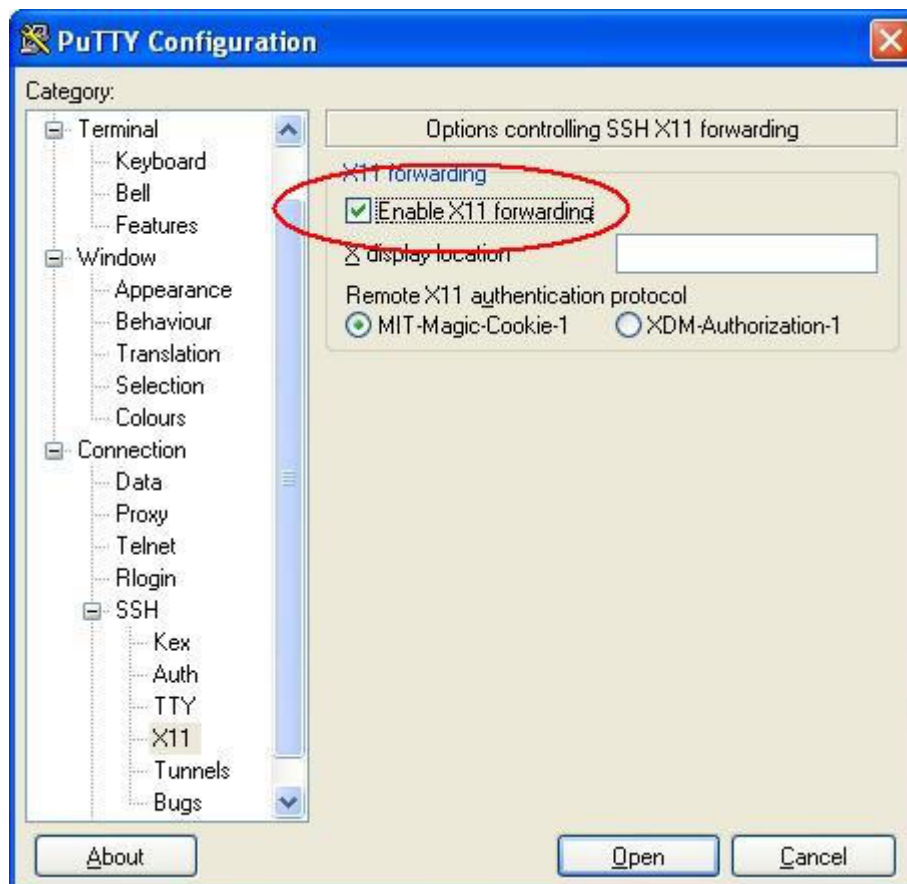
Fenêtre principale



Permettre au pavé numérique de fonctionner correctement (dans "vim" par ex.)



Permettre aux accents de s'afficher normalement

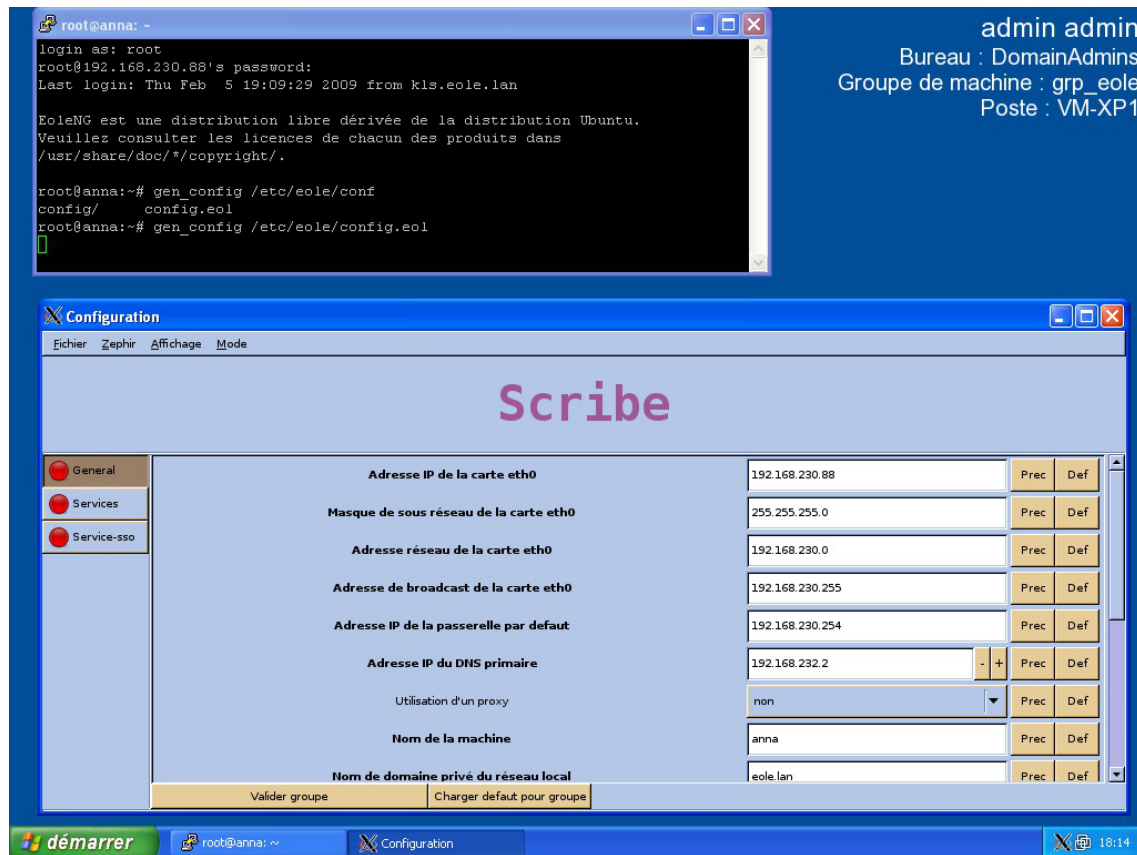


Pouvoir lancer des applications graphique du serveur depuis la station (Ex. "gen_config")

La dernière capture montre comment autoriser la redirection des applications graphiques vers votre poste.

Cependant vous devrez utiliser Xming [<http://sourceforge.net/projects/xming>].

C'est un logiciel libre permettant d'émuler un serveur X [http://fr.wikipedia.org/wiki/X_Window] vers lequel sera redirigé l'application graphique lancée à travers ssh sur le serveur EOLE.



Lancement de "gen_config" sur un poste Windows

Transfert de fichier à distance

Il existe une interface graphique de transfert de fichier à distance. Il s'agit de WinSCP.

On utilise le logiciel comme un client FTP normal.

1.2.8. Quelques références

- Le site du Kernel Linux : <http://www.kernel.org> ;
- Le projet GNU : <http://www.gnu.org> ;
- Site réputé pour ses documentations et son forum d'entraide : <http://www.lea-linux.org/> ;
- Guide de survie du débutant : <http://www.delafond.org/survielinux/> ;
- Un manuel en ligne (man) : <https://www.tldp.org/guides.html> ;
- Définitions sur Wikipédia :
 - Noyau Linux : http://fr.wikipedia.org/wiki/Noyau_Linux,
 - Projet GNU : <http://fr.wikipedia.org/wiki/GNU>,
 - Distribution : http://fr.wikipedia.org/wiki/Distribution_Linux,
 - Les Permissions Unix : http://fr.wikipedia.org/wiki/Permissions_Unix.

1.3. Reconfiguration

Suite à un diagnostic, à une modification de la configuration ou à une mise à jour, il est nécessaire de reconfigurer le serveur.

On réalise cette opération avec la commande `reconfigure`, plutôt qu'avec la commande `instance`.

Les différentes valeurs attribuées aux variables sont enregistrées dans un fichier `config.eol` au format JSON^[p.550] dans le répertoire `/etc/eole/`.

Il convient donc de réaliser les modifications sur ce fichier en utilisant l'interface de configuration du module.



Un fichier `config.eol.bak` est 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.

À chaque reconfiguration du serveur, si la configuration a changé, un fichier `config.eole.bak.1` est généré. Celui-ci est une copie de l'avant-dernière configuration fonctionnelle.

S'il existe une différence entre les fichiers `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Reconfigure

Cette commande `reconfigure` sert à appliquer un changement de configuration (par exemple, le changement d'adressage IP) ou à appliquer des changements apportés par la mise à jour d'un ou de plusieurs paquets.

Avec `Maj-Auto`, un message indique s'il est nécessaire de lancer `reconfigure`.

Cette commande :

- ré-applique le SID^[p.560] trouvé dans l'annuaire sur les modules Horus et Scribe ;
- supprime des paquets (utilisé pour les noyaux notamment) ;
- exécute les scripts pre et postreconf ;
- met à jour les valeurs par défaut des dictionnaires ;
- recrée le compte `admin` s'il n'a pas été trouvé (modules Scribe et Horus) ;
- copie, patch^[p.558] et renseigne les templates ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (redémarrage automatique si mise à jour par EAD) ;
- relance les services.

Lors d'une mise à jour via l'EAD^[p.545], `reconfigure` est lancé automatiquement. Si la mise à jour a été effectuée sur la console ou via SSH avec la commande `Maj-Auto` un message indique s'il est nécessaire de lancer `reconfigure`.

reconfigure is not instance : pourquoi reconfigure au lieu d'instance

La commande `instance` est exécutée à l'installation d'un nouveau serveur.

Cette commande :

- initialise les mots de passe des comptes `root`, `eole` et `admin` ;
- propose de créer des comptes d'administration supplémentaires ;
- génère un nouveau SID ;
- génère l'annuaire et les bases MySQL si inexistantes ;
- lance des commandes spécifiques à l'instanciation ;
- copie, patch et renseigne les templates ;
- (re)lance les services ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD).



Il existe plusieurs contre-indications à l'utilisation de la commande `instance` sur un serveur déjà instancié :

- les commandes exécutées peuvent être différentes ;
- la commande `instance` demande une interaction tandis que `reconfigure` est automatique, il ne pose pas de question et est donc plus rapide ;
- l'interaction est source d'erreur (possibilité d'écrasement de l'annuaire ou des bases de données). Sur les modules Scribe et Horus si l'utilisateur répond oui à la question concernant la re-génération de l'annuaire, tous les comptes utilisateurs et les stations intégrés au domaine sont effacés.

1.4. L'interface d'administration EAD

EOLE offre une interface simplifiée de gestion du serveur : l'interface d'administration EAD.



Accueil EAD outil d'administration

Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

1.4.1. Principe général

L'EAD (Eole ADmin) est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible avec un navigateur à l'adresse `https://<adresse_module>:4200`.

L'EAD est composé de deux parties :

- un serveur de commandes (**ead-server**), présent et actif sur tous les modules ;
- une interface (**ead-web**), désactivable depuis l'interface de configuration du module dans l'onglet **Services** en passant Activer l'interface web de l'EAD à non.

Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, Sentinelle, ...) ne disposent que de la **version de base** qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...).

Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.



Accueil EAD outil d'administration

★ Aide

Un point d'interrogation est accessible en bas à droite de certaines pages, il permet d'afficher une aide associée.



1.4.2. Premier pas dans l'administration d'un serveur

Lorsque vous vous êtes connecté sur un serveur de commandes, vous avez quatre éléments :



Page d'accueil lors de la connexion à un serveur

1. la gondole d'administration ;
2. le menu d'action (propose les actions auxquelles vous avez accès) ;
3. les onglets (les serveurs enregistrés sur l'interface) ;
4. la partie centrale ou espace de travail (il s'agit de la partie venant du serveur de commandes).

1 - La gondole d'administration

Elle permet d'accéder aux actions de base de l'interface (ajout/suppression de serveur, déconnexion, retour vers l'accueil, choix de la feuille de style CSS, connexion locale).

2 - Le menu d'action

Il permet d'accéder aux actions disponibles sur le serveur de commandes.

3 - Les onglets (les serveurs enregistrés sur l'interface)

Ils permettent d'accéder aux divers serveurs EOLE enregistrés sur l'interface.

4 - La partie centrale ou espace de travail

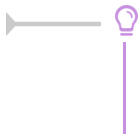
Les éléments affichés dans cette partie viennent du serveur de commandes.

C'est un conteneur pour les actions (sous forme de rapport, formulaire ...).

La page d'accueil d'un serveur de commandes affiche les rapports de :

- mise à jour (sur tous les modules) ;
- mise à jour de listes de sites interdits sur le module Amon ;
- sauvegarde Bareos sur les modules Horus et Scribe ;
- importation sur le module Scribe.

Elle affiche également les diodes d'état du serveur (agents Zéphir).



Les agents Zéphir peuvent être consultés directement en utilisant l'adresse :

`http://<adresse module>:8090`

Voir aussi...

Surveillance de l'état du serveur [p.304]

1.4.3. Ajout/suppression de serveurs

Il est possible de connecter plusieurs serveurs de commandes à une même interface. Une seule interface sert alors à administrer l'ensemble des serveurs EOLE d'un établissement.

Ajout/suppression de serveurs de commandes dans l'interface

L'interface de l'EAD est une coquille vide.

Elle permet de se connecter à des serveurs de commandes qui proposent des actions.

Lors de l'instanciation du serveur, le serveur de commandes du serveur est enregistré auprès de son interface.

La coquille n'est pas laissée vide.

Il est possible d'enregistrer plusieurs serveurs EOLE sur l'interface.

On obtient ainsi un point d'entrée unique pour administrer l'ensemble des serveurs d'un établissement.

Une seule interface web dans laquelle chaque onglet représente un des serveurs.

Il est ensuite possible de gérer les accès ainsi que les actions autorisées par utilisateur ou par groupe.

Ajout de serveur

Dans la gondole d'administration, cliquer sur **Ajouter serveur** et renseigner :

- l'IP du serveur ;
- le port du serveur de commandes (4201) ;
- le nom à afficher dans l'onglet ;
- le nom de l'utilisateur `eole` du serveur de commandes à enregistrer ;
- le mot de passe correspondant (sur le serveur à enregistrer).

Administration

- Accueil
- Recharger
- Ajouter Serveur
- Supprimer Serveur
- Déconnexion

Choix de la position du menu:
main1.css

Authentification Locale

amonecole

AJOUTER UN SERVEUR

IP du serveur (pas de https): 192.168.230.197

Port du serveur de commande [4201] 4201

Nom du serveur (afficher dans le menu) monscribe

Login (local sur le serveur cible) eole

Mot de passe

Ajouter

Aide

Ajout d'un serveur dans l'interface



Le compte `root` peut être utilisé à la place du compte `eole` pour toutes les manipulations présentées ici.

Suppression de serveur

Suppression normale

C'est le mécanisme de suppression classique. L'onglet du module est vert et on souhaite le retirer.

Dans la gondole d'administration, cliquer sur **Supprimer Serveur** :

- choisir le serveur à supprimer ;
- entrer le login `eole` du serveur de commandes à désinscrire ;
- entrer le mot de passe ;
- valider.

Administration

- Accueil
- Recharger
- Ajouter Serveur
- Supprimer Serveur
- Déconnexion

Choix de la position du menu:
main1.css

Authentification Locale

amonecole **monscribe**

SUPPRIMER UN SERVEUR

serveur à supprimer 2 - monscribe (https://192.168.230.197:4201)

Login (local) eole

Mot de passe

Forcer la désinscription (non recommandé)

Supprimer

Aide

Suppression d'un serveur

La référence sera supprimée côté interface et côté serveur de commandes.

Suppression forcée

Il ne faut utiliser la suppression forcée du serveur que si l'onglet est rouge ou que le mot de passe du serveur de commandes à supprimer est inconnu.

Il est préférable d'utiliser la suppression normale d'un serveur.

Dans la gondole d'administration, cliquez sur **Supprimer Serveur** :

- choisir le serveur à supprimer ;
- entrer le login (utilisez le compte `eole` du serveur de l'interface et non celui du serveur de commandes à désinscrire) ;
- entrer le mot de passe ;
- cocher la case **Forcer la désinscription** ;
- valider.

Suppression forcée d'un serveur

La référence ne sera supprimée que du côté de l'interface.

💡 Désinscription forcée suite à un changement d'adresse IP

Si vous avez modifié l'adresse IP d'un serveur, il est possible que son onglet devienne rouge dans l'EAD.

Il faut alors utiliser la suppression forcée et ré-enregistrer le serveur.

Complément technique

Les interfaces associées au serveur de commandes local sont enregistrées dans le fichier `/usr/share/ead2/backend/config/frontend_keys.ini`

```
[keys]
127.0.0.1 = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Les serveurs de commandes associés à l'interface EAD locale sont enregistrés dans le fichier `/usr/share/ead2/frontend/config/servers.ini`



```
[11]
url = https://127.0.0.1
port = "4201"
comment = u"amon"
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

1.4.4. Surveillance de l'état du serveur

La page d'accueil d'un serveur de commandes affiche les rapports de :

- mise à jour ;
- mise à jour de listes de sites interdits sur le module Amon ;
- sauvegarde Bareos sur les modules Horus et Scribe ;
- importation sur le module Scribe.

Elle affiche également les diodes d'état du serveur (agents Zéphir).

Les remontés des agents Zéphir sont classés dans 3 catégories : Système, Services et Utilisation.

1.4.4.a. Système

Quelques agents sont fournis de base et sont commun à tous les modules :

- Informations systèmes
- Occupations des disques
- Statistiques réseau
- État des sommes MD5 de paquets

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- Onduleur

> Surveillance de l'état des sommes MD5 des paquets

L'outil `eole-debsums` permet de surveiller les modifications apportées aux fichiers présents sur les modules EOLE grâce à la vérification des sommes de contrôle MD5^[p.553] des paquets installés.



Les fichiers de configuration (en général ceux situés dans `/etc`) ne sont pas concernés par cette vérification.

La vérification des sommes de contrôle est exécutée toutes les nuits via une commande cron^[p.544].

La commande suivante permet de forcer la vérification des MD5 (compter entre 1 et 2 minutes) :

```
/usr/share/eole/debsums/eole-debsums.sh
```

Rapport et suivi des modifications

La commande suivante affiche un rapport d'exécution :

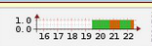
```
1 root@amon:~# /usr/share/eole/debsums/show-reports.py
2 Container: root
3 =====
4
5 Filename: /var/log/eole-debsums/report.log
6 Last update: 2018-02-22 11:09:15
7
8 eole-amon:
9   /usr/share/eole/creole/dicos/30_amon.xml
10
11 Ignored by eole
12 -----
13
```

Un agent^[p.540] de surveillance Zéphir permet de surveiller les sommes MD5 des paquets.

État des sommes MD5 de paquets

[Retour](#)

État : Avertissement
 Date de la mesure : 2018-02-22 11:59:19
 Dernier problème (Avertissement) : 2018-02-22 11:09:19
 Intervalle de mesure : 300 s



Surveillance des sommes MD5 des paquets :

Conteneur	État	Nombre de fichiers modifiés
root	●	1

Il permet également de consulter la liste des fichiers signalés comme modifiés.

État des sommes MD5 de paquets pour root

[Retour](#)

État : Avertissement
 Date de la mesure : 2018-02-22 12:05:10
 Dernier problème (Avertissement) : 2018-02-22 12:05:10
 Intervalle de mesure : 7200 s

Surveillance des MD5 des paquets :

Paquet	Fichier
eole-amon	/usr/share/eole/creole/dicos/30_amon.xml

1.4.4.c. Services

Quelques agents sont fournis de base et sont commun à tous les modules :

- État des interfaces réseau
- Services distants
- État des services

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- État des démons bacula

Enfin d'autres agents sont propres à un module en particulier :

- État des tunnels

1.4.4.d. Utilisation

Quelques agents sont fournis de base et sont commun à tous les modules :

- Mise à jour

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

- Sauvegarde

Enfin d'autres agents sont propres à un module en particulier :

- Statistiques Squid
- Statistiques courrier
- Application des règles bastion
- Instance Dansguardian
- Mise à jour antivirus Clam

1.4.5. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur

Le serveur Scribe étant derrière un serveur Amon, la configuration des deux modules permet de faire écouter l'EAD du serveur Scribe sur le port 4203 et donc d'y accéder depuis l'extérieur grâce à une redirection Nginx.

Avantages

Cette configuration présente plusieurs avantages par rapport à la méthode consistant à ajouter le serveurs de commandes du module Scribe dans l'interface EAD du serveur Amon :

- elle ne nécessite pas de déclarer le serveur SSO du serveur Scribe comme source d'authentification de l'EAD du serveur Amon ;
- il n'y a pas de problème d'incompatibilité (templates, protocoles obsolètes, ...) dans le cas où les versions des EAD des deux modules sont différentes ;
- elle simplifie la gestion des certificats.

Configuration côté Scribe

Dans l'interface de configuration du module Scribe, en mode expert, aller dans l'onglet **Ead-web** et passer la variable Activer l'interface web de l'EAD sur un second port à **oui** et vérifier que le port personnalisé est bien le **4203**.

Ead-web

Configuration

Activer l'interface web de l'EAD sur un second port * oui

Port d'accès EAD personnalisé * 4203

Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande `reconfigure` est nécessaire afin que l'EAD écoute sur le port `4203`.

Configuration côté Amon

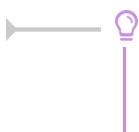
Dans l'interface de configuration du module Amon, aller dans l'onglet `Reverse proxy`, passer la variable `Activer la redirection de l'EAD d'un Scribe` à `oui` puis renseigner l'adresse IP du module Scribe et vérifier que le port renseigné est le `4203`.

Activer la redirection de l'EAD Scribe * oui

IP du Scribe pour la redirection EAD * 10.1.3.5

Port de l'EAD sur le Scribe * 4203

Une fois le module paramétré de cette manière, une reconfiguration du serveur à l'aide de la commande `reconfigure` est nécessaire afin que la redirection soit appliquée.



L'autorisation d'accès au port configuré est gérée par ERA via la directive optionnelle cachée [p.544] : `ead_scribe`.

Voir aussi...

Onglet Ead-web : EAD et proxy inverse

Onglet Reverse proxy : Configuration du proxy inverse

1.4.6. Authentification locale et SSO

Dans l'EAD, il existe deux systèmes d'authentification :

- l'authentification unique (SSO^[p.561]) ;
- l'authentification locale (PAM).

Dans le cas de l'authentification SSO, le serveur de commandes et l'interface se connectent à un même serveur d'authentification.

Pour se connecter en tant qu'*administrateur* :

- authentification SSO : l'utilisateur `admin` de l'annuaire associé au serveur sera utilisé ;
- authentification locale : les utilisateurs `root` et `eole` peuvent être utilisés.

1.4.6.a. Authentification locale

L'authentification locale est un mécanisme plus simple mais moins souple que l'authentification SSO. Il utilise les comptes système de la machine hébergeant le serveur de commandes. Le nombre d'utilisateurs et leur gestion est donc plus limitée.

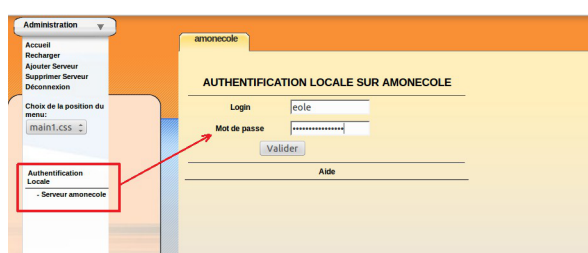
L'authentification locale est systématiquement activée et peut être utilisée conjointement avec l'authentification SSO.

Pour vous authentifier localement, dans la gondole d'administration :

- cliquer sur **authentification locale** ;
- cliquer sur le nom de votre serveur.

Vous accédez alors au formulaire d'authentification locale.

Si le serveur SSO n'est pas activé, vous arriverez sur ce même formulaire en cliquant sur l'onglet.



Formulaire d'authentification locale



Il est possible d'utiliser la gestion des rôles pour déléguer une partie de l'administration à d'autres comptes systèmes.

1.4.6.b. L'authentification SSO

Connexion

Entrer l'adresse `https://<adresse_serveur>:4200` dans le navigateur et cliquer sur l'onglet du serveur à administrer.

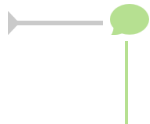
Une re-direction vers le serveur SSO (`https://<adresse_serveur>:8443/`) est effectuée et le formulaire d'authentification apparaît :



Formulaire d'authentification SSO

L'utilisation d'un serveur SSO permet de centraliser l'authentification. En s'authentifiant une seule fois vous pouvez vous connecter aux différents serveurs de commandes enregistrés dans l'interface (naviguer d'un onglet à l'autre).

Les rôles permettent d'utiliser d'autres comptes pour se connecter (ex : sur Scribe, les professeurs ont un rôle prédéfini).



Pour utiliser l'authentification SSO, il est indispensable que le serveur SSO utilisé par l'interface et par les serveurs de commandes qui y sont inscrits **soit identique**.

1.4.7. Redémarrer, arrêter et reconfigurer

Il est possible de redémarrer, arrêter ou reconfigurer un module EOLE directement depuis l'interface d'administration EAD.

Ces actions sont accessibles depuis **Système/Serveur**.



Ces trois actions vous déconnectent de l'EAD.

Redémarrer un serveur



Action de redémarrage d'un serveur

Reconfigurer un serveur



Action de reconfiguration d'un serveur

Arrêter un serveur



Action d'arrêt d'un serveur

1.4.8. Mise à jour depuis l'EAD

Dans **Système / Mise à jour**, l'EAD propose une interface de mise à jour du serveur, il est possible de :

- de lister les paquets disponibles pour la mise à jour ;
- de programmer une mise à jour différée (dans 3 heures par exemple, ou dans 0 heure pour le faire tout de suite) ;
- d'activer / désactiver les mises à jour hebdomadaires (le jour et l'heure de la mise à jour automatique sont déterminés aléatoirement).

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.



Rapport de mise à jour

Penser à consulter le rapport de mise à jour et l'état des services sur la page d'accueil.

Reconfiguration et redémarrage automatique

Une mise à jour lancée depuis l'EAD exécute automatiquement une reconfiguration du serveur avec la commande `reconfigure`, il n'est donc pas nécessaire d'en lancer un par la suite comme c'est le cas depuis la console.

Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

1.4.9. Arrêt et redémarrage de services

Dans l'EAD, il existe deux manières d'arrêt ou de redémarrage des services :

- le mode normal ;
- le mode expert.

1.4.9.a. Redémarrer ou arrêter des services (mode normal)

Pour utiliser la fonctionnalité en mode normal il faut dans un premier temps créer des groupes de services.

Création de groupes de services

Le nom des services, au sens système, n'est pas souvent parlant. Par exemple, il faut savoir que le service `apache2` est le nom du serveur web.

Les groupes de services permettent de regrouper un ou plusieurs services sous une dénomination plus claire. Cela permet de regrouper et donc de faciliter le redémarrage/arrêt de services.

Création un groupe de services nommé `web` :

Pour créer un groupe, cliquer sur le bouton `créer groupe` dans `Système/Editeur de services` :

1. entrer le nom du groupe ;
2. choisir les services du groupe (cocher les cases) ;
3. cliquer sur la flèche verte ;
4. valider avec le bouton `Créer`.

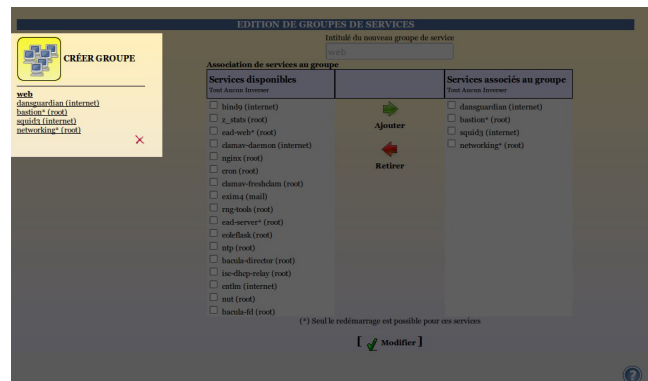


Création d'un groupe de services (1)



Création d'un groupe de services (2)

Une fois créé le groupe de services apparaît sous l'icône CRÉER GROUPE à gauche de l'écran.



Création d'un groupe de services (2)

Un groupe de services peut être modifié en cliquant sur son nom dans la liste de gauche sous l'icône CRÉER GROUPE.

Un groupe de services peut être supprimé en cliquant sur la croix rouge sous son descriptif dans la liste de gauche sous l'icône CRÉER GROUPE.

Redémarrer ou arrêter un groupe de services

Une fois créé, un groupe apparaît dans l'onglet **Système/Services (mode normal)**, il est alors possible de redémarrer ou d'arrêter le groupe de services.



Redémarrage d'un groupe de services

La gestion des rôles permet de déléguer l'accès à des actions, on peut ainsi permettre à la documentaliste de l'établissement de redémarrer le logiciel BCDI.

Tous les groupes de services lui seront néanmoins accessibles.

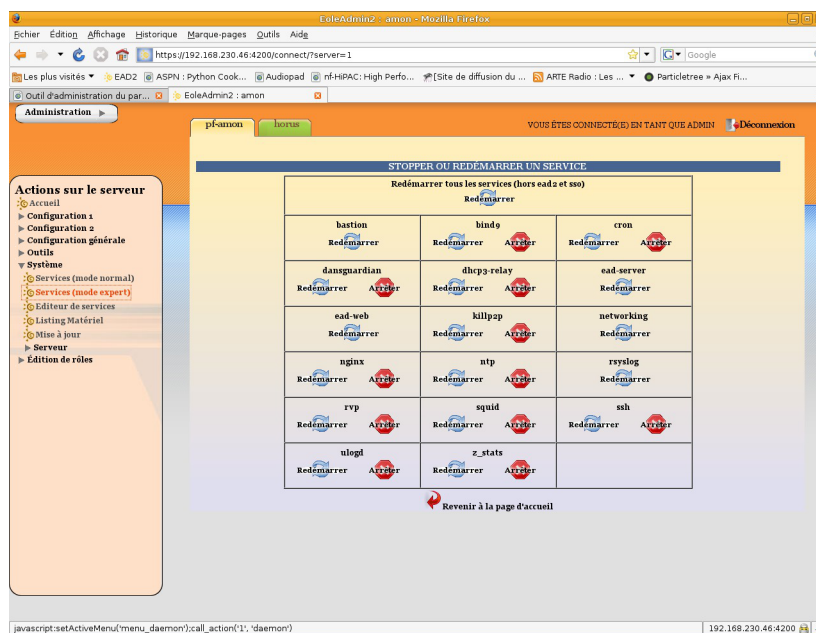
Complément technique

Les groupes de services déclarés dans l'EAD sont enregistrés dans le fichier `/usr/share/ead2/backend/config/simple_services.ini`

```
[amon]
w_____e_____b_____
squid3#internet, networking#root, eole-guardian#internet, bastion#root
```

1.4.9.b. Redémarrer ou arrêter des services (mode expert)

Dans `Système/Services (mode expert)`, cliquer sur le bouton `Arrêter` ou `Redémarrer` du service voulu.



Actions sur les services (mode expert)

Les services liés au fonctionnement de l'EAD ne sont disponibles qu'en redémarrage. Sinon, vous perdrez tout accès à l'interface.

Pour relancer l'ensemble des services (sauf l'EAD et le serveur SSO) choisir le bouton : `Redémarrer tous les services (hors EAD et SSO)`.

1.4.10. Rôles et association de rôles

L'EAD est composé, d'actions. Chaque action ayant un but bien précis.

L'EAD dispose d'un mécanisme de délégation d'actions à des utilisateurs déterminés.

Pour affecter certaines actions à un utilisateur, l'EAD utilise une mécanisme interne : les rôles.

Par défaut sur les modules EOLE, l'utilisateur **admin** est associé au rôle **administrateur**.

Plusieurs rôles sont prédéfinis sur les différents modules EOLE et certains sont propres à certains d'entre eux :

- administrateur ;
- professeur (utilisé sur le module Scribe) ;
- élève (utilisé sur le module Scribe) ;
- administrateur de classe (utilisé sur le module Scribe) ;
- administratif dans Scribe (utilisé sur le module Scribe) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon) ;
- administrateur du Scribe (utilisé sur le module AmonEcole) ;
- administrateur de l'Amon (utilisé sur le module AmonEcole).

1.4.10.a. Déclaration des actions

Les actions de l'EAD sont déclarées dans les fichiers :
`/usr/share/ead2/backend/config/actions/actions_*.cfg`

Ces fichiers au format *texte* permettent de déclarer les fichiers python déclarant eux-mêmes des actions EAD à charger.

Ces fichiers sont situés dans `/usr/share/ead2/backend/actions` et ses sous-répertoires.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/actions.cfg` : fichiers des actions de base ;
- ainsi que tout les fichiers `actions_*.cfg` présents dans le répertoire `/usr/share/ead2/backend/config/actions`.

Syntaxe des fichiers

Les fichiers d'action sont déclarés avec leur chemin court depuis `/usr/share/ead2/backend/actions` et sans l'extension ".py".



La déclaration des fichiers d'action suivants :

- `/usr/share/ead2/backend/actions/mes_actions.py`
- `/usr/share/ead2/backend/actions/repertoire/autres_actions.py`

prend la forme suivante dans le fichier `actions_perso.cfg` :

```
$ cat /usr/share/ead2/backend/actions/actions_perso.cfg
mes_actions
repertoire/autres_actions
```

1.4.10.b. Gestion des rôles

Les rôles de l'EAD sont déclarés dans les fichiers : `/usr/share/ead2/backend/config/perms/perm_*.ini`
Ces fichiers au format *ini* permettent d'associer des actions (permissions) à un ou plusieurs rôles.

Fichiers pris en compte

Sur un module EOLE, les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/perm.ini` : rôles de base ;
- `/usr/share/ead2/backend/config/perm_local.ini` : rôles déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/perm_acad.ini` : rôles déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers `perm_*.ini` présents dans le répertoire `/usr/share/ead2/backend/config/perms`.

Syntaxe des fichiers

Les permissions associent un rôle à une ou plusieurs actions.

Les fichiers `perm*.ini` doivent posséder une section `[role]` et une section `[permissions]`.

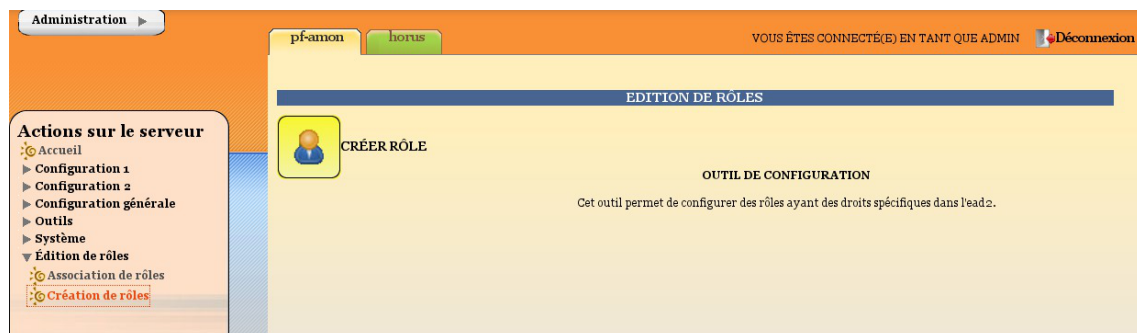
```
[role]
nom du role = libelle du role
[permissions]
action1 = nom du role
action2 = nom du role
```

Création de rôle via l'EAD

L'interface EAD permet de créer des rôles personnalisés.

Ces rôles ne sont, en fait, qu'une liste d'actions regroupées sous un intitulé et un libellé unique.

Il est possible, dans un deuxième temps d'associer ces rôles à des utilisateurs.



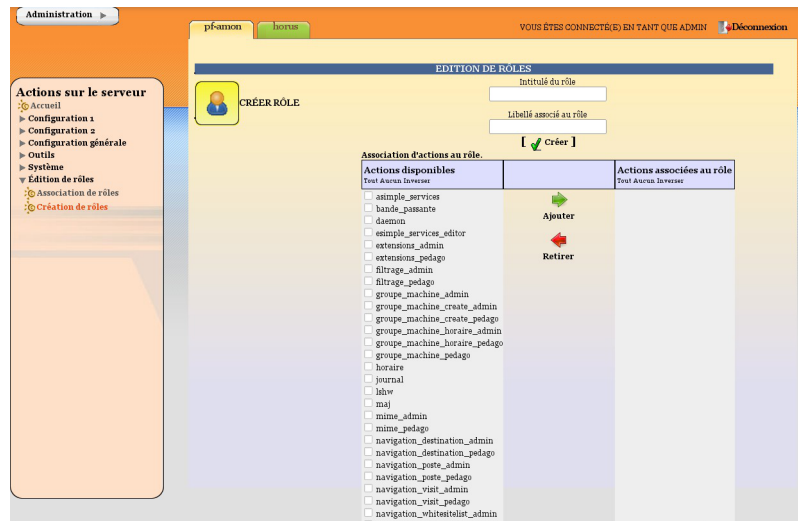
La fenêtre d'édition des rôles

Pour créer un nouveau rôle cliquer sur :

- **Édition de rôles/Création de rôles**

puis

- **Créer rôle**
- entrer l'intitulé (le nom) du rôle (sans caractère spécial, sans accent et sans espace) ;
- entrer un libellé (courte description) du rôle ;
- cocher les actions à autoriser ;
- ajouter ;
- créer.



Création d'un rôle

Actions obligatoires

Certaines actions doivent être obligatoirement permises pour tous les utilisateurs :

- **help** : utilisé notamment pour l'affichage d'aide ;
- **main_status** : page d'accueil appelée par défaut, elle gère un rôle prof (n'affiche pas les états de services) et un rôle admin ;
- **update_ead** : outil de téléchargement des javascripts, CSS, images spécifiques au module.

Actions communes aux différents modules

- **lshw** : listing matériel ;
- **maj** : action de mise à jour ;
- **daemon** : relancer des services (mode expert) ;
- **simple_services_editor** : éditer des groupes de services pour le mode simplifié ;
- **simple_services** : redémarrer/arrêter les services (mode simplifié) ;
- **server-configure/server-reboot/server-stop** : redémarrer/arrêter/reconfigurer le serveur ;
- **role_editor** : création de rôles ;
- **role_manager** : association de rôle (appelée par d'autres actions).

Actions spécifiques au module Amon

La modification du système de filtrage sur le module Amon apporte de profondes modifications sur ce

module.

Selon les choix effectués lors de la phase de configuration avec l'interface de configuration du module, vous pouvez choisir d'utiliser une ou deux zones de configuration pour le filtrage et les options du pare-feu.

La zone 1 correspond à la réseau admin et la zone 2 correspond au réseau pedago.

- Gestion des postes
 - **navigation_poste_admin** (ou pedago) : action de gestion des postes à interdire ;
 - **navigation_destination_admin** (ou pedago) : interdire des destinations.
- Gestion des groupes de machine
 - **groupe_machine_admin** (ou pedago) : action d'entrée pour la gestion des groupes de machine (gère des restrictions pour le rôle prof) ;
 - **groupe_machine_create_admin** (ou pedago) : action de création de groupe de machine (nécessite groupe_machine) ;
 - **groupe_machine_horaire_admin** (ou pedago) : action de gestion des horaires pour les groupes de machine.
- Gestion des utilisateurs
 - **navigation_banned_user_admin** (ou pedago) : action de gestion des utilisateurs à interdire ;
 - **navigation_moderateur_admin** (ou pedago) : action de gestion des modérateurs ;
 - **navigation_whitelist_admin** (ou pedago) : action de gestion des utilisateurs en liste blanche ;
 - **navigation_whitesitelist_admin** (ou pedago) : action de gestion des sites en liste blanche.
- Gestion des sites
 - **opt_filters_admin** (ou pedago) : gestion des filtres optionnels pour la zone de configuration 1 (ou 2) ;
 - **filtrage_admin** (ou pedago) : gestion du mode de filtrage syntaxique pour la zone de configuration 1 (ou 2) ;
 - **sites_interdits_admin** (ou pedago) : gestion des sites interdits pour la zone de configuration 1 (ou 2) ;
 - **sites_autorises_admin** (ou pedago) : gestion des sites autorisés pour la zone de configuration 1 (ou 2) ;
 - **extensions_admin** (ou pedago) : gestion des extensions interdites pour la zone de configuration 1 (ou 2) ;
 - **mime_admin** (ou pedago) : gestion des types mime interdits pour la zone de configuration 1 (ou 2).
- Gestion des règles du pare-feu
 - **regles** : mode de fonctionnement du pare-feu ;
 - **peertopeer** : autorisation/interdiction du peer to peer ;
 - **horaire** : horaire de fonctionnement du pare-feu.
- Autres actions
 - **navigation_visit** : action de consultation des logs ;

- **filtrage_bayes** : action d'évaluation d'URL à l'aide du filtrage bayésien ;
- **bande_passante** : outil de test de bande passante.

Actions spécifiques au module Scribe

- Gestion des utilisateurs
 - **scribe_user_create** : action de création ;
 - **scribe_user_list** : renvoie le formulaire de recherche par critères qui appelle scribe_user_table pour la validation ;
 - **scribe_user_table** : action de listing d'utilisateur (gère les rôles prof_admin et admin) appelle scribe_user_modify, scribe_user_delete, scribe_user_modpassword ;
 - **scribe_user_modify** : action de modification d'utilisateur (utilisée par scribe_user_table gère les rôles prof_admin et admin) ;
 - **scribe_user_delete** : action de suppression d'utilisateur (gère les rôles prof_admin et admin) ;
 - **scribe_user_modpassword** : action de modification d'un mot de passe (gère les rôles prof_admin et admin).
- Actions restreintes (créées pour les professeurs, les personnels administratifs et les professeurs admins, gère le rôle de prof et prof_admin)
 - **scribe_prof_preference** : préférences du professeur connecté (mot de passe, inscription aux groupes, mail) ;
 - **scribe_prof_mod_mail** : modifie le mail d'un professeur (nécessite scribe_prof_preference) ;
 - **scribe_user_password** : action de modification de son propre mot de passe (nécessite scribe_prof_preference) ;
 - **scribe_prof_mod_groupe** : Inscription du prof connecté aux groupes ;
 - **scribe_prof_user** : action d'entrée pour la gestion des utilisateurs par les profs lien vers scribe_prof_user_create et scribe_prof_user_modify ;
 - **scribe_prof_user_create** : action de création d'utilisateur (nécessite scribe_prof_user) ;
 - **scribe_prof_user_modify** : action d'entrée pour la modification des utilisateurs (nécessite scribe_prof_user) ;
 - **scribe_grouped_edition** : action d'entrée pour l'édition groupée d'utilisateur (appelle scribe_user_table).
- Gestion des groupes
 - **scribe_group_create** : création de groupes, niveau, classe..., appelle scribe_group_list ;
 - **scribe_group_list** : liste les groupes, appelle scribe_group_delete, appelle scribe_group_create ;
 - **scribe_group_modify** : modification de groupe ;
 - **scribe_group_delete** : suppression de groupe ;
 - **scribe_prof_group** : entrée pour la gestion des groupes par un prof_admin ou un prof, appelle scribe_prof_user_modify et scribe_prof_group_create ;
 - **scribe_prof_group_create** : action de création de groupe par un prof_admin.
- Gestion des partages
 - **scribe_share** : attribution de lettre de lecteur à un partage.

- Gestion des stations et connexions
 - **scribe_station** : action de suppression forcée de station du domaine ;
 - **scribe_extraction** : action d'extraction sconet ;
 - **scribe_connexion_index** : page d'accueil des observations des connexions ;
 - **scribe_connexion_machine** : page d'affichage des machines connectées ;
 - **scribe_connexion_quota** : observation des quotas ;
 - **scribe_connexion_virus** : affiche la liste les virus repérés ;
 - **scribe_connexion_history** : affiche l'historique des connexions.
- Autres actions
 - **scribe_devoir_distribuer** / **scribe_devoir_ramasser** / **scribe_devoir_rendre** / **scribe_devoir_supprimer** : gestion des devoirs ;
 - **bareos** : action de programmation de sauvegarde ;
 - **bareos_config** : action de configuration de sauvegarde ;
 - **scribe_sympa** : action renvoyant des liens pour l'interface de gestion de listes de diffusion ;
 - **printers** : action de gestion simplifiée des imprimantes.

Actions spécifiques au module Horus

- Gestion des connexions
 - **isis** : action d'entrée pour l'interface d'observation des connexions, appelle les actions isis ;
 - **isis_stop** : action d'arrêt de toutes les connexions ;
 - **isis_disconnect** : action de déconnexion d'utilisateur connectés au domaine ;
 - **isis_sendmsg** : action d'envoi de message à des utilisateurs connectés ;
 - **isis_machine** : action de listing des machines connectées au domaine (client, maîtres explorateurs...) ;
 - **isis_login** : action d'autorisation des utilisateurs par login ;
 - **isis_quota** : action d'affichage des quotas ;
 - **gestion_index** : action d'entrée vers les gestions d'utilisateur, groupe, partage, appelle les actions gestion.
- Gestion des utilisateurs
 - **gestion_user_modify** : action de modification d'utilisateur ;
 - **gestion_user_create** : action de création d'utilisateur ;
 - **gestion_user_suppr** : action de suppression d'utilisateur.
- Gestion des partages
 - **gestion_share_create** : action de création de partage ;
 - **gestion_share_modify** : action de modification de partage ;
 - **gestion_share_suppr** : action de suppression de partage.
- Gestion des groupes
 - **gestion_group_create** : action de création de groupe ;
 - **gestion_group_modify** : action de modification de groupe ;

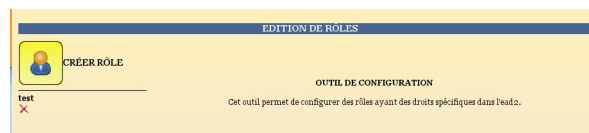
- **gestion_group_suppr** : action de suppression de groupe.
- Autres actions
 - **gestion_account_suppr** : action de suppression forcée de compte ;
 - **extraction_aaf** : action pour l'extraction AAF ;
 - **bareos** : action programmation de sauvegarde ;
 - **bareos_config** : action de configuration de Bareos pour la sauvegarde ;
 - **scripts_admin** : action pour l'exécution de scripts d'administration ;
 - **printers** : action de gestion des imprimantes.

Actions spécifiques au module Seshat

- Menu Messagerie
 - **routes** : gestion du routage des messages vers les établissements de l'Académie.

Modification et suppression de rôle via l'EAD

- Pour modifier un rôle, il suffit de cliquer sur le nom voulu ;
- pour le supprimer, cliquer sur la croix rouge associée.



Modification/suppression d'un rôle

1.4.10.c. Association des rôles

Les associations de rôle de l'EAD sont déclarées dans les fichiers :
`/usr/share/ead2/backend/config/roles/roles_*.ini`

Ces fichiers au format INI^[p.549] permettent d'associer des rôles à un ou plusieurs utilisateurs.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/roles.ini` : associations de base (admin, eleve, prof, ...)
- `/usr/share/ead2/backend/config/roles_<module>.ini` : associations spécifiques au module installé (ex : `roles_scribe.ini`) ;
- `/usr/share/ead2/backend/config/roles_local.ini` : associations déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/roles_acad.ini` : associations déclarés au niveau académique (via Zéphir).

Syntaxe des fichiers

L'association d'un rôle se fait à partir du login d'un utilisateur système (section `[pam]`) ou de la valeur associée à un attribut ldap (section `[nom_attribut]`) de l'annuaire utilisé pour l'authentification SSO sur l'EAD du module.



- `[pam]`
- `scribe2=admin`
- `[uid]`
- `.jean.dupont=prof_admin`
- `[user_groups]`
- `minedu=admin_horus`



La clé spéciale `[user_groups]` permet d'attribuer un rôle à tous les membres d'un groupe déclaré dans l'annuaire LDAP.

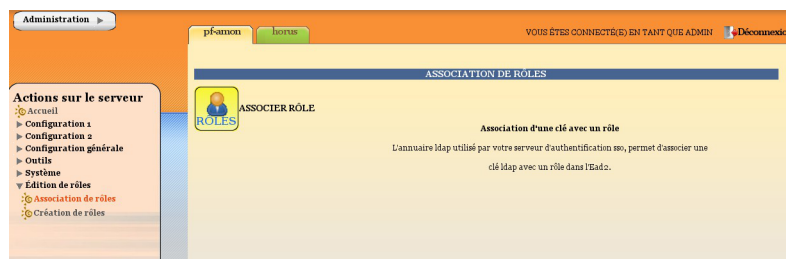
Création d'association via l'EAD

Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

Certaines de ces informations sont utilisées pour lui attribuer des rôles et ainsi lui donner accès à certaines actions.

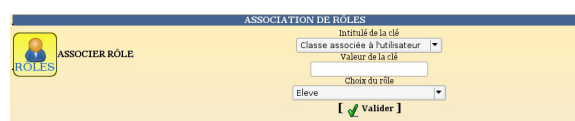
Pour associer un rôle à des utilisateurs:

- dans `Édition des rôles/Association de rôle` ;
- cliquer sur `Associer Rôle` .



La fenêtre d'association de rôles

- choisir la clef (attribut de l'utilisateur) ;
- renseigner la valeur recherchée pour cet attribut (dans le cas d'une authentification locale on mettra le login de l'utilisateur) ;
- choisir le rôle à associer ;
- valider.



Association d'un rôle

L'intitulé de la clef dépend du système d'authentification utilisé pour se connecter :

Authentification locale :

- le login de l'utilisateur.

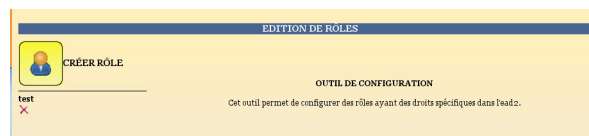
Authentification SSO :

- l'élève fait partie de la classe ;
- la valeur de la clé LDAP typeadmin :
 - 0 → enseignant
 - 1 → administrateur
 - 2 → enseignant responsable de classe
 - 3 → personnel administratif
- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.

Il est indispensable de redémarrer le service ead-server dans **Système->Services (mode expert)** pour que les modifications soient prises en compte.

Suppression d'une association via l'EAD

Une association de rôle peut par la suite être supprimée en cliquant sur la croix rouge.



Modification/suppression d'un rôle

1.4.10.d. Les rôles sur le module Amon

L'EAD est accessible aux utilisateurs locaux *root* et *eole*.

Si l'authentification SSO est configurée, il est également accessible à l'utilisateur *admin*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module Amon, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon).

Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.
L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

📁 Fonctionnalités Amon

L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques du proxy ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Administrateur du réseau pédago"

Dans le cas où plusieurs filtres web (instances de e2guardian) sont configurés, ce rôle permet de déléguer la gestion des options de filtrage pour le filtre n°2, traditionnellement associé à la zone pédagogique.



1.4.10.e. Les rôles sur le module Scribe

L'EAD est accessible :

- en authentification locale aux utilisateurs *root* et *eole* ;
- en authentification SSO au compte *admin* ainsi qu'à tous les *personnels enseignant et administratif*.

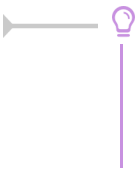
En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module Scribe, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions comme par exemples : redémarrage des services, mise à

jour du serveur, création et affectation des rôle aux autres utilisateurs, etc (valeur de l'attribut LDAP `uid` → admin et comptes locaux root et eole);

- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS (valeur de l'attribut LDAP `typeadmin` → 0) ;
- responsable de classe : en plus des actions "professeur", il peut ré-initialiser le mot de passe des élèves des classes dont il est responsable (valeur de l'attribut LDAP `typeadmin` → 2). Attention, le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable (pour cela il doit être ajouté à l'équipe pédagogique) ;
- personnel administratif : modification des préférences personnelles, gestion des files d'impression CUPS (membres du groupe administratifs).



Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.



Fonctionnalités Scribe

L'EAD du module Scribe, dans son mode le plus complet, présente les fonctionnalités suivantes :

- distribution de devoirs et de documents ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/SIECLE/AAF/ONDES ;
- gestion des ACL ;
- gestion des quotas disque ;
- gestion des listes de diffusion ;
- test de la bande passante du serveur ;
- modification du mode de visualisation des postes élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;

- gestion des rôles EAD.

Accès "Professeur"

Un enseignant dispose d'actions lui permettant de :

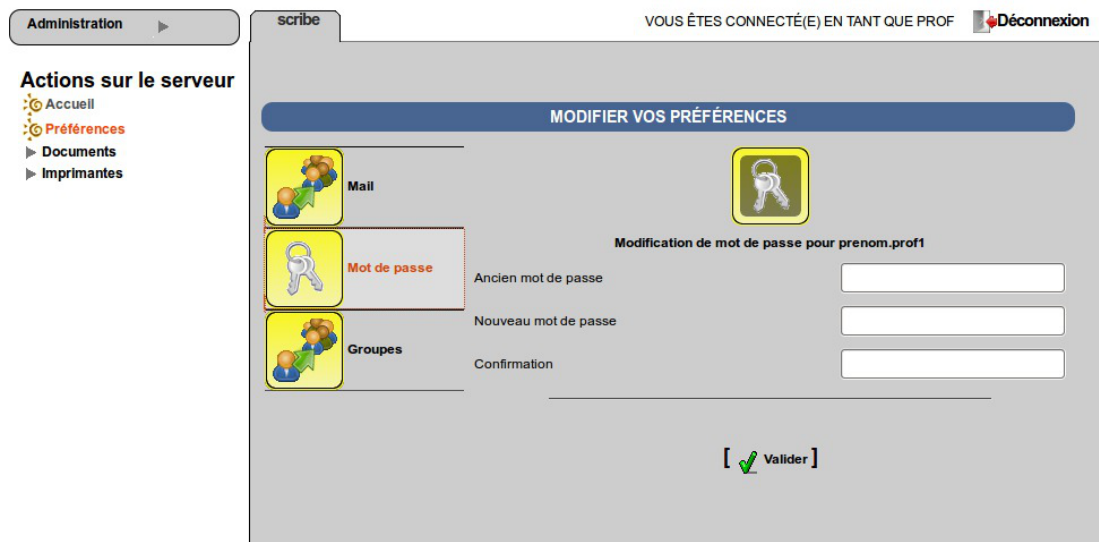
- configurer ses préférences personnelles ;
- distribuer des documents ;
- gérer les imprimantes.



l'EAD pour un professeur

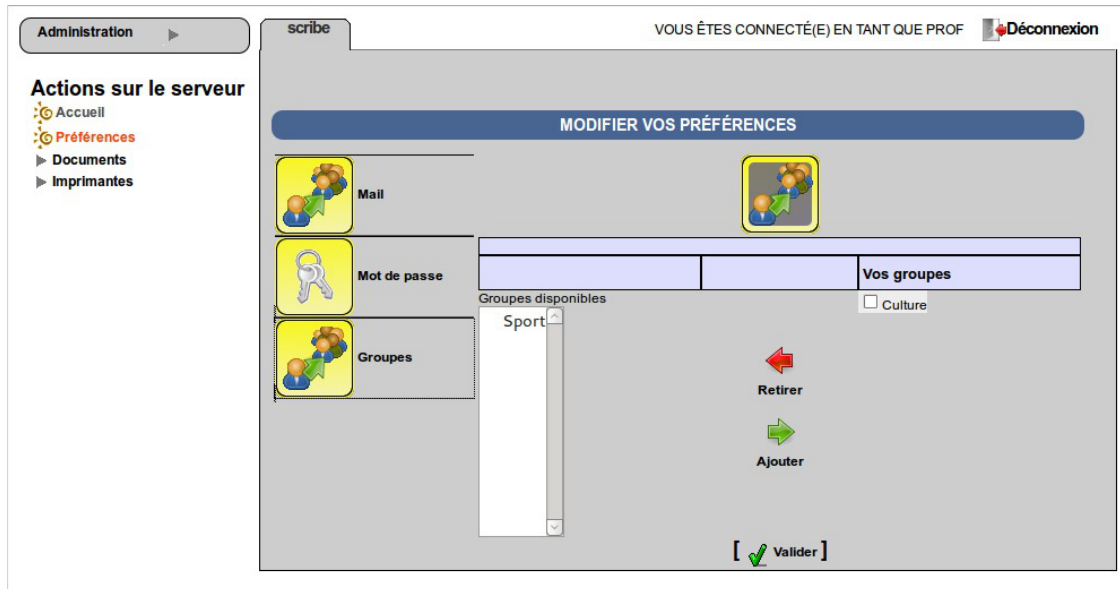
L'item *Préférences* permet à un utilisateur de :

- modifier son mot de passe ;



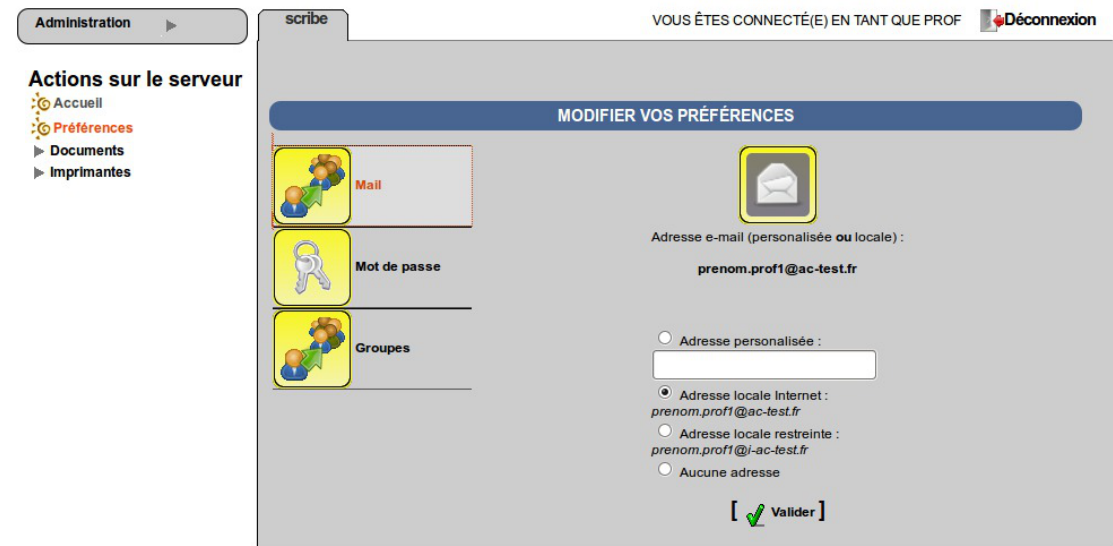
EAD vue enseignant avec thème Envole, changement de mot de passe

- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

- Un professeur peut être responsable de plusieurs classes.
- Une classe peut se voir affecter plusieurs responsables.



- Le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable, pour cela il doit être ajouté à l'équipe pédagogique.

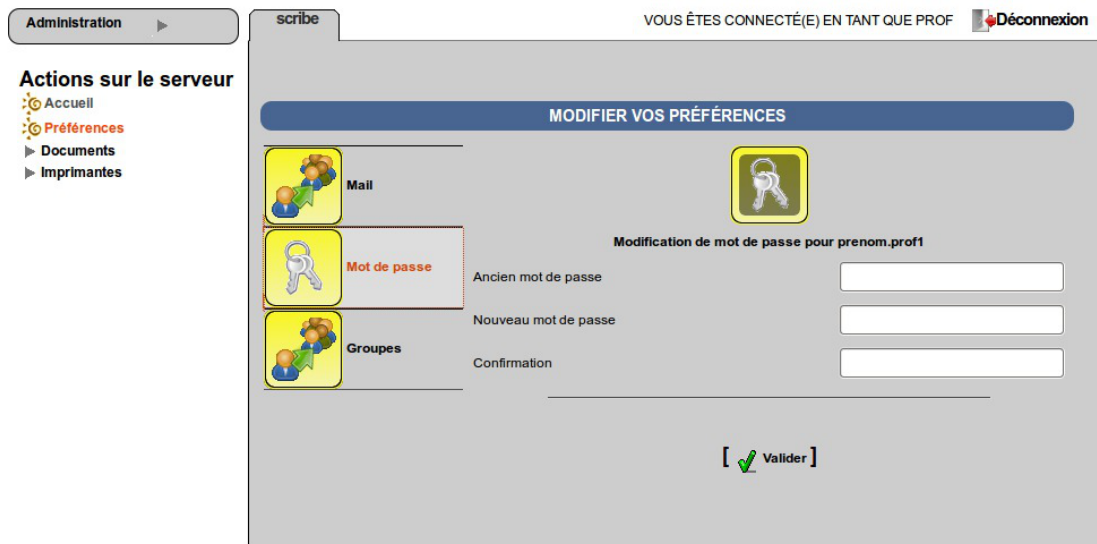
Accès "Administratif du Scribe"

Les personnels administratifs possédant un compte sur le module ont accès à leurs préférences personnelles et à la gestion des imprimantes.



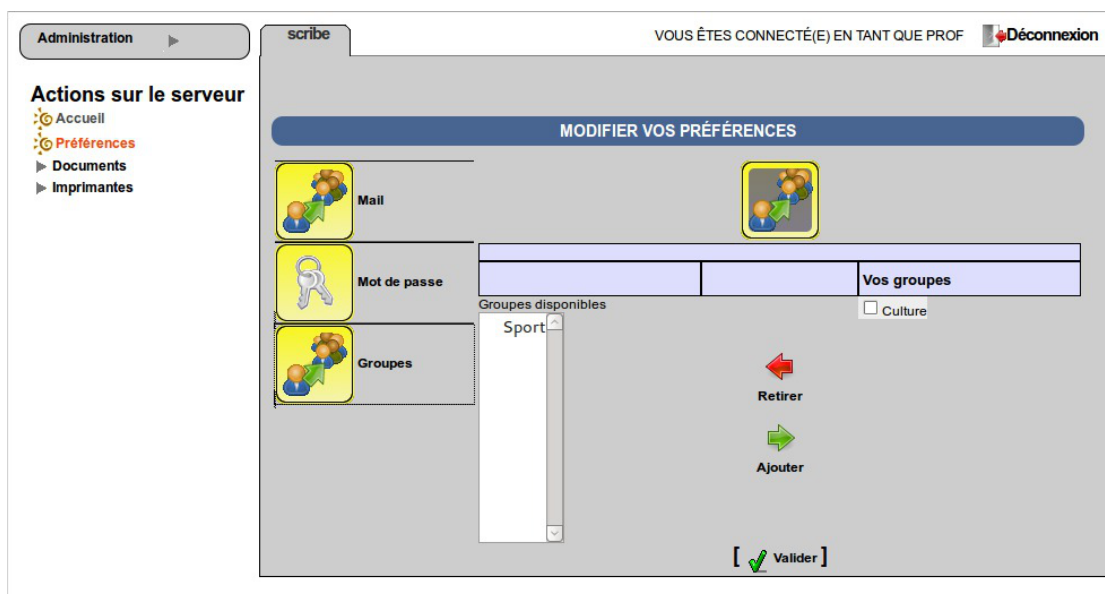
L'item *Préférences* permet à un utilisateur de :

- modifier son mot de passe ;



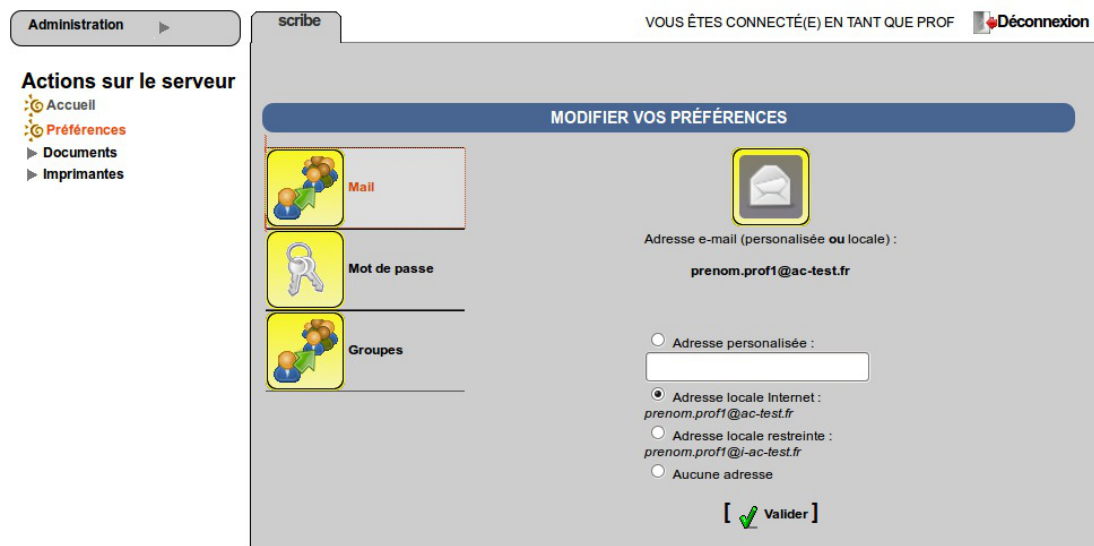
EAD vue enseignant avec thème Envole, changement de mot de passe

- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

1.4.10.f. Les rôles sur le module AmonEcole

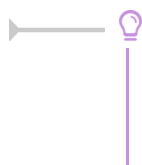
L'EAD est accessible :

- en authentification locale aux utilisateurs *root* et *eole* ;
- en authentification SSO au compte *admin* ainsi qu'à tous les *personnels enseignant et administratif*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module AmonEcole, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- professeur : modification des préférences personnelles, distribution de devoirs et gestion des files d'impression CUPS ;
- responsable de classe : en plus des actions "professeur", peut ré-initialiser le mot de passe des élèves des classes dont il est responsable ;
- administratif dans Scribe ;
- administrateur du Scribe ;
- administrateur de l'Amon.



Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.
L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

Accès "Professeur"

Un enseignant dispose d'actions lui permettant de :

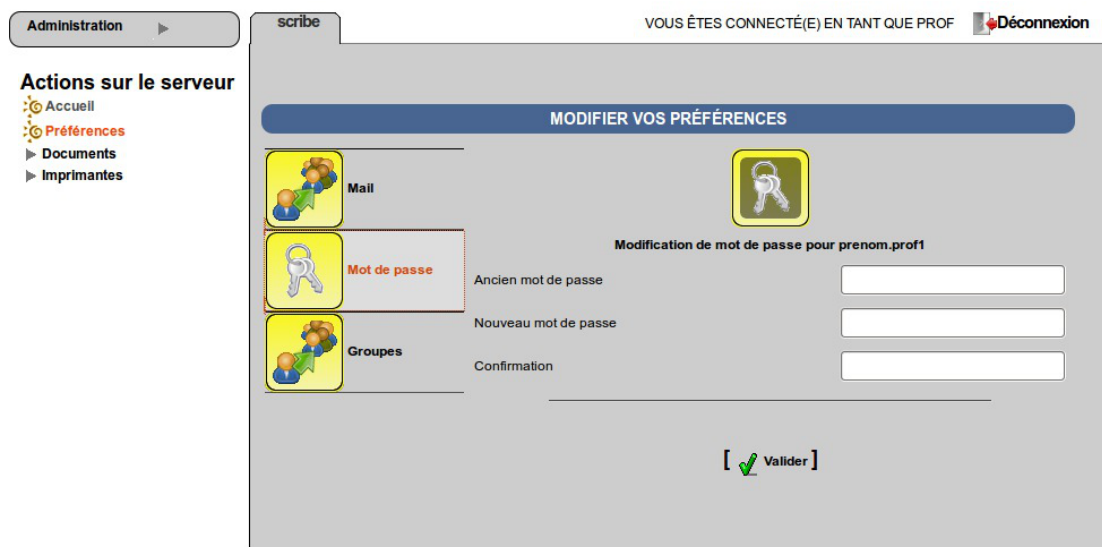
- configurer ses préférences personnelles ;
- distribuer des documents ;
- gérer les imprimantes.



l'EAD pour un professeur

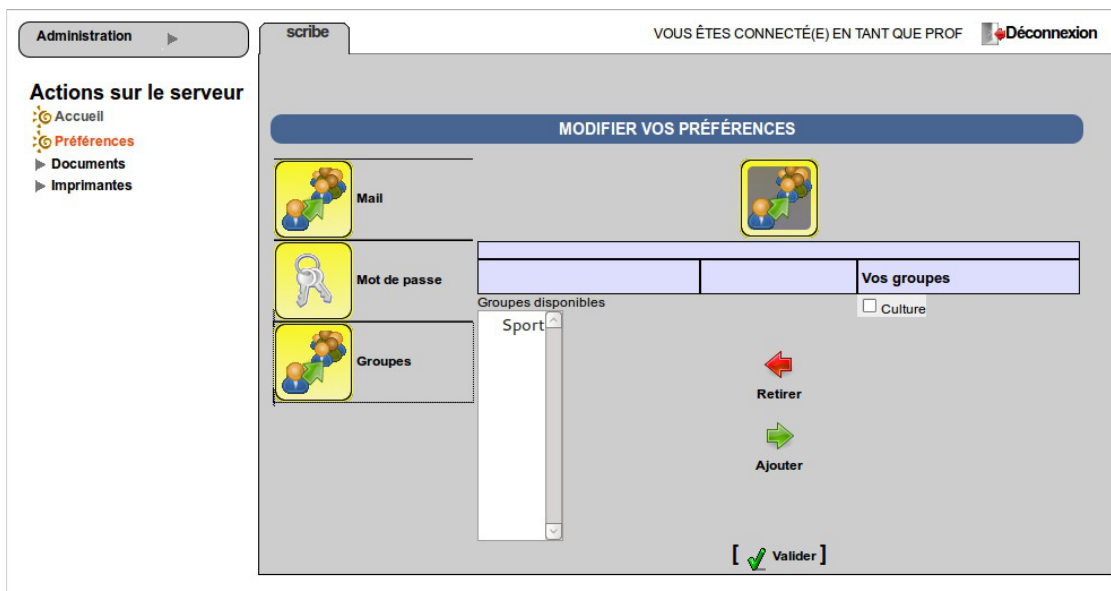
L'item *Préférences* permet à un utilisateur de :

- modifier son mot de passe ;



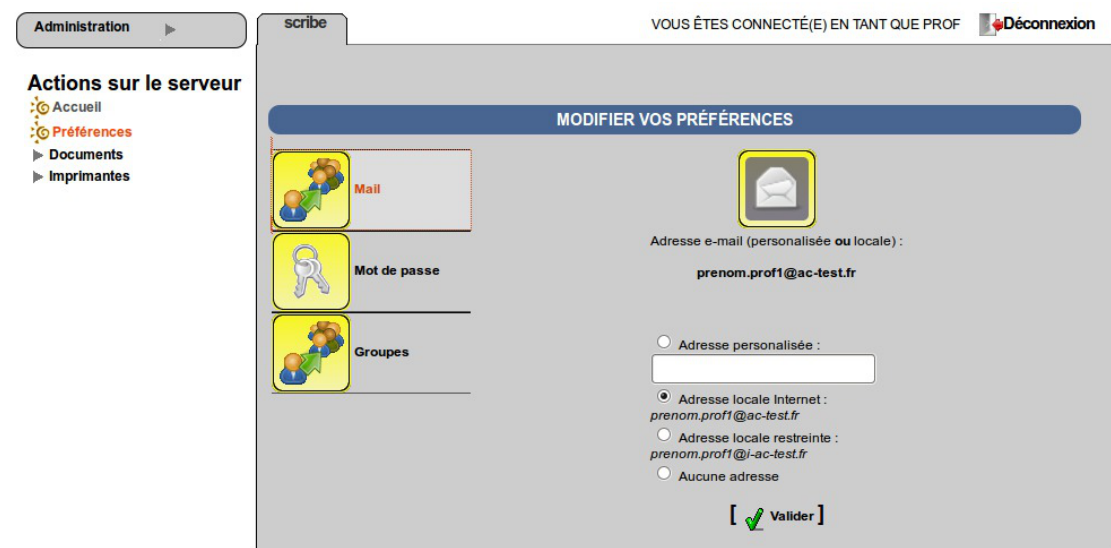
EAD vue enseignant avec thème Envole, changement de mot de passe

- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

- Un professeur peut être responsable de plusieurs classes.
- Une classe peut se voir affecter plusieurs responsables.

- **!** Le responsable de classe n'est pas membre du groupe et n'a pas accès aux partages des classes dont il est responsable, pour cela il doit être ajouté à l'équipe pédagogique.

Accès "Administrateur du Scribe"

Sur un module AmonEcole, le rôle "Administrateur du Scribe" (admin_scribe) permet de déléguer à un utilisateur les fonctionnalités EAD propres au module Scribe.

Fonctionnalités Scribe

L'EAD du module Scribe, dans son mode le plus complet, présente les fonctionnalités suivantes :

- distribution de devoirs et de documents ;
- création/gestion des utilisateurs, des groupes et des partages ;
- configuration et gestion des imprimantes (CUPS) ;
- importation CSV/SIECLE/AAF/ONDES ;
- gestion des ACL ;
- gestion des quotas disque ;
- gestion des listes de diffusion ;
- test de la bande passante du serveur ;

- modification du mode de visualisation des postes élèves ;
- consultation de l'historique des connexions ;
- envoi d'un message aux utilisateurs connectés ;
- extinction/redémarrage/fermeture de session sur les postes clients ;
- gestion des comptes de machine ;
- paramétrage et programmation des sauvegardes du serveur ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Administrateur de l'Amon"

Sur un module AmonEcole, le rôle "Administrateur de l'Amon" (admin_amon) permet de déléguer à un utilisateur les fonctionnalités EAD propres au module Amon.

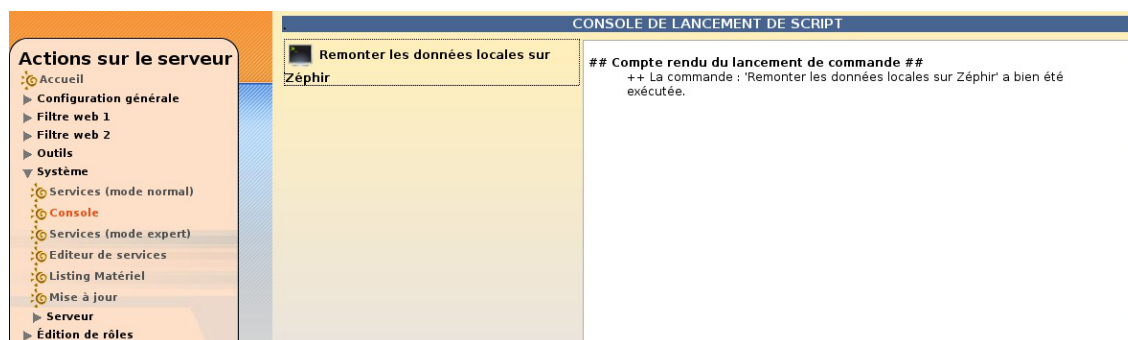
— Fonctionnalités Amon

L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques du proxy ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

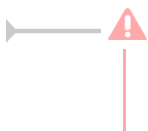
1.4.11. La console

Cette fonctionnalité permettra d'ajouter des actions et des scripts personnalisés directement dans l'EAD.



Remontée des données locales sur Zéphir par la console EAD

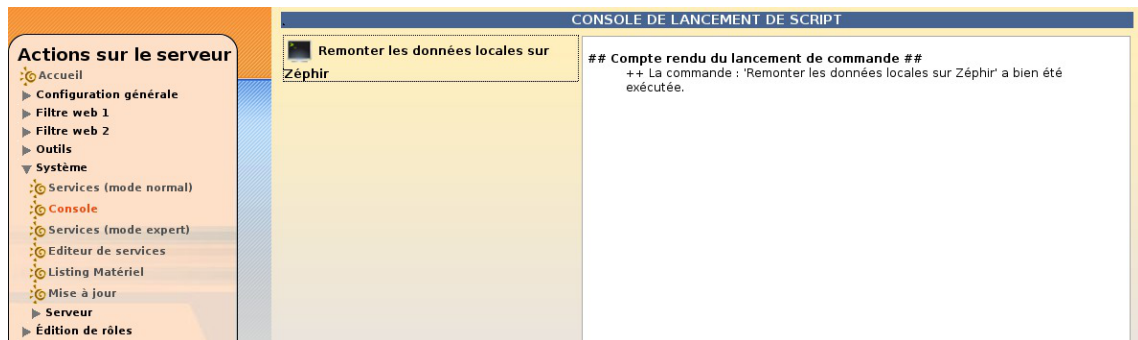
Seul le script Remonter les données locales sur Zéphir est fourni par défaut.



Cette fonctionnalité n'est pas stabilisée. De plus, les actions et scripts personnalisés seront supprimés à la prochaine mise à jour.

Remonter les données locales sur Zéphir

Cette action permet de déclencher la remontée des données sur le Zéphir (appel de la commande : `zephir_client_save_files_3`).



Remontée des données locales sur Zéphir par la console EAD

Écrire des scripts personnalisés

Copier avec un nouveau nom le script existant :

```
# cp /usr/share/ead2/backend/actions/cmd_update_zephir.py
/usr/share/ead2/backend/actions/cmd_df.py
```

Éditer le script et renommer la classe, le nom du script, la commande à exécuter et le libellé de la commande :

```
# vim /usr/share/ead2/backend/actions/cmd_df.py
1 # -*- coding: UTF-8 -*-
2 from ead2.backend.actions.lib.main import Cmd
3
4 class Cmd_Df(Cmd): # renommer la classe
5     """
6     Action du mode commande
7     """
8     name = "cmd_df" # nom du script
9     # propriété de la commande à exécuter
10    cmd_template = "df -h"
11    cmd_libelle = "Occupation disque" # libellé du script dans l'EAD
```

Ajouter le nom du nouveau script au fichier `zstats.cmd` :

```
# vim /usr/share/ead2/backend/config/cmds/zstats.cmd
```

ou

```
# echo "cmd_df" >> /usr/share/ead2/backend/config/cmds/zstats.cmd
```

Déclarer le nouveau script dans le fichier `actions_zstats.cfg` :

```
# vim /usr/share/ead2/backend/config/actions/actions_zstats.cfg
```

ou


```
# echo "cmd_df" >> /usr/share/ead2/backend/config/actions/actions_zstats.cfg
```

Ajouter les droits d'utilisation du script dans le fichier `perm_zstats.ini` :

```
# vim /usr/share/ead2/backend/config/perms/perm_zstats.ini
```

ou

```
# echo "cmd_df=admin" >> /usr/share/ead2/backend/config/perms/perm_zstats.ini
```

Relancer le service :

```
# service ead-server restart
```

L'action est accessible dans le menu de l'EAD. Lorsque la commande réussit un message s'affiche :

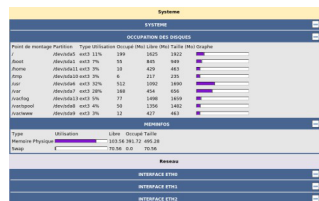
```
++ La commande : 'Occupation disque' a bien été exécutée.
```

Cliquer sur Afficher le contenu reçu permet d'afficher le résultat de la commande.

1.4.12. Listing matériel

Le listing matériel permet de visualiser les éléments matériels du serveur.

Il indique notamment l'occupation des disques, de la mémoire vive et de la partition swap.



Listing matériel (lshw)

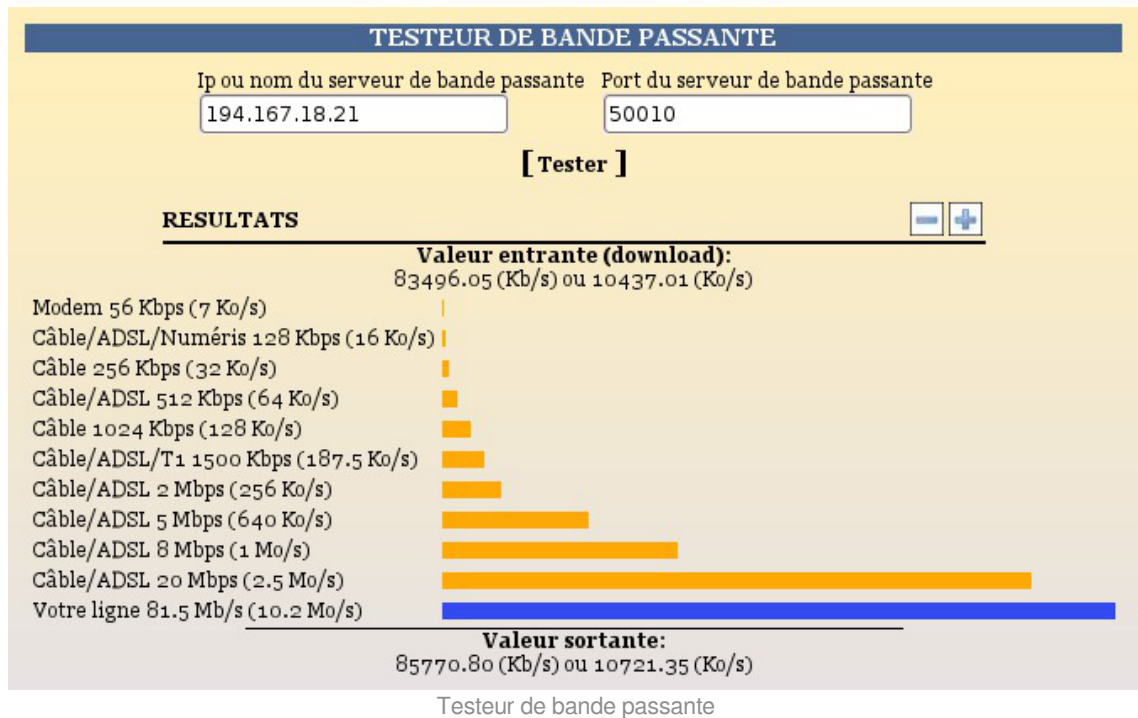
! La mémoire physique (RAM)

Le noyau Linux^[p.551] utilise un système de cache mémoire pour limiter les accès disque. Le chiffre "mémoire physique" comprend ce cache. Cela signifie qu'il n'est pas inquiétant de voir une valeur proche de 100%.

Le critère important étant l'occupation le swap (mémoire virtuelle). Une utilisation du swap indique que le serveur manque de RAM. Il faut alors envisager d'en augmenter la quantité ou chercher à alléger la charge de la machine.

1.4.13. Bande passante

Le menu `Outils/Bande passante` permet de tester la bande passante dont dispose le serveur.



1.4.14. Résoudre des dysfonctionnements liés à l'EAD

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation du fichier journal `/var/log/ead/ead-server.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```
1 service ead-server stop
2 cd /tmp
3 export PYTHONPATH=/usr/share
4 twisted -noy /usr/share/ead2/backend/eadserver.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

Si c'est le service `ead-web` qui est en erreur et que le fichier journal `/var/log/ead/ead-web.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

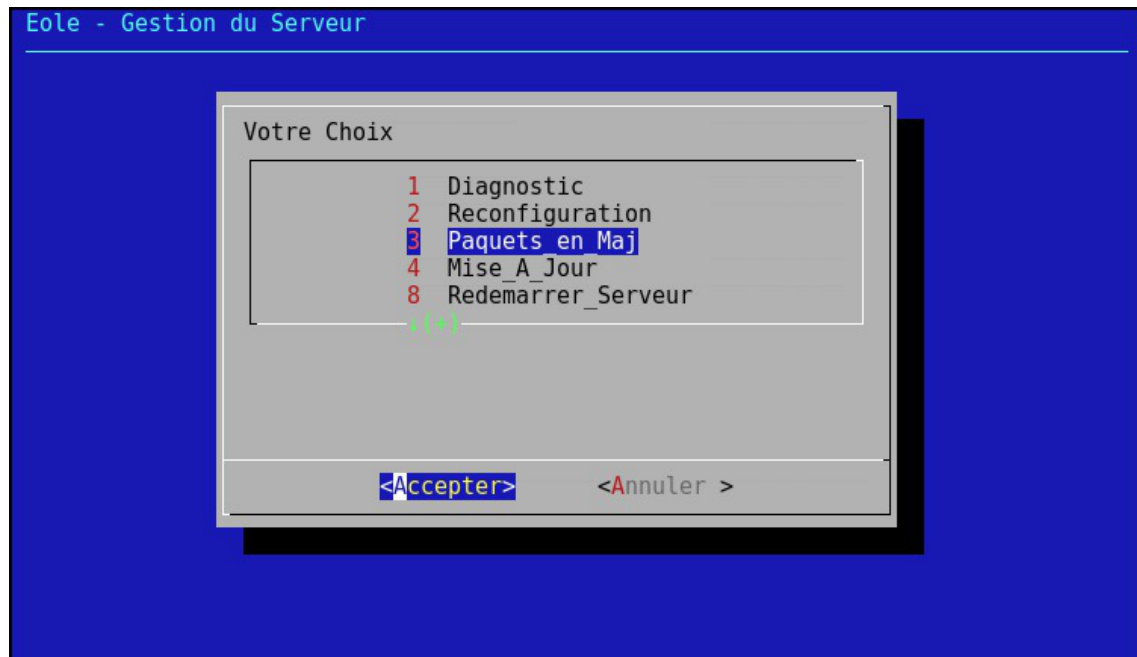
```
1 service ead-web stop
2 cd /tmp
3 export PYTHONPATH=/usr/share
4 twisted -noy /usr/share/ead2/frontend/frontend.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

1.5. L'interface d'administration semi-graphique

En plus de l'EAD, une interface semi-graphique est disponible.

Cette interface (`manage-eole`) permet d'exécuter quelques tâches simples d'administration du serveur : diagnostique, mise à jour, liste des paquets en mise à jour, etc.



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ...

1.6. Les mises à jour

Avec GNU/Linux, comme avec d'autres systèmes d'exploitation, les logiciels doivent être compilés avant de pouvoir être utilisés.

Au début du projet Debian (sur lequel est basé Ubuntu), les auteurs jugèrent nécessaire de disposer d'un système d'installation et de désinstallation de logiciels et bibliothèques efficace et simple. Ce système fut nommé **dpkg** et utilise des paquets portant l'extension **.deb**.

Les paquets

Un paquet contient un logiciel ou une bibliothèque déjà compilé et qui s'installe de façon automatique au travers du gestionnaire de paquets. Le format natif des paquets pour Ubuntu et donc pour EOLE est le paquet Debian.



Pour limiter la taille des paquets et pour rendre plus efficace l'utilisation de votre ordinateur, le paquet ne contient que le logiciel ou la bibliothèque. Si ce logiciel a besoin d'un autre logiciel ou d'une bibliothèque particulière pour fonctionner, le paquet indique quelles sont ces exigences à satisfaire. On les appelle les dépendances.

La dépendance permet une réutilisation d'une même composante par plusieurs logiciels. Par exemple, si un logiciel nécessite une bibliothèque particulière et qu'un autre logiciel nécessite aussi cette bibliothèque, une ne sera installée qu'une seule fois pour les deux programmes. Cette dépendance apporte plusieurs avantages: lors d'une mise à jour, un paquet est mis à jour pour tous les logiciels, il y a alors une économie de bande passante et d'espace utilisé sur les disques durs.

Le gestionnaire de paquets

Le fait qu'un paquet puisse dépendre d'autres paquets serait infernal à gérer de façon manuelle.

Advanced Packaging Tool (APT) est un système complet et avancé de gestion de paquets, permettant une recherche facile et efficace, une installation simple et une désinstallation propre de logiciels et utilitaires. Il gère les dépendances automatiquement et paramètre les fichiers de configuration durant l'installation et les mises à jour.

Les mises à jour sont continues et incrémentales. Le système offre une méthode de mise à jour cohérente et un processus de mise à jour sûr.

APT est un ensemble d'utilitaires utilisables en ligne de commande.

Il facilite la mise à jour d'une distribution Debian et Ubuntu.

EOLE utilise également ce système et fournit un ensemble de facilité :

- mise à jour hebdomadaire est configurée automatiquement ;
- mise à jour au travers de l'EAD et de Zéphir ;
- commandes Maj-Auto, Query-Auto et apt-eole.

Proxy et mise à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le blocage de certaines mises à jour aussi, la déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon. La déclaration du proxy s'effectue dans l'onglet **Général** de l'interface de configuration du module, passer Utiliser un serveur mandataire (proxy) pour accéder à Internet à oui et paramétrer l'adresse du proxy dans le champ Nom ou adresse IP du serveur proxy.

1.6.1. Les différents types de mises à jour

Les mises à jour pour une version donnée permettent de corriger les problèmes bloquants, de sécurité et/ou ne permettant pas un fonctionnement normal du module.

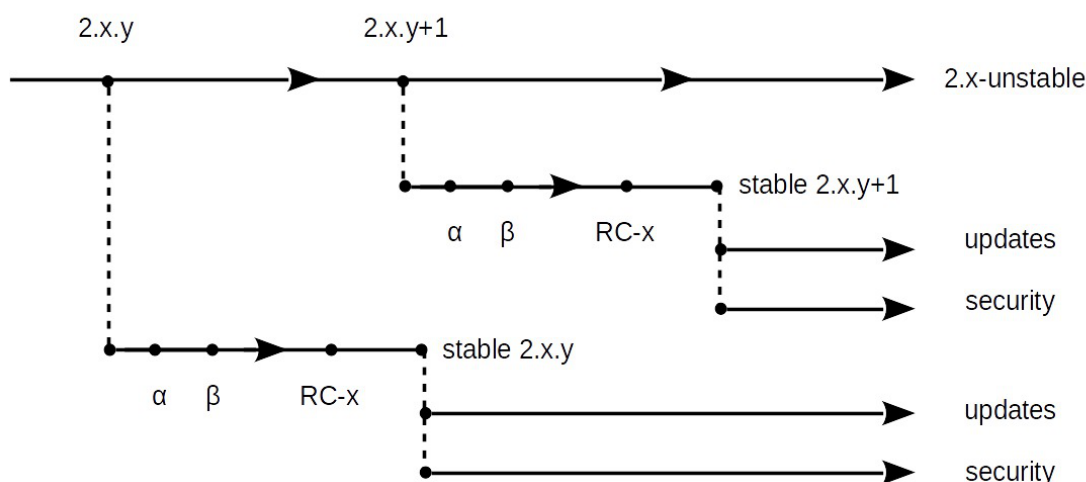
Par défaut une mise à jour hebdomadaire est configurée automatiquement à la fin de l'instanciation du module. Ce comportement est paramétrable et désactivable.

Sur EOLE 2.5, il n'existe plus qu'un seul niveau de mise à jour. Le concept de mise à jour minimale et complète a été supprimé. L'ajout de nouvelles fonctionnalités entraîne une nouvelle version d'EOLE

(2.5.x). Le passage d'une version à une autre est manuel.

Les mises à jour fonctionnelles et les corrections sont proposées sur le dépôt de développement (Unstable), puis proposées en Release candidate (RC)^[p.563] lorsque les paquets sont stabilisés et testés. Plusieurs RC successives ont lieu avant la publication de la totalité des RC en stable. Cela donne lieu à une nouvelle version d'EOLE (2.5.x). Chaque version d'EOLE bénéficie des dépôts :

- Security : paquets fixant un problème de sécurité ;
- Updates : paquets fixant des dysfonctionnements bloquants ou suffisamment importants et ne pouvant pas attendre la sortie d'une nouvelle version d'EOLE (durée de rétention en RC et publication en stable).
- Proposed-updates : paquets candidats pour la version d'EOLE utilisée.



Mise à jour corrective

La dénomination "mise à jour corrective" concerne les paquets qui sont diffusés en version stable sur une version mineure d'EOLE.

Il s'agit généralement des paquets proposés dans la "mise à jour candidate annoncée" sur lesquels des correctifs additionnels mineurs ont pu être apportés.

Ces paquets font l'objet d'annonces officielles :

- publication d'une annonce dans la forge : <https://dev-eole.ac-dijon.fr/projects/modules-eole/news> ;
- reprise de l'annonce dans les flux RSS du site officiel du projet : <http://pctl.ac-dijon.fr/eole/> ;
- envoi d'un message sur les principales listes de diffusion du projet : <https://pctl.ac-dijon.fr/listes> ;
- publication d'un message sur le compte Twitter du pôle de compétences : <https://twitter.com/poleeole> ;

- publication d'un message sur le compte Mastodon de l'équipe EOLE : <https://mastodon.etalab.gouv.fr/@EOLE>.

Le détail des paquets disponibles est indiqué dans les journaux des versions mineures concernées (exemple : <https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Journaux252> pour EOLE 2.5.2).

Les paquets diffusés en version stable sont disponibles dans les dépôts stables du site de référence.

Ils s'installent à l'aide de la commande : `Maj-Auto` et sont également installés automatiquement pas la mise à jour hebdomadaire.

Mise à jour candidate annoncée

La dénomination "mise à jour candidate annoncée" concerne les paquets prêts à être diffusés en version stable sur une version mineure d'EOLE.

Il s'agit généralement des paquets proposés dans la "mise à jour candidate en préparation" qui ont été validés par l'équipe.

Ces paquets font l'objet d'annonces officielles :

- publication d'une annonce dans la forge : <https://dev-eole.ac-dijon.fr/projects/modules-eole/news> ;
- reprise de l'annonce dans les flux RSS du site officiel du projet : <http://pctl.ac-dijon.fr/eole/> ;
- envoi d'un message sur les principales listes de diffusion du projet : <https://pctl.ac-dijon.fr/listes> ;
- publication d'un message sur le compte Twitter du pôle de compétences : <https://twitter.com/poleeole> ;
- publication d'un message sur le compte Mastodon de l'équipe EOLE : <https://mastodon.etalab.gouv.fr/@EOLE>.

Le détail des paquets disponibles est indiqué dans les journaux des versions mineures concernées (exemple : <https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Journaux252> pour EOLE 2.5.2).

Obtenir manuellement les paquets candidats

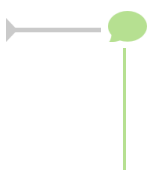
Les paquets en version candidate annoncés sont disponibles pendant la période de transition dans les dépôts candidats des dépôts du site de référence.

Ils s'installent **manuellement** à l'aide de la commande : `Maj-Auto -C`.

Obtenir automatiquement les paquets candidats

Les paquets candidats en préparation et non annoncés peuvent être obtenus **automatiquement** et à tout moment en déclarant les serveurs de test en tant que Serveur de mise à jour.

Ils s'installent à l'aide de la commande `Maj-Auto -S test-eole.ac-dijon.fr`.



Les mises à jour candidates sont testées par l'équipe EOLE, durant la période de transition et leur passage en stable, elles peuvent être installées et des remontées positives ou négatives peuvent être formulées sur la forge ou sur les listes de discussion.

Mise à jour candidate en préparation

La dénomination "mise à jour candidate en préparation" concerne les paquets prêts à être diffusés en version candidate sur une version mineure d'EOLE mais qui n'ont pas encore été annoncés officiellement.

Le détail des paquets disponibles est généralement indiqué dans les journaux des versions mineures concernées (exemple : <https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Journaux252> pour EOLE 2.5.2).

Les paquets en version candidate non annoncée sont disponibles uniquement dans les dépôts candidats du dépôt de test.

Ils s'installent à l'aide de la commande : `Maj-Auto -C -S test-eole.ac-dijon.fr`

Les mises à jour candidates sont testées par l'équipe EOLE, durant la période de transition et leur passage en stable, elles peuvent être installées et des remontées positives ou négatives peuvent être formulées sur la forge ou sur les listes de discussion.

Mise à jour de développement

Les paquets mis à disposition en version de développement sont généralement ceux de la prochaine version mineure d'EOLE qui est en cours d'élaboration.

Comme son nom l'indique, ce type de mise à jour s'adresse principalement aux développeurs et aux contributeurs qui souhaitent tester les dernières évolutions de la distribution EOLE.

Les paquets en version de développement s'installent à l'aide de la commande : `Maj-Auto -D`.

Les mises à jour de développement sont susceptibles de rendre le serveur instable. Il est fortement déconseillé de les utiliser sur un serveur en production.

Les dépôts de développement (`eole-2.5-unstable` pour EOLE 2.5) ne sont pas versionnés. Leur utilisation sur une version mineure d'EOLE précédente entraînera un changement de version du serveur.

Voir aussi...

Les dépôts EOLE ^[p.494]

1.6.2. Les procédures de mise à jour

Les procédures manuelles de mise à jour des modules EOLE sont accessible de quatre manières :

- EAD^[p.545] ;
- interface semi-graphique ;

- Zéphir ;
- ligne de commande.

De plus, à la fin de l'instanciation, une mise à jour hebdomadaire est configurée automatiquement.

⚠ Intégrité de la mise à jour

Une mise à jour EOLE représente un ensemble de paquets.

L'installation manuelle de seulement l'un d'entre eux peut rendre votre système instable.

L'utilisation des méthodes listées ci-dessus permet de garantir l'intégrité du serveur.

1.6.2.a. Mise à jour depuis l'EAD

Dans `Système / Mise à jour`, l'EAD propose une interface de mise à jour du serveur, il est possible de :

- de lister les paquets disponibles pour la mise à jour ;
- de programmer une mise à jour différée (dans 3 heures par exemple, ou dans 0 heure pour le faire tout de suite) ;
- d'activer / désactiver les mises à jour hebdomadaires (le jour et l'heure de la mise à jour automatique sont déterminés aléatoirement).

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.



💡 Rapport de mise à jour

Penser à consulter le rapport de mise à jour et l'état des services sur la page d'accueil.

🗨 Reconfiguration et redémarrage automatique

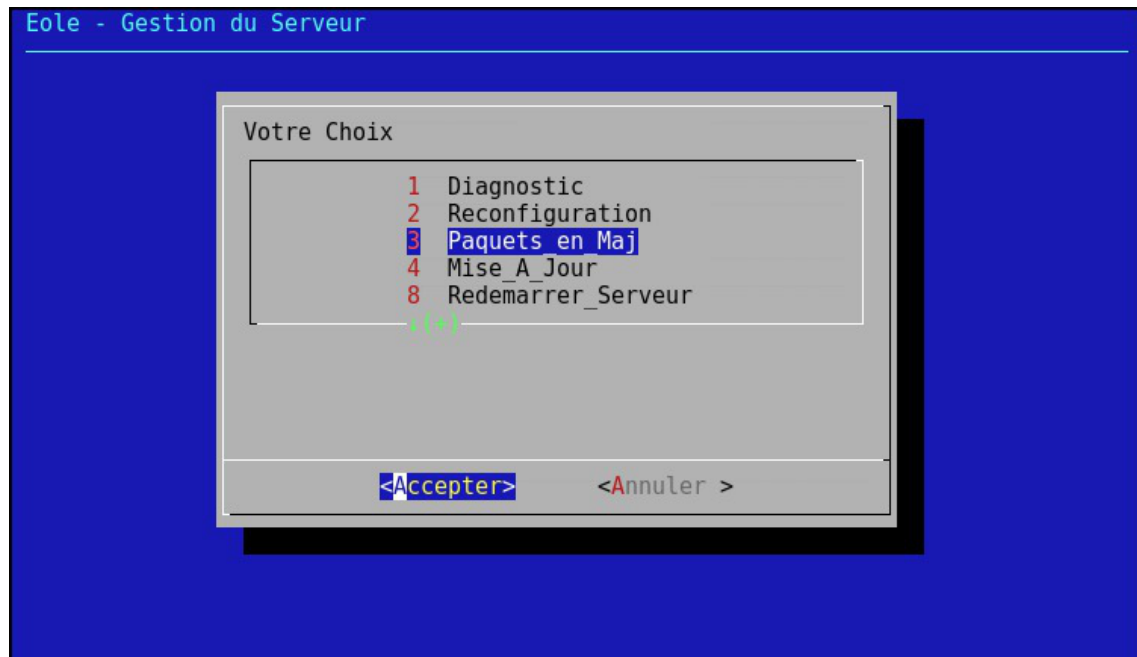
Une mise à jour lancée depuis l'EAD exécute automatiquement une reconfiguration du serveur avec la commande `reconfigure`, il n'est donc pas nécessaire d'en lancer un par la suite comme c'est le cas depuis la console.

Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

1.6.2.b. L'interface d'administration semi-graphique

En plus de l'EAD, une interface semi-graphique est disponible.

Cette interface (`manage-eole`) permet d'exécuter quelques tâches simples d'administration du serveur : diagnostique, mise à jour, liste des paquets en mise à jour, etc.



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ...

1.6.2.c. Activation automatique de la mise à jour hebdomadaire

À la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée.

La mise à jour permet de maintenir votre serveur avec le niveau de fonctionnalité le plus récent et surtout de bénéficier des dernières corrections. Certaines corrections peuvent combler des failles de sécurité importantes, il est donc important de les appliquer aussitôt qu'elles sont publiées.

Il est conseillé d'effectuer la mise à jour immédiatement, comme proposé à la fin de l'instance.

Une mise à jour est recommandée

Voulez-vous effectuer une mise à jour via le réseau maintenant ? [oui/non]

L'heure est définie aléatoirement entre 01h00 et 05h59 un des sept jours de la semaine.

Voir aussi...

➤ Gestion des tâches planifiées eole-schedule [p.474]

1.6.2.d. Les mises à jour en ligne de commande

Il est important de tenir son système à jour. Pour cela, il est possible de lancer manuellement une mise à jour.

Les commandes Maj-Auto et Query-Auto

Ces scripts sont à utiliser pour mettre à jour un module au travers d'un accès internet :

- `Maj-Auto` : télécharge et installe les paquets à mettre à jour depuis le réseau ;
- `Query-Auto` : télécharge et affiche la liste des paquets à mettre à jour depuis le réseau.

Sans préciser d'option, ces deux commandes affichent, téléchargent et installent des paquets stables, ils permettent également de tester (sur une machine dédiée aux tests) :

- les paquets candidats lors de la sortie d'une version candidates avec l'option `-C` ;
- les paquets de développements au fil de l'eau avec l'option `-D` .

Il est également possible de simuler l'installation avec l'option `-n` ou de seulement télécharger en cache les paquets `--download` .

⚠ Reconfiguration

À la fin de l'exécution de la commande `Maj-Auto` , si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur avec la commande `reconfigure` .

La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état intermédiaire qui pourrait s'avérer instable.

Reconfigurer applique les changements venants des mises à jour tout en tenant compte de la configuration telle que définie lors de la configuration du serveur.

La version candidate (nommée aussi RC pour Release Candidate) est une version d'EOLE qui correspond, du côté pratique, à la version stable. Elle est mise à disposition à des fins de tests de dernière minute visant à déceler les toutes dernières erreurs subsistant avant la sortie définitive de la version.

Tester les paquets candidats permet :

- de contribuer et de participer à l'amélioration du projet ;
- une validation par les utilisateurs des comportements attendus ;
- de faire remonter des dysfonctionnements avant la publication définitive.

Les commandes Maj-Cd et Query-Cd

`Maj-Cd` et `Query-Cd` sont les scripts à utiliser pour mettre un module à jour depuis un CD-ROM d'installation plus récent que celui utilisé lors de l'installation :

- `Maj-Cd` : installe les paquets à mettre à jour depuis un CD-ROM ;
- `Query-Cd` : affiche la liste des paquets à mettre à jour depuis un CD-ROM.

Les mises à jour à l'aide d'un CD-ROM ne se font que depuis un CD-ROM d'une même version mineure (par exemple : mise à jour de la version 2.5.0 avec un CD-ROM 2.5.0.1).

⚠ Reconfiguration

À la fin de l'exécution de la commande `Maj-Cd` , si des paquets ont été mis à jour, un message vous invite à reconfigurer votre serveur avec la commande `reconfigure` .

La reconfiguration est nécessaire car les paquets mis à jour ont copié leurs propres fichiers de configuration, le serveur est donc dans un état intermédiaire qui pourrait s'avérer instable.

Reconfigurer applique les changements venants des mises à jour tout en tenant compte de la configuration telle que définie lors de la configuration du serveur.

Options de mise à jour

Options communes aux scripts de mise à jour

- -f : passer outre les autorisations Zéphir ;
- -h : affiche l'aide ;
- -d : mode debug ;
- -W : génère une sortie formatée pour l'EAD^[p.545].

Options spécifiques aux scripts Maj-Auto et Query-Auto

- -C : force la mise à jour en version candidate ;
- -D : force la mise à jour des paquets en développement ;
- -S : force le site de mise à jour EOLE (ex : -S test-eole.ac-dijon.fr) ;
- -U : force le site de mise à jour Ubuntu (ex : -U fr.archive.ubuntu.com) ;
- -V : force le site de mise à jour Envole (ex : -V test-eole.ac-dijon.fr).

Options spécifiques aux scripts Maj-Auto et Maj-Cd

- -n : exécuter en mode simulation (*dry run*) équivaut à utiliser les commandes `Query-Auto` ou `Query-Cd` ;
- -r : exécuter reconfigure après une mise à jour réussie ;
- -R : exécuter reconfigure après une mise à jour réussie et redémarrer si nécessaire.

Options spécifiques au script Maj-Auto

- --download : procéder uniquement au téléchargement des paquets en cache.



L'utilisation des options `-C` ou `-D` entraîne un avertissement et une demande de confirmation.

Toutes les options sont documentées dans les pages de manuel de chaque commande :

```
# man Maj-Auto
```

Voir aussi...

Les dépôts EOLE ^[p.494]

Reconfiguration ^[p.297]

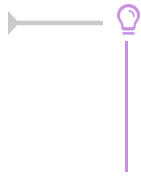
1.6.3. Ajout de dépôts supplémentaires

Les outils `Query-Auto`, `Query-Cd`, `Maj-Auto` et `Maj-Cd` réinitialisent systématiquement la liste des dépôts à utiliser pour les mises à jour et donc les fichiers `/etc/apt/sources.list`.

Pour déclarer des dépôts supplémentaires, il est possible d'ajouter des fichiers possédant l'extension `.list` dans le répertoire `/etc/apt/sources.list.d`.

En mode conteneur, chacun des conteneurs utilise son propre répertoire. Il est donc possible de mettre

en place des sources différentes en fonction du conteneur.



Pour tester les dépôts ajoutés, il est possible de lancer manuellement la mise à jour des sources avec la commande :

```
# apt-get update
```

1.7. Installation manuelle de paquets

Il est possible d'installer manuellement des paquets :

- pour installer des fonctionnalités additionnelles au module ;
- pour éventuellement installer de manière sélective des mises à jour en vue de les tester.

Avant de procéder à l'installation d'un paquet, il faut s'assurer que les sources APT^[p.541] sont configurées sur le bon type de mises à jour (stable, candidate, développement) et que la liste des paquets est à jour. Cela s'effectue avec la commande `Query-Auto` :

- mises à jour stables : `Query-Auto` ;
- mises à jour candidates : `Query-Auto -C` ;
- mises à jour de développement : `Query-Auto -D` ;

Ensuite il faut utiliser la commande `apt-eole` qui procède au téléchargement et à l'installation.

Au même titre que la commande `apt-get`, la commande `apt-eole` utilise APT^[p.541] et permet de gérer les paquets et leurs mises à jour.

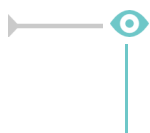
L'usage de la commande `apt-eole` en lieu et place de la commande `apt-get` est recommandée pour l'installation des paquets EOLE.

La commande `apt-eole` s'utilise comme `apt-get` :

```
# apt-eole install nomDuPaquet
```

Pour installer un paquet dans un conteneur, il faut utiliser l'option `--container` :

```
# apt-eole --container <conteneur> install nomDuPaquet
```



Pour installer le paquet `eole-bareos` :

```
# apt-eole install eole-bareos
```



La commande `apt-eole` appelle la commande `apt-get` avec les options adéquat (notamment les opérations **install** et **remove**) pour répondre aux besoins d'administration des modules EOLE :

- elle n'est pas interactive pour fluidifier l'installation, le paramétrage sera de toute façon écrasé (le paramétrage demandé par le mode interactif est fait par la mécanique EOLE selon le contexte et selon les paramètres saisis dans l'interface de configuration du

module) ;

- elle permet de pouvoir gérer les paquets et les mises à jour à l'intérieur des conteneurs^[p.543] proposés par EOLE.

Voir aussi...

Choisir le mode du module [p.58]

Les mises à jour en ligne de commande [p.342]

1.8. Passage d'une version d'EOLE à une autre



2.5.n vers 2.5.n+x

Le passage d'une version mineure à une autre est manuel et volontaire et se fait par l'intermédiaire de la commande `Maj-Release`.



Consulter le manuel de la commande pour voir toutes les options :

```
# man Maj-Release
```

2.5.2 vers 2.6.n

Le passage de la version mineure 2.5.2 vers une version 2.6 constitue un passage vers une version majeure. Le script `Upgrade-Auto` disponible sur le serveur permet d'effectuer manuellement la migration d'un module vers les dernières versions stables.



DKMS

La procédure de migration refusera de s'exécuter si elle détecte des pilotes compilés (DKMS ^[p.544]).

Les DKMS sont en effet susceptibles de faire échouer la procédure : impossibilité de démarrer sur le nouveau noyau, fichier présent dans le paquet DKMS fourni par un autre paquet en standard...

Pour des structures avec un faible débit réseau il est possible de limiter la taille du téléchargement en utilisant une image ISO stockée sur une clef USB ou un cédérom. Dans ce cas, seuls les paquets plus récents que ceux présents sur l'image ISO seront téléchargés.



- `Upgrade-Auto --cdrom` permet de copier le contenu du nouveau CD d'installation EOLE et évite le téléchargement de l'image ISO et des paquets présents sur le CD.
- `Upgrade-Auto --download` permet de ne procéder qu'au téléchargement de l'image ISO de la version cible. La migration n'est effectuée qu'après un nouvel `Upgrade-Auto`.
- `Upgrade-Auto --iso <chemin de l'image ISO>` permet de copier le contenu de l'image ISO d'installation EOLE, évite son téléchargement et évite le téléchargement des paquets présents sur le CD.
- Ajouter l'option `--download` à la commande `Upgrade-Auto --cdrom` permet de copier le contenu du nouveau CD d'installation EOLE. La migration n'est effectuée qu'après un nouvel `Upgrade-Auto`.
- Ajouter l'option `--download` à la commande `Upgrade-Auto --iso <chemin de l'image ISO>` permet de ne procéder qu'à la copie de l'image ISO. La migration n'est effectuée qu'après un nouvel `Upgrade-Auto`.
- L'option `--limit-rate <bande passante>` permet de personnaliser la limite de la bande passante à utiliser pour le téléchargement. Sa valeur est par défaut fixée à `120k` (120 kilooctets). Cette option est passée directement à la commande `wget`, la valeur `0` désactive la limitation.

Exemples d'utilisation

```
# Upgrade-Auto --limit-rate 0
# Upgrade-Auto --limit-rate 120k
# Upgrade-Auto --download --limit-rate 10M
```



Consulter le manuel de la commande pour voir toutes les options :

```
# man Upgrade-Auto
```

1.9. Passage d'une version RC à une version stable

Avant d'être publiée en version RC la distribution Linux EOLE a subi de nombreux tests. Aussi elle ne contient plus aucun changement qui ne peuvent être résolu par mise à jour.

Il est donc possible d'installer une version EOLE RC, de la tester, de l'utiliser et de la mettre à jour pour être au même niveau de mise à jour que la version stable une fois que cette dernière version est publiée. La mise à jour se fait avec la commande `Maj-Auto`.



Les versions RC porte un numéro, il signifie uniquement qu'une image ISO a été régénérée, un nombre conséquent de paquet ont été recompilés et cela évite une trop grosse mise à jour.

2. Fonctionnalités de l'EAD propres au module Amon

2.1. Rôles et association de rôles

L'EAD est composé, d'*actions*. Chaque action ayant un but bien précis.

L'EAD dispose d'un mécanisme de délégation d'*actions* à des utilisateurs déterminés.

Pour affecter certaines actions à un utilisateur, l'EAD utilise une mécanisme interne : les **rôles**.



Par défaut sur les modules EOLE, l'utilisateur **admin** est associé au rôle **administrateur**.

Plusieurs rôles sont prédéfinis sur les différents modules EOLE et certains sont propres à certains d'entre eux :

- administrateur ;
- professeur (utilisé sur le module Scribe) ;
- élève (utilisé sur le module Scribe) ;
- administrateur de classe (utilisé sur le module Scribe) ;
- administratif dans Scribe (utilisé sur le module Scribe) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon) ;
- administrateur du Scribe (utilisé sur le module AmonEcole) ;
- administrateur de l'Amon (utilisé sur le module AmonEcole).

2.1.1. Gestion des rôles

Les rôles de l'EAD sont déclarés dans les fichiers : `/usr/share/ead2/backend/config/perms/perm_*.ini`

Ces fichiers au format INI^[p.549] permettent d'associer des actions (permissions) à un ou plusieurs rôles.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/perm.ini` : rôles de base ;
- `/usr/share/ead2/backend/config/perm_<module>.ini` : rôles spécifiques au module installé (ex : `perm_scribe.ini`) ;
- `/usr/share/ead2/backend/config/perm_local.ini` : rôles déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/perm_acad.ini` : rôles déclarés au niveau académique (via Zéphir) ;
- ainsi que tout les fichiers `perm_*.ini` présents dans le répertoire `/usr/share/ead2/backend/config/perms`.

Syntaxe des fichiers

Les permissions associent un rôle à une ou plusieurs actions.

Les fichiers `perm*.ini` doivent posséder une section `[role]` et une section `[permissions]`.

```
[role]
nom du role = libelle du role

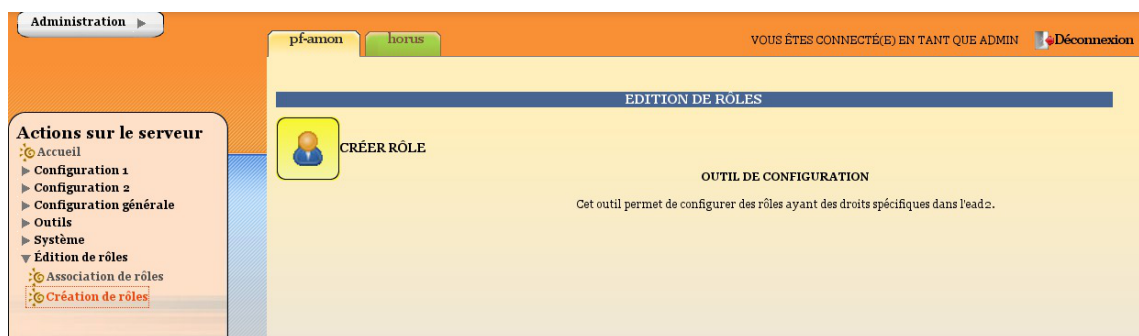
[permissions]
action1 = nom du role
action2 = nom du role
```

Création de rôle via l'EAD

L'interface EAD permet de créer des rôles personnalisés.

Ces rôles ne sont, en fait, qu'une liste d'actions regroupées sous un intitulé et un libellé unique.

Il est possible, dans un deuxième temps d'associer ces rôles à des utilisateurs.



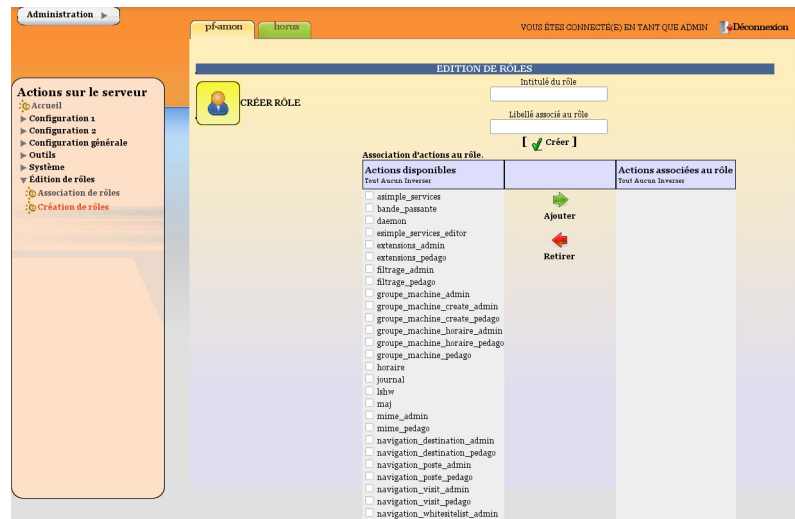
La fenêtre d'édition des rôles

Pour créer un nouveau rôle cliquer sur :

- `Édition de rôles/Création de rôles`

puis

- `Créer rôle`
- entrer l'intitulé (le nom) du rôle (sans caractère spécial, sans accent et sans espace) ;
- entrer un libellé (courte description) du rôle ;
- cocher les actions à autoriser ;
- ajouter ;
- créer.



Création d'un rôle

Actions obligatoires

Certaines actions doivent être obligatoirement permises pour tous les utilisateurs :

- **help** : utilisé notamment pour l'affichage d'aide ;
- **main_status** : page d'accueil appelée par défaut, elle gère un rôle prof (n'affiche pas les états de services) et un rôle admin ;
- **update_ead** : outil de téléchargement des javascripts, CSS, images spécifiques au module.

Actions communes aux différents modules

- **lshw** : listing matériel ;
- **maj** : action de mise à jour ;
- **daemon** : relancer des services (mode expert) ;
- **simple_services_editor** : éditer des groupes de services pour le mode simplifié ;
- **simple_services** : redémarrer/arrêter les services (mode simplifié) ;
- **server-configure/server-reboot/server-stop** : redémarrer/arrêter/reconfigurer le serveur ;
- **role_editor** : création de rôles ;
- **role_manager** : association de rôle (appelée par d'autres actions).

Actions spécifiques au module Amon

La modification du système de filtrage sur le module Amon apporte de profondes modifications sur ce module.

Selon les choix effectués lors de la phase de configuration avec l'interface de configuration du module, vous pouvez choisir d'utiliser une ou deux zones de configuration pour le filtrage et les options du pare-feu.

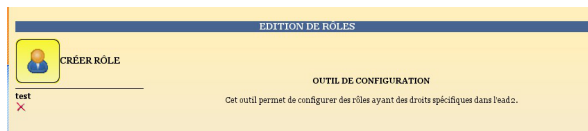
La zone 1 correspond à la réseau admin et la zone 2 correspond au réseau pedago.

- Gestion des postes
 - **navigation_poste_admin** (ou pedago) : action de gestion des postes à interdire ;
 - **navigation_destination_admin** (ou pedago) : interdire des destinations.

- Gestion des groupes de machine
 - **groupe_machine_admin** (ou pedago) : action d'entrée pour la gestion des groupes de machine (gère des restrictions pour le rôle prof) ;
 - **groupe_machine_create_admin** (ou pedago) : action de création de groupe de machine (nécessite groupe_machine) ;
 - **groupe_machine_horaire_admin** (ou pedago) : action de gestion des horaires pour les groupes de machine.
- Gestion des utilisateurs
 - **navigation_banned_user_admin** (ou pedago) : action de gestion des utilisateurs à interdire ;
 - **navigation_moderateur_admin** (ou pedago) : action de gestion des modérateurs ;
 - **navigation_whitelist_admin** (ou pedago) : action de gestion des utilisateurs en liste blanche ;
 - **navigation_whitesitelist_admin** (ou pedago) : action de gestion des sites en liste blanche.
- Gestion des sites
 - **opt_filters_admin** (ou pedago) : gestion des filtres optionnels pour la zone de configuration 1 (ou 2) ;
 - **filtrage_admin** (ou pedago) : gestion du mode de filtrage syntaxique pour la zone de configuration 1 (ou 2) ;
 - **sites_interdits_admin** (ou pedago) : gestion des sites interdits pour la zone de configuration 1 (ou 2) ;
 - **sites_autorises_admin** (ou pedago) : gestion des sites autorisés pour la zone de configuration 1 (ou 2) ;
 - **extensions_admin** (ou pedago) : gestion des extensions interdites pour la zone de configuration 1 (ou 2) ;
 - **mime_admin** (ou pedago) : gestion des types mime interdits pour la zone de configuration 1 (ou 2).
- Gestion des règles du pare-feu
 - **regles** : mode de fonctionnement du pare-feu ;
 - **peertopeer** : autorisation/interdiction du peer to peer ;
 - **horaire** : horaire de fonctionnement du pare-feu.
- Autres actions
 - **navigation_visit** : action de consultation des logs ;
 - **filtrage_bayes** : action d'évaluation d'URL à l'aide du filtrage bayésien ;
 - **bande_passante** : outil de test de bande passante.

Modification et suppression de rôle via l'EAD

- Pour modifier un rôle, il suffit de cliquer sur le nom voulu ;
- pour le supprimer, cliquer sur la croix rouge associée.



Modification/suppression d'un rôle

2.1.2. Association des rôles

Les associations de rôle de l'EAD sont déclarées dans les fichiers :
`/usr/share/ead2/backend/config/roles/roles_*.ini`

Ces fichiers au format INI^[p.549] permettent d'associer des rôles à un ou plusieurs utilisateurs.

Fichiers pris en compte

Sur un module EOLE, seuls les fichiers suivants sont pris en compte :

- `/usr/share/ead2/backend/config/roles.ini` : associations de base (admin, eleve, prof, ...)
- `/usr/share/ead2/backend/config/roles_<module>.ini` : associations spécifiques au module installé (ex : `roles_scribe.ini`) ;
- `/usr/share/ead2/backend/config/roles_local.ini` : associations déclarés localement (édition manuelle ou via l'EAD) ;
- `/usr/share/ead2/backend/config/roles_acad.ini` : associations déclarés au niveau académique (via Zéphir).

Syntaxe des fichiers

L'association d'un rôle se fait à partir du login d'un utilisateur système (section `[pam]`) ou de la valeur associée à un attribut ldap (section `[nom_attribut]`) de l'annuaire utilisé pour l'authentification SSO sur l'EAD du module.

```
[pam]
scribe2=admin
[uid]
.jean.dupont=prof admin
[user_groups]
minedu=admin horus
```

La clé spéciale `[user_groups]` permet d'attribuer un rôle à tous les membres d'un groupe déclaré dans l'annuaire LDAP.

Création d'association via l'EAD

Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

Certaines de ces informations sont utilisées pour lui attribuer des rôles et ainsi lui donner accès à certaines actions.

Pour associer un rôle à des utilisateurs:

- dans **Édition des rôles/Association de rôle** ;
- cliquer sur **Associer Rôle** .



La fenêtre d'association de rôles

- choisir la clef (attribut de l'utilisateur) ;
- renseigner la valeur recherchée pour cet attribut (dans le cas d'une authentification locale on mettra le login de l'utilisateur) ;
- choisir le rôle à associer ;
- valider.



Association d'un rôle

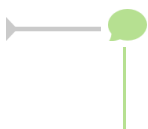
L'intitulé de la clef dépend du système d'authentification utilisé pour se connecter :

Authentification locale :

- le login de l'utilisateur.

Authentification SSO :

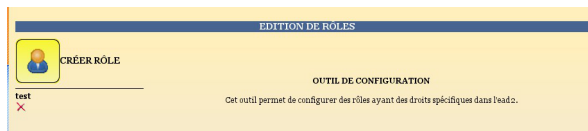
- l'élève fait partie de la classe ;
- la valeur de la clé LDAP typeadmin :
 - 0 → enseignant
 - 1 → administrateur
 - 2 → enseignant responsable de classe
 - 3 → personnel administratif
- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.



Il est indispensable de redémarrer le service ead-server dans **Système->Services (mode expert)** pour que les modifications soient prises en compte.

Suppression d'une association via l'EAD

Une association de rôle peut par la suite être supprimée en cliquant sur la croix rouge.



Modification/suppression d'un rôle

2.1.3. Les rôles sur le module Amon

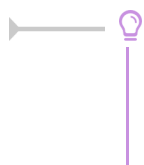
L'EAD est accessible aux utilisateurs locaux *root* et *eole*.

Si l'authentification SSO est configurée, il est également accessible à l'utilisateur *admin*.

En fonction de l'utilisateur un rôle différent peut être appliqué. À chaque rôle est affecté différentes actions.

Dans le cadre du module Amon, les rôles importants sont les suivants :

- administrateur : accès à toutes les actions (ex. redémarrage des services, mise à jour du serveur, création et affectation des rôle aux autres utilisateurs, etc.) ;
- administrateur du réseau pédagogique (utilisé sur le module Amon).



Il est possible de créer davantage de rôles ayant accès à diverses actions afin, par exemple, de donner le droit à un professeur de pouvoir redémarrer un groupe de services en plus de ses autorisations de base.

Accès "Administrateur"

Par défaut, les utilisateurs *admin*, *root* et *eole* ont accès à toutes les fonctions.

L'accès avec les utilisateurs *root* et *eole* s'effectue en utilisant l'authentification locale.

Fonctionnalités Amon

L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques du proxy ;
- redémarrage des services ;
- mise à jour ;
- arrêt/redémarrage du serveur ;
- gestion des rôles EAD.

Accès "Administrateur du réseau pédago"

Dans le cas où plusieurs filtres web (instances de e2guardian) sont configurés, ce rôle permet de

déléguer la gestion des options de filtrage pour le filtre n°2, traditionnellement associé à la zone pédagogique.



2.2. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles^[p.544].

Une règle peut être :

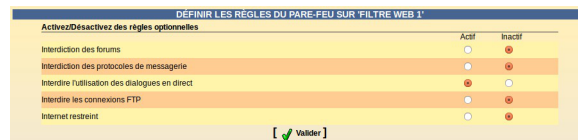
- générale, si elle concerne l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone.

La configuration générale est accessible par le menu EAD : Configuration générale / Règles du pare-feu .

La configuration spécifique est accessible par le menu EAD : Filtre web X / Règles du pare-feu :

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



Activation des directives optionnelles dans l'EAD

⚠ Lien entre ERA et les directives optionnelles de l'EAD

Pour les règles optionnelles, l'EAD prime sur l'ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comme étant active par défaut dans ERA et ne pas être active car désactivée dans l'interface EAD.

Voir aussi...

Les directives optionnelles ^[p.397]

2.3. Exceptions sur la source ou la destination

Par défaut, tous les accès à des sites nécessitent une authentification (si elle est active) et toutes les machines du réseau doivent s'identifier. Mais certains systèmes ou logiciels doivent pouvoir se mettre à jour de façon transparente.

Par ailleurs, le proxy conserve une version des pages téléchargées en cache pour limiter la consommation réseau. Ce comportement n'est pas adapté à tous les sites.

Pour les sites comportant des données sensibles, il est nécessaire de s'assurer que des données relatives à la navigation sur ce domaine ne soient pas placées dans le cache du serveur.

Certaines machines peuvent également avoir besoin de naviguer avec des données provenant directement du site consulté.

Certains postes clients ou serveurs du réseau ont besoin d'effectuer des mises à jour automatiquement, les sites de mise à jour doivent être accessibles sans authentification.

Certaines machines peuvent également avoir besoin de naviguer sans être authentifiées.

Pour cela, il existe deux mécanismes :

- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

Pour paramétrer les destinations et les sources qui n'utiliseront pas le cache ou l'authentification lors de la navigation il faut se rendre dans **Configuration générale** puis **Cache et Authentification** de l'interface EAD du module.

Cache et authentification de la destination

Dans **Configuration générale** / **Cache et Authentification** / **Destinations** :

- entrer l'adresse IP ou le nom du domaine ;
- cocher authentification et/ou cache ;
- valider.

Ajout d'une destination à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

Destination	Cache	Authentification
10.121.58.5	✗	✗
ac-dijon.fr	✗	✗
scribe		✗

Listes des destinations à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Cache et authentification de la source

Dans **Configuration Générale** / **Cache et Authentification** / **Sources** :

- entrer l'adresse IP ou réseau
- cocher authentification et/ou cache ;

- valider.

Machine ou réseau source à ajouter

Ne pas utiliser le cache du proxy

Ne pas authentifier les accès

[Valider]

Ajout d'une source à ne pas authentifier et/ou pour laquelle ne pas utiliser le cache

Pour supprimer une référence, cliquer sur la croix rouge correspondante :

Source	Cache	Authentification
10.121.58.5	×	×
10.21.58.10	×	×
172.16.0.0/24		×
172.16.0.6	×	×

Listes des sources à ne pas authentifier et/ou pour lesquelles ne pas utiliser le cache

Personnalisations académiques

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid3/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/src_noauth_acad` : liste de sources à ne pas authentifier ;
- `/etc/squid3/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid3/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père.



L'utilisation du fichier `/etc/squid3/domaines_noauth_acad` pour gérer la liste de destinations à ne pas authentifier est dépréciée depuis la version 2.5.2. Il faut utiliser la fonctionnalité de l'onglet `Exceptions proxy` de l'interface de configuration du module.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD ^[p.267]

2.4. Filtrage web

Avec le filtrage web, il est possible :

- de configurer la manière dont le filtrage s'effectue ;
- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des utilisateurs (seulement si l'authentification est activée durant la phase de configuration) ;

- d'associer une politique de filtrage (interdits, modérateurs, liste blanche...) à des machines.

Cette configuration s'effectue :

- par zone de configuration ;
- de manière plus fine, par politique de filtrage ;
- de façon prioritaire sur les utilisateur puis sur les machines si l'authentification est désactivée sinon de façon prioritaire sur les machines puis sur les utilisateurs.

2.4.1. Filtrage par utilisateur

Si l'authentification a été activée sur la zone durant la phase de configuration, il est possible de définir, pour l'utilisateur, une des politiques de filtrage suivante :

- modérateur (lorsqu'un site est interdit, un lien lui est proposé pour outrepasser l'interdiction) ;
- interdits (aucune navigation web n'est possible pour cet utilisateur) ;
- mode liste blanche (seuls les sites de la liste blanche sont autorisés) ;
- politique de filtrage web spécifique.

Placer un professeur sur la liste des modérateurs pour la zone de filtre web 1

Il est parfois intéressant de voir un site interdit, qui, parfois, empêche l'accès à un contenu pédagogique. En définissant un professeur comme modérateur, on lui permet d'outrepasser l'interdiction de navigation et, le cas échéant, le placer sur la liste des sites autorisés.

Dans **Filtre web 1 / Utilisateurs** :

- entrer le nom de l'utilisateur ;
- valider ;
- choisir **Modérateur** dans la liste.

Login des utilisateurs	politique de filtrage	suppression
user-interdit	interdits	×
user-moderateur	modérateur	×
user-pol1	Défaut	×
user-whiteisted1	liste blanche	×

Configurer des politiques de filtrage pour un utilisateur sur la zone de filtre web 2

Ces informations sont stockées dans :

`/var/lib/blacklists/dansguardian<num_instance>/common/filtergroupslis`

Sur **AmonEcole**, ces fichiers sont dans le conteneur **reseau**.

Si le menu **Utilisateurs** n'apparaît pas, c'est que la zone n'est pas authentifiée.

2.4.2. Filtrage par machine ou par groupe de machine

Présentation

Le module Amon propose de gérer des groupes de machine par plage d'adresse IP.

En ajoutant une référence à ce groupe, il est possible :

- de lui interdire l'accès au réseau ;
- de lui interdire la navigation web seulement ;
- de lui autoriser la navigation web selon des horaires ;
- de lui associer une politique de filtrage web spécifique.



Les informations liées aux groupes de machine sont stockées dans :

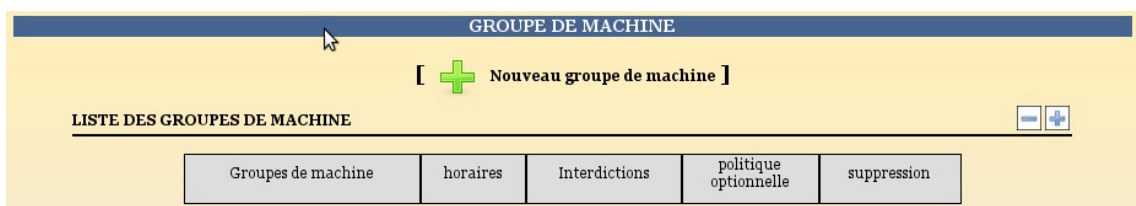
```
/usr/share/ead2/backend/tmp/ipset_group<num_instance>.txt
```

Les éventuelles plages horaires associées sont dans :

```
/usr/share/ead2/backend/tmp/ipset_schedules<num_instance>.pickle
```

Créer un groupe de machine

Pour configurer un groupe de machine de la zone 1, aller dans **Filtre web 1 / Groupe de machine**.



Interface de gestion de groupe de machine

Cliquer sur **Nouveau groupe de machine** et un formulaire de création apparaît.


Formulaire de création

Remplir :



- nom pour le groupe de machine (sans accents ni caractères spéciaux) ;
- donner l'adresse IP de début de plage ;
- donner l'adresse IP de fin de plage ;
- si plusieurs interfaces réseau sont associés à cette zone, il vous demandera le nom de l'interface ;
- valider.

Le groupe de machine est dans la liste et peut être géré.

GRUPE DE MACHINE

[ Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE [-] [+]

Groupes de machine	horaires	Interdictions	politique optionnelle	suppression
bibliotheque plage IP: 192.168.230.10 à 192.168.230.20 sur l'interface eth1		Jamais	Défaut	

Le groupe de machine est ajouté

S'il ne vous est pas possible de choisir l'interface de votre groupe lors de sa création, c'est qu'une seule interface du pare-feu est associée à cette zone.

À partir de la version 2.5.2 d'EOLE, il n'est plus obligatoire que la plage d'adresse du groupe soit de classe C.

Un trop grand nombre d'adresses dans un groupe peut entraîner une baisse de performance.

Limiter l'accès réseau

Dans la colonne **Interdictions**, il est possible de choisir parmi :

- jamais ;
- le web tout le temps ;
- le web selon des horaires (à définir au préalable) ;
- toute activité réseau.

Interdire le groupe de navigation web

Dans la colonne **Interdictions**, choisir **Le web tout le temps**

Le groupe de machine est alors interdit d'accès sur les ports :

- 80 (HTTP)
- 443 (HTTPS)
- 3128 (e2guardian)
- 8080 (Squid)

Si vous désirez faire une interdiction de navigation selon des horaires, il faut :

- configurer des horaires ;
- appliquer l'interdiction.

Configuration des horaires

Dans la colonne **Interdictions**, choisir **Le web selon horaires**.

Cliquer sur l'horloge, la gestion des horaires apparaît.

GRUPE DE MACHINE

[+ Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE [-] [+]

Groupes de machine	horaires	Interdictions	politique optionnelle	suppression
secretariat plage IP: 10.21.11.15 à 10.21.11.18 sur l'interface eth1		Le web selon	1	X

DEFINIR DES PLAGES HORAIRES D'OUVERTURE POUR LE GROUPE SECRETARIAT X Fermer

Début de plage: 0:00 Fin de plage: 0:00

Choix du (des jours):

- lundi
- mardi
- mercredi
- jeudi
- vendredi
- samedi
- dimanche

OU

Copier les horaires d'un autre groupe:

[✓ Valider]

[✓ Valider]

■ Navigation interdite
■ Navigation autorisée

lundi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

Autorisation de navigation web:

mardi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

Autorisation de navigation web:

mercredi

Gestionnaire d'horaires pour les groupes de machine

- choisir la plage horaire d'autorisation ;
- choisir les jours d'applications ;
- valider.

GROUPE DE MACHINE

[+ Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE [-] [+]

Groupes de machine	horaires	Interdictions	politique optionnelle	suppression
secretariat plage IP: 10.21.11.15 à 10.21.11.18 sur l'interface eth1	🕒	Jamais ▾	Défaut ▾	✖

DEFINIR DES PLAGES HORAIRES D'OUVERTURE POUR LE GROUPE SECRETARIAT ✖ Fermer

Début de plage: 13:30 ▾ Fin de plage: 18:30 ▾

Choix du (des jours)

- lundi
- mardi
- mercredi
- jeudi
- vendredi
- samedi
- dimanche

OU

Copier les horaires d'un autre groupe ▾

[✓ Valider]

[✓ Valider]

Navigation interdite
 Navigation autorisée

lundi

0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

✖

Autorisation de navigation web:
 de 8:00 à 12:00

mardi

0 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h 0

✖

Autorisation de navigation web:
 de 8:00 à 12:00

mercredi

Remplir le formulaire

Les plages horaires définies s'affichent (la croix permet de supprimer la plage).

GRUPE DE MACHINE

[+ Nouveau groupe de machine]

LISTE DES GROUPES DE MACHINE [-] [+]

Groupes de machine	horaires	Interdictions	politique optionnelle	suppression
secretariat plage IP: 10.21.11.15 à 10.21.11.18 sur l'interface eth1		Jamais	Défaut	X

DEFINIR DES PLAGES HORAIRES D'OUVERTURE POUR LE GROUPE SECRETARIAT X Fermer

Début de plage: 0:00 Fin de plage: 0:00

Choix du (des) jours:

- lundi
- mardi
- mercredi
- jeudi
- vendredi
- samedi
- dimanche

OU

Copier les horaires d'un autre groupe:

[✓ Valider]

[✓ Valider]

■ Navigation interdite
■ Navigation autorisée

lundi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

■ 01h-07h ■ 08h-12h ■ 13h-17h ■ 18h-23h

Autorisation de navigation web:
 de 8:00 à 12:00
 de 13:30 à 18:30

mardi

o 01h 02h 03h 04h 05h 06h 07h 08h 09h 10h 11h 12h 13h 14h 15h 16h 17h 18h 19h 20h 21h 22h 23h o

■ 01h-07h ■ 08h-12h ■ 13h-17h ■ 18h-23h

Autorisation de navigation web:
 de 8:00 à 12:00
 de 13:30 à 18:30

Affichage des plages horaires

Sans plage horaire définie, la navigation web est interdite tout le temps

La modification des plages horaires est dynamique.

Si le groupe de machine est interdit de navigation web selon horaires, il est possible de modifier les plages horaires.

Il est aussi possible de copier les horaires depuis un autre groupe de machine.

- choisir le groupe dans la liste ;
- valider.

Interdire l'accès au réseau

Pour interdire tout accès réseau à notre groupe de machine, dans la colonne **Interdictions**, choisir **Toute activité réseau**.

Spécifier une politique de filtrage

Il est possible d'associer une politique de filtrage au groupe de machine. Pour cela choisir la politique dans la colonne **politique optionnelle**.

Certaines politiques de filtrage sont fixes :

- modérateur ;
- interdit ;

- mode liste blanche.

D'autres sont configurables :

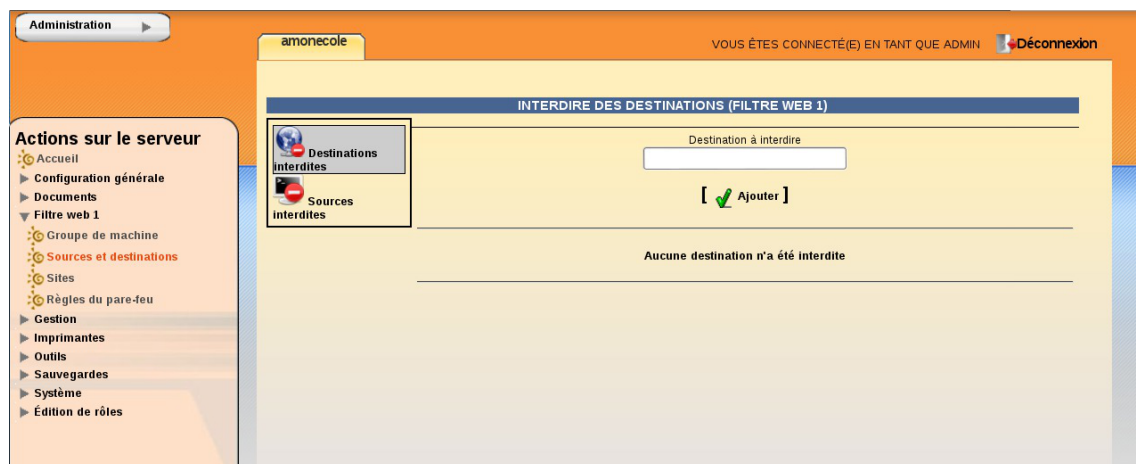
- Défaut ;
- 1 ;
- 2 ;
- 3 ;
- 4.

Supprimer un groupe de machine

Pour supprimer un groupe de machine, cliquez sur la croix en face de votre groupe de machine.

2.4.3. Interdire l'accès à un sous-réseau depuis une interface

Dans l'EAD il est possible d'interdire l'accès à un sous-réseau depuis une interface.



Vue d'ensemble pour l'ajout d'une destination à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut **Filtre web 1**. Puis sélectionner **Sources et destinations** et enfin **Destinations interdites**.

Pour interdire une destination il faut :

- définir le sous-réseau (ou le poste) de destination ;
- choisir l'interface source depuis laquelle interdire l'accès (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné).

Nommage des filtres dans la configuration du filtrage web

Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) [p.226]

Interdire l'accès au sous-réseau 10.121.11.0/255.255.255.0 depuis l'interface admin (eth1)

Ajout d'une destination à interdire

Soit l'interface eth1 sur la zone de filtre web 1.

- Saisir `10.121.11.0/255.255.255.0` dans `Destinations à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des destinations interdites. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Destinations interdites`.

Suppression d'une destination interdite

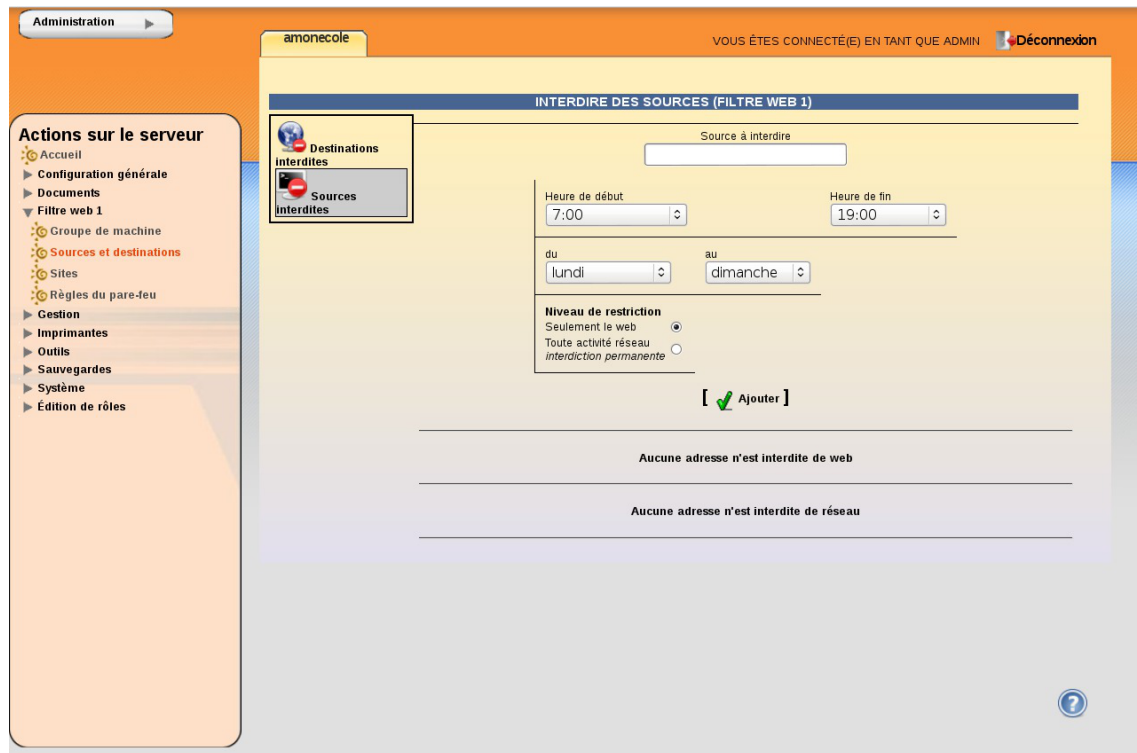
- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur `Supprimer`.

Les destinations interdites sont écrites dans :

```
/usr/share/ead2/backend/tmp/dest_interdites<num_instance>.txt
```

2.4.4. Interdire ou restreindre l'activité d'un sous-réseau

Dans l'EAD il est possible d'interdire l'accès web en fonctions de plages horaires ou d'interdire l'activité à tout un sous-réseau .



Vue d'ensemble pour l'ajout d'une source à interdire

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut **Filtre web 1** . Puis sélectionner **Sources et destinations** et enfin **Sources interdites** .

Les paramètres à saisir sont :

- la Source à interdire : le sous-réseau (ou poste) sur lequel les restrictions doivent être appliquées ;
- l'Interface associée à l'adresse (n'apparaît que s'il existe plusieurs interfaces rattachées au filtre web sélectionné) ;
- les plages horaires et journalières de la restriction (restriction web uniquement) ;
- le Niveau de restriction : web ou réseau.

Interdire l'accès web depuis le sous-réseau 10.21.11.0/255.255.255.0 provenant de l'interface eth1 tous les jours entre minuit et 6 heures du matin

Ajout d'une source à interdire

Soit l'interface eth1 sur la zone de filtre web 1 :

- Saisir `10.121.11.0/255.255.255.0` dans `Source à interdire` ;
- Choisir `admin (eth1)` dans la liste `Interface associée à l'adresse` ;
- Sélectionner `0:01` comme heure de début et `06:30` comme heure de fin ;
- Sélectionner les jours : du lundi au dimanche ;
- Choisir `Seulement le web` comme `Niveau de restriction` ;
- Cliquer sur `Ajouter`.

Un message de confirmation "L'adresse 10.121.11.0/255.255.255.0 a été ajoutée à la liste des postes interdits de navigation web. Le pare-feu a bien été redémarré" apparaît.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.



Suppression d'une source interdite

- Choisir l'interdiction à supprimer dans la liste ;
- Cliquer sur **Supprimer**.



Les sources interdites d'accès web sont écrites dans :

`/usr/share/ead2/backend/tmp/horaire_ip<num_instance>.txt`

Les sources interdites d'accès réseau sont écrites dans :

`/usr/share/ead2/backend/tmp/poste_all<num_instance>.txt`

Nommage des filtres dans la configuration du filtrage web

Onglet Filtrage web : Configuration du filtrage web [p.226]

2.4.5. Bases de filtres optionnels

Les bases de filtres proposées sur le module Amon sont des copies de celles gérées par l'université de Toulouse 1 Capitole : <http://cri.univ-tlse1.fr/blacklists> [<http://cri.univ-tlse1.fr/blacklists/>].



L'université de Toulouse 1 Capitoile diffuse depuis de nombreuses années une liste noire d'URLs, gérée par Fabrice Prigent afin de permettre un meilleur contrôle de l'utilisation d'Internet.

Les bases, publiées sous licence d'utilisation Creative Commons by-sa 4.0 [<http://creativecommons.org/licenses/by-sa/4.0/deed.fr>], sont largement utilisées par les écoles et sont également intégrées dans un grand nombre d'outils libres ou commerciaux, en complément d'autres listes.

Les bases sont mises à jour 2 à 3 fois par semaine en fonction des disponibilités du mainteneur, elles peuvent être enrichies grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Ces bases de filtres proposent des catégories avec des listes de domaines et d'URL triés par catégories.

Les sites référencés dans les catégories `adult` et `redirector` sont interdits d'office.

Les autres bases de filtres sont activables depuis l'interface EAD.

L'activation se fait :

- par filtre web ;
- par politique de filtrage.

La mise à jour des bases de filtres est lancée automatiquement toutes les nuits

Un rapport de mise à jour est disponible sur la page d'accueil de l'EAD.

LISTE DE SITES INTERDITS

Dernière mise à jour de la liste de sites interdits :
Mise à jour le 16.11.2012 à 02:38 :

[Afficher le rapport](#)

Rapport de mise à jour des bases de filtres

➤ Pour activer la catégorie "agressif" sur toute la zone de configuration 1

Dans `Filtre 1 / Sites / Filtres` :

- cocher les quatre cases (pour les quatre politiques de filtrage de la zone 1) ;
- valider.

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

FILTRES	DÉFAUT	1	2	3
	tous aucun	tous aucun	tous aucun	tous aucun
contenus agressifs (xenophobie...)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
audio/video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
téléphones mobiles, sonneries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radios en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
drogue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mail et chat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
webmail les plus connus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux de hasard et d'argent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
hacking (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
warez (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
triche aux examens	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bandeaux publicitaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
divers (humour...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
utilisation de proxy distants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
proxy spécifiques	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


valider

Activation de filtres optionnels

Pour activer une catégorie seulement pour une politique de filtrage^[p.558], seule la case correspondant à la politique doit être cochée.

ACTIVATION DES FILTRES FACULTATIFS SUR LA ZONE DE CONFIGURATION 1

FILTRES	DÉFAUT	1	2	3
	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>	<u>tous</u> <u>aucun</u>
contenus agressifs (xenophobie...)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
audio/video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
téléphones mobiles, sonneries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
radios en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
drogue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mail et chat	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
webmail les plus connus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux de hasard et d'argent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
jeux en ligne	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
hacking (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
warez (piratage)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
triche aux examens	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
bandeaux publicitaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
divers (humour...)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
utilisation de proxy distants	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
proxy spécifiques	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

 **Valider**

Restreindre l'activation d'un filtre à une politique

La commande suivante permet de forcer la mise à jour les bases de filtrages :

```
/usr/share/eole/Maj-blacklist.sh
```

La liste des bases de filtres d'interdiction gérées sur le module EOLE est fournie par le fichier : `/usr/share/ead2/backend/config/filtres-opt`.

La modification des filtres optionnels activés impactent les fichiers suivants :

- `/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedsitelist`
- `/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/bannedurllist`

Sur le module *AmonEcole*, ces fichiers sont dans le conteneur **reseau**.

2.4.6. Filtrage syntaxique

Configuration du filtrage syntaxique

Le module Amon filtre dynamiquement les pages web grâce au filtrage syntaxique^[p.547].

Ce système de pondération par mot clef se base sur le fichier `/var/lib/blacklists/meta/weighted` qui est mis à jour toutes les nuits, à partir des données gracieusement gérées et mises à disposition par l'académie de Rouen.

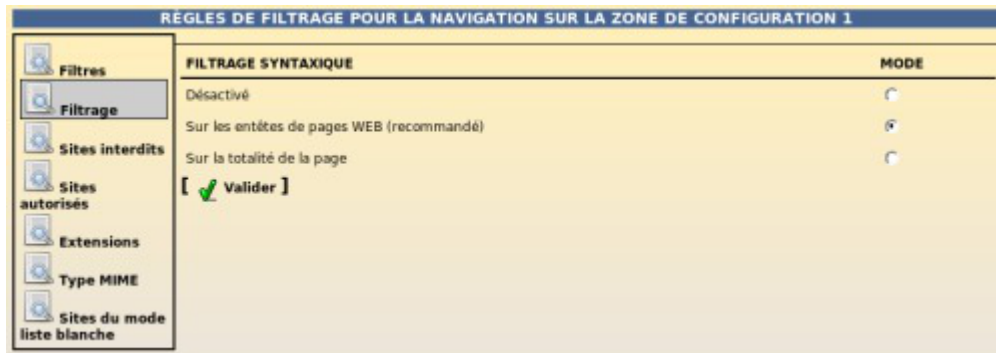
Dans l'EAD, le filtrage syntaxique peut être :

- sur les balises méta^[p.541] (par défaut) ;
- sur la page entière ;

- désactivé.

Il est possible de régler ce filtrage pour chaque zone de configuration.

Pour modifier la configuration, aller dans **Filtre web 1 / Filtrage**.



Configuration du mode de filtrage web pour la zone de configuration 1

Le mode de filtrage syntaxique choisi est enregistré dans le fichier :

```
/var/lib/eole/config/filtrage-contenu<num_instance>
```

Mode "safe search" dans les moteurs de recherche

Le proxy utilise un système de réécriture des *URL* afin que le mode "safe search" des principaux moteurs de recherche et sites d'hébergement de vidéos soit activé automatiquement.

<http://www.google.com/support/websearch/bin/answer.py?answer=510>

Certaines fonctionnalités de recherche avancée ont également été désactivées afin de limiter la charge du serveur.

Filtrage PICS

Le filtrage PICS (<http://www.w3.org/PICS>) ne s'active automatique que si le filtrage syntaxique est configuré sur la page entière.

2.4.7. Interdire et autoriser des domaines

Interdire des domaines et des URL

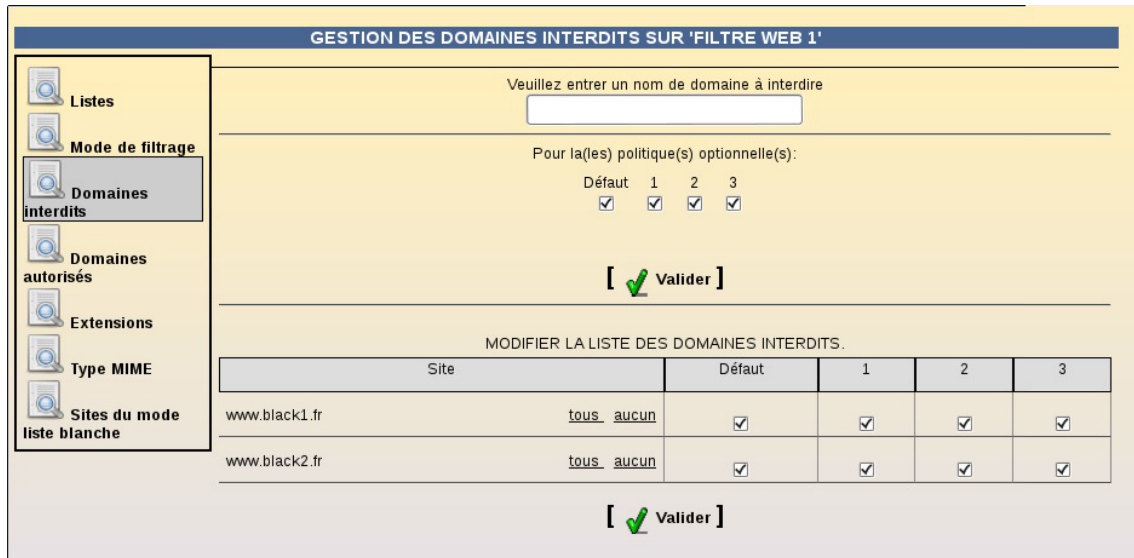
Il est possible de compléter la liste de sites interdits (liste noire^[p.551]) en ajoutant des domaines ou des URL sur la liste personnalisée de domaines interdits.

Cette liste est applicable :

- a une zone entière ;
- de manière plus fine sur une seule politique de filtrage.

Le formulaire qui permet d'interdire des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, **Filtre web 1** par défaut puis **Sites / Domaines interdits**.

Nommage des filtres dans la configuration du filtrage web : > Configuration du filtrage web (cf. Onglet Filtrage web : Configuration du filtrage web) ^[p.226]



Interdiction de domaines pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines interdits sont écrits dans :

```
/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/domains
```

Sur un module AmonEcole, ces fichiers sont dans le conteneur `internet`.

Personnalisations académiques

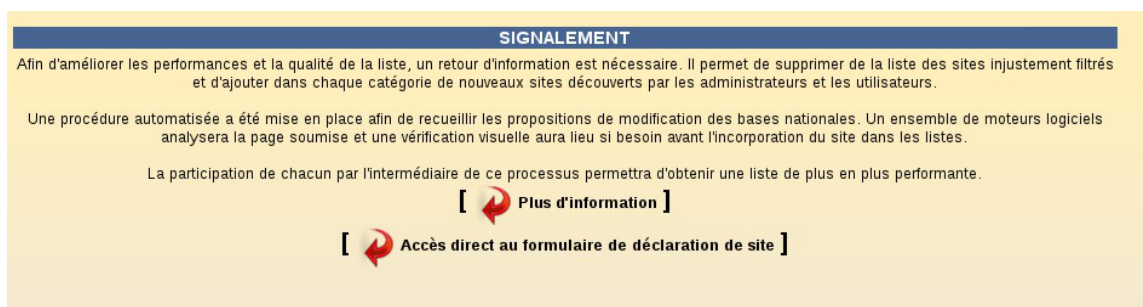
Des listes de domaines et d'URL peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/var/lib/blacklists/dansguardian<num_instance>/common/domains_acad`
- `/var/lib/blacklists/dansguardian<num_instance>/common/urls_acad`



Il est possible de signaler des domaines à interdire qui amélioreront les performances et la qualité des bases nationales de domaines interdits.

Pour cela, aller dans `Outils / Signalements`.

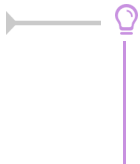


Vue du formulaire de signalement

Une procédure automatisée a été mise en place afin de recueillir les propositions de domaine à interdire dans les bases nationales.

Un ensemble de moteurs logiciels analysera l'URL soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du domaine dans les listes de domaines interdits.

La participation de chacun à ce processus permet d'améliorer les bases nationales et leur performance et ce afin que chacun puisse en bénéficier.



Il est également possible de faire un signalement directement auprès de l'université de Toulouse 1 Capitole grâce à un formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Autoriser des domaines et des URL

Il est possible de forcer l'autorisation de domaines ou d'URL (liste blanche^[p.551]) en les ajoutant à la liste des domaines autorisés.

Cette liste de domaines s'applique :

- sur une zone de filtre web portant le nom du filtre choisi dans l'interface de configuration du module ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / Sites autorisés**

Le formulaire qui permet d'autoriser des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, **Filtre web 1** par défaut puis **Sites / Domaines autorisés**.

GESTION DES DOMAINES AUTORISÉS SUR 'FILTRE WEB 1'

Veuillez entrer un nom de domaine à autoriser

Pour la(les) politique(s) optionnelle(s):

Défaut 1 2 3

[Valider]

MODIFIER LA LISTE DES DOMAINES AUTORISÉS.

Site		Défaut	1	2	3
www.white1.fr	tous aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
www.white2.fr	tous aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Valider]

Autorisation de sites pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines autorisés sont écrits dans :

```
/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/whites
```

Sur le module AmonEcole, ces fichiers sont dans le conteneur `reseau`.

2.4.8. Interdire des extensions et des types MIME

Interdire des extensions

Il est possible d'interdire des extensions, ainsi si l'URL de navigation pointe vers un fichier portant cette extension, l'accès sera interdit.

Cette interdiction s'applique :

- sur une zone de configuration ;

- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / Extensions**.

extensions	Défaut	1	2	3
.ext1	<u>tous</u> , aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
.ext2	<u>tous</u> , aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Interdiction d'extensions pour les quatre politiques de la zone de configuration 1

Les extensions interdites sont écrites dans :

```
/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/extensions
```

Sur AmonEcole, ces fichiers sont dans le conteneur reseau.

Interdire des types MIME

Il est possible d'interdire des types MIME^[p.563]. Cette interdiction fonctionne comme celle des extensions. Cette interdiction s'applique :

- sur une zone de configuration ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans **Filtre web 1 / Sites / type MIME**.

types MIME	Défaut	1	2	3
Données composites avec mentions d'octets	<u>tous</u> , aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Données composites choix	<u>tous</u> , aucun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Interdiction de types MIME pour les quatre politiques de la zone de configuration 1

Les types MIME interdits sont écrits dans :

```
/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/types_mime
```

Sur AmonEcole, ces fichiers sont dans le conteneur reseau.

2.4.9. Politique liste blanche

Le politique liste blanche^[p.551] permet de restreindre la navigation web à une liste de sites.

Le principe est "tout est interdit sauf".

Restreindre la navigation au site Wikipédia pour les utilisateurs en mode liste blanche de la zone nommée par défaut "Filtre web 2"

Dans **Filtre web 2 / Sites / Sites du mode liste blanche**

- ajouter un domaine avec ou sans sous-domaine (exemple fr.wikipedia.org) dans le champ **Ajouter un site au mode liste blanche** ;
- cliquer sur le bouton **Valider**.

Les utilisateurs et les postes ayant pour politique de filtrage "mode liste blanche" ne pourront naviguer que sur le site ajouté à la liste blanche (exemple Wikipédia).

Ajout d'un site dans la liste blanche

Supprimer un site de la liste blanche

- sélectionner le site dans la liste déroulante **SITES DU MODE LISTE BLANCHE** ;
- cliquer sur la bouton **Valider**.

Suppression d'un site dans la liste blanche



Les sites de la liste blanche sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/site_liste_blanche`

Sur un module AmonEcole, ces fichiers sont dans le conteneur **internet**.

2.5. Observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian^[p.545].

Configuration

L'accès à cet outil se paramètre dans l'interface de configuration du module, dans l'onglet expert : **Filtrage web**.



La question **Autoriser la consultation des logs liés au filtrage web dans l'EAD** propose plusieurs options :

- **oui** : accès autorisé pour les utilisateurs EAD possédant les actions **navigation_visit_admin** et/ou **navigation_visit_pedago** ;
- **non** : accès interdit pour tout le monde, personne ne voit le lien **Visites des sites** (configuration par défaut) ;
- **admin_seulement** : accès autorisé uniquement pour le rôle **admin**.

Consultation

La consultation des visites de sites se fait au travers de l'EAD, menu : **Filtre web X/visites des sites**.

DATE	LOGIN	URL	IP
2012.10.12 15:21:41	-	exch-eu.atdmt.com	172.16.0.202
2012.10.12 15:21:41	-	a.rad.msn.com	172.16.0.202
2012.10.12 15:21:43	-	leparc.ac-dijon.fr:443	172.16.0.39
2012.10.12 15:21:43	-	rad.msn.com	172.16.0.202
2012.10.12 15:21:43	-	a.rad.msn.com	172.16.0.202
2012.10.12 15:21:44	-	m.adnxs.com	172.16.0.202
2012.10.12 15:21:44	-	cm.g.doubleclick.net	172.16.0.202
2012.10.12 15:21:44	-	view.atdmt.com	172.16.0.202
2012.10.12 15:21:44	-	distributif.espace-plus.net	172.16.0.202
2012.10.12 15:21:44	-	by174w.bay174.mail.live.com	172.16.0.202

Les noms des menus (ici : **Filtre web proxy 2**) sont modifiables dans l'interface de configuration du module (variables **dansguardian_ead_filtre1** et **dansguardian_ead_filtre2**).

2.6. Outil d'analyse de logs LightSquid

LightSquid est un analyseur de logs pour le proxy/cache Squid^[p.561].

Les statistiques générées manuellement ou automatiquement par cet outil sont consultables dans l'interface EAD.

<http://lightsquid.sourceforge.net/>

Configuration

LightSquid se paramètre dans l'interface de configuration du module, dans l'onglet expert **Squid**. Pour activer la génération automatique des statistiques (toutes les nuits) il faut passer la variable Générer les statistiques Squid automatiquement à oui. Le port par défaut est 8062.

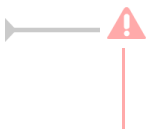


Paramétrage de Lightsquid

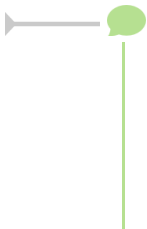
La génération des statistiques proxy peut se faire manuellement, en exécutant la commande `squid_parselogs.sh`.

La méthode d'anonymisation des statistiques générées est également paramétrable :

- aucune : aucune anonymisation ;
- par IP : n'affiche que les adresses IP ;
- anonyme : entièrement anonyme (remplace par un tiret).



Suite à un incident, les statistiques sont celles de la veille, il faut penser à forcer la génération manuellement.



Techniquement, LightSquid fonctionne en mode *cgi* sur un port local (8062 par défaut).

Cela entraîne certaines limitations :

- la ré-authentification nécessaire en mode "pam" ;
- l'accès aux statistiques est impossible depuis un frontend EAD distant.

Consultation

La consultation des statistiques LightSquid se fait au travers de l'EAD, dans le menu **Outils / Statistiques proxy**.

STATISTIQUES SQUID

Les statistiques sont générées une fois par jour.
Pensez à lancer le script squid_parselogs.sh en root sur le serveur.

Accéder aux statistiques

Pour afficher les statistiques il faut cliquer sur le lien [Accéder aux statistiques](#). La navigation se fait dans une nouvelle fenêtre qui demande une authentification. Par défaut, ces statistiques ne sont accessibles que pour le rôle `admin`, un clic sur le bouton `Connexion` sans mot de passe permet de passer à la demande d'authentification pour le compte `root`.

Une fois connecté la vue initiale propose de naviguer dans les statistiques par date (année, jour, mois), par groupe, par quota dépassé.

Squid rapport d'accès utilisateur
Periode de travail: Oct 2012

Calendar												Top Sites	Total	Groupe
2012												ANNEE	ANNEE	ANNEE
01	02	03	04	05	06	07	08	09	10	11	12	MOIS	MOIS	MOIS

Date	Groupe	Utilisateurs	Quota Dépassé	Octets	Moyenne	Hit %
11 Oct 2012	grp	4	0	6.0 M	1.5 M	1.27%
10 Oct 2012	grp	30	8	313.0 M	10.4 M	8.47%
09 Oct 2012	grp	81	15	587.4 M	7.3 M	3.10%
08 Oct 2012	grp	66	18	702.7 M	10.6 M	3.48%
07 Oct 2012	grp	5	1	30.0 M	6.0 M	0.95%
06 Oct 2012	grp	4	1	27.4 M	6.8 M	1.21%
05 Oct 2012	grp	79	33	5.7 G	73.4 M	1.92%
04 Oct 2012	grp	95	50	5.9 G	63.9 M	3.00%
03 Oct 2012	grp	51	11	561.1 M	11.0 M	1.83%
02 Oct 2012	grp	51	21	1.9 G	38.4 M	7.52%
01 Oct 2012	grp	50	22	1.7 G	34.1 M	4.60%
Total/Moyenne:		46	16	17.4 G	24.0 M	3.40%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Consultation au travers de l'EAD

Dans la vue journalière, si la méthode d'anonymisation choisie est par IP, LightSquid n'affiche que les adresses IP utilisées lors de la navigation. Il affiche également le nombre de connexions et le nombre d'octets utilisés. Il est possible d'afficher un rapport sur le top des sites visités et le top des gros fichiers téléchargés dans la journée. Il est possible de repasser à des statistiques journalières par IP.

Squid rapport d'accès utilisateurDate: **02 Jun 2014 (Rafraîchir :: 04:00 :: 2 Jun 2014)**[Top Sites](#) Rapport[Gros Fichiers](#) Rapport

#	Temps	Utilisateur	Real Name	Connexion(s)	Octets	%	Groupe
1		172.16.0.6	?	1 211	20.8 M	96.3%	?
2		172.16.0.129	?	23	222 384	0.9%	?
3		172.16.0.126	?	12	164 134	0.7%	?
4		172.16.0.134	?	10	130 837	0.5%	?
5		172.16.0.128	?	7	116 574	0.5%	?
6		10.21.58.10	?	80	36 720	0.1%	?
7		172.16.0.135	?	4	19 206	0.0%	?

Vue journalière des statistiques

Dans la vue des statistiques journalières par IP, toutes les adresses visitées par l'utilisateur s'affichent avec le nombre de connexions et les octets consommés.

Squid rapport d'accès utilisateurUtilisateur: **172.16.0.6 (?)**

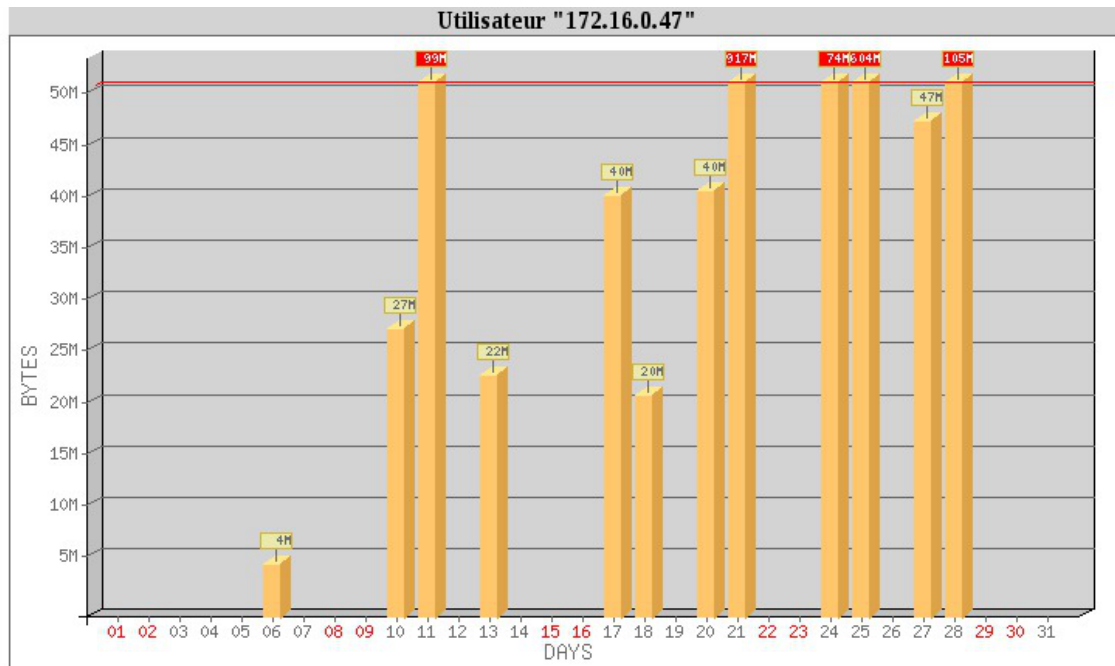
Groupe: ?

Date: **02 Jun 2014**[User download "Big Files"](#)

Total		20.8 M			
#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	osce106-ilspn25-p.activeupdate.trendmicro.com	28	19.6 M	19.6 M	94.3%
2	osce106-ilspn25wr-p.activeupdate.trendmicro.com	16	869 227	20.5 M	3.9%
3	92.51.156.70	1	152 340 194	20.8 M	1.5%
4	cyberlib.crdp-poitiers.org:443	14	25 142	20.8 M	0.1%
5	ctldl.windowsupdate.com	1	337	20.8 M	0.0%
Total			20.8 M		

Vue journalière par IP des statistiques

Dans la vue par mois, un clic sur la consommation total des Octets donne un classement de la consommation d'octets par adresse IP. Dans le tableau affiché, un graphe mensuel de la consommation d'octets par adresse IP est disponible.



Graphe mensuel de la consommation d'octets pour une adresse IP

3. ERA, éditeur de règles pour le module Amon

3.1. Introduction

3.1.1. Présentation

Présentation et fonctionnalités

L'outil EOLE de génération de règles de pare-feu^[p.557] pour les modules Amon et AmonEcole se nomme ERA^[p.546].

Il permet de gérer la description de la politique de sécurité d'un pare-feu^[p.557]. Cette politique est sauvegardée intégralement dans un fichier de type XML avec un format spécifique à l'application.

Par un processus de compilation, ERA transforme le fichier XML en un bloc de règles iptables^[p.550], de manière à instancier ces règles sur un pare-feu^[p.557] cible.

ERA et sa documentation sont sous licence libre.

Un logiciel en deux parties

- L'interface de conception permet d'organiser la politique de filtrage et l'enregistre dans un fichier XML ;
- le compilateur génère le script iptables , par compilation, à partir du fichier XML de description du pare-feu.

Seul le format XML est utilisé par le module Amon. L'exportation au format iptables^[p.550] permet d'être utilisable sur un autre pare-feu disposant de Netfilter.

Il n'est bien sûr pas nécessaire de connaître la syntaxe iptables pour manipuler ERA. Le but d'un tel logiciel est justement de s'abstraire de la syntaxe iptables, afin de pouvoir concevoir un pare-feu sans pour autant être un expert. Pour cela, l'interface graphique de ERA est un outil intéressant :

	exterieur	dmz	pedago	admin	bastion
exterieur		0 directive	0 directive	0 directive	13 directives
dmz	7 directives		1 directive	0 directive	13 directives
pedago	12 directives	0 directive		0 directive	15 directives
admin	7 directives	0 directive	0 directive		14 directives
bastion	0 directive	0 directive	0 directive	0 directive	

L'interface graphique d'ERA

Le fichier lance.firewall

Sur le pare-feu Amon, le fichier `lance.firewall` présent dans `/sbin/` est un fichier de règles iptables qui a été généré par ERA.

Remarquons que si le serveur sur lequel est lancé le compilateur de règles est en mode conteneurs, ERA va générer autant de fichiers de règles iptables que de conteneurs.

3.1.2. Les fichiers XML de modèles

Un modèle^[p.554] est un fichier de description du pare-feu. Le format d'enregistrement est un format XML. Divers modèles caractéristiques de description de pare-feu sont disponibles dans le répertoire `/usr/share/era/modeles` et sont des exemples de types de pare-feux (deux, trois, quatre ou cinq cartes réseau).

En général il est préférable, pour commencer un pare-feu, de partir d'un des modèles exemples, et d'y rajouter des directives (ou bien d'en enlever). Partez plutôt du modèle qui correspond au nombre de cartes réseau dont vous disposez sur le serveur.



Lorsque vous modifiez un modèle exemple, il faut impérativement l'enregistrer dans un fichier différent. Sinon, il sera écrasé à la mise à jour suivante.

De plus, il faut que vos nouveaux fichiers XML soient enregistrés dans le répertoire `/usr/share/era/modeles/`.



Charger un modèle à la ligne de commande.

Il est possible d'ouvrir directement un modèle à la ligne de commande. Pour cela, il suffit de spécifier l'option `-f` avec le nom du fichier.

Par exemple :

```
era -f /usr/share/era/modeles/3zones-amonecole.xml
```

Le format XML interne est facilement lisible avec un éditeur de texte (ou un éditeur XML) si l'on est familiarisé avec :

- la notation XML ;
- les différents concepts propres à ERA (tableau des flux, services, directives, ...).

Version des modèles ERA

Les modèles XML ERA sont versionnés.

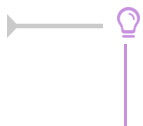
Dans les modèles fournis, la version est indiquée dans l'attribut version de la balise `<firewall>`.

```
1 <firewall name="Concatenated_Do_Not_Edit" netbios="1" qos="0" version="2.4">
```

Le numéro de version des modèles XML ERA est incrémenté lorsque des changements importants sont apportés à la DTD^[p.545].

Les numéros de version sont généralement corrélés avec les versions des modules EOLE : 2.0, 2.3, 2.4, 2.42.

Sur EOLE 2.5.1 et supérieur, les commandes `instance`, `reconfigure` et le redémarrage du service bastion affichent un avertissement si le modèle de pare-feu utilisé possède une version inférieure à celle gérée par l'outil ERA du module.



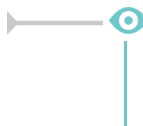
Il est possible de mettre à niveau un modèle XML existant en l'éditant et en le sauvegardant à l'aide du logiciel ERA.

3.1.3. Les variables Creole

ERA^[p.546] a été conçu dans le cadre du projet EOLE et pour le pare-feu Amon. Il peut très bien être utilisé en dehors de ce cadre, mais c'est sur un module Amon qu'il devient vraiment possible de déployer toutes les possibilités du logiciel.

Il est possible, à plusieurs endroits de l'interface, d'insérer des variables Creole^[p.544] (elles commencent par `%%`) plutôt que des valeurs fixes.

Le fichier XML de description de pare-feu devient alors un template^[p.562] Creole.



Dans la fenêtre d'édition d'une zone, entrer une valeur du type `%%ip_variable` plutôt qu'une valeur IP fixe.

Ces variables seront instanciées sur un serveur EOLE. Mais elles peuvent aussi être utilisées pour le déploiement d'autres pare-feux tant que Netfilter est présent.

Limitations de l'intégration entre ERA et Creole

Cette intégration des variables Creole dans ERA a des limites dans le cas des variables multivaluées. Une variable multivaluée au sens de Creole est une variable dont les valeurs sont multiples (c'est une liste d'ips, de networks, etc...).

Il est autorisé d'utiliser des variables multivaluées dans ERA, mais il y a une limitation : si dans une

directive donnée plusieurs variables multivaluées sont utilisées (par exemple au niveau d'une extrémité source, d'une extrémité de destination ou d'un service, ou d'un port de redirection...), alors il faut que les autres variables multivaluées utilisées soient déclarées dans le dictionnaire Creole comme esclaves de la première variable multi-valuée, sinon le cas d'utilisation ne sera pas géré.

Le support des groupes de variables multivaluées est très partiel dans ERA, si dans une directive une variable multivaluée est utilisée alors elle doit être déclarée comme maître dans le dictionnaire Creole, et il ne faut pas qu'il y ait dans cette directive une deuxième variable multivaluée **indépendante**, donc les autres variables impliquées sont soit des variables multivaluées esclaves, soit simplement des variables Creole non-multivaluées.

3.2. Utilisation

3.2.1. Les zones de sécurité

Présentation

L'éditeur ERA est un outil de conception par zones^[p.565]. Une zone^[p.565] correspond physiquement à une carte réseau. Cela permet de découper le parc de machines en réseau ou sous-réseau.

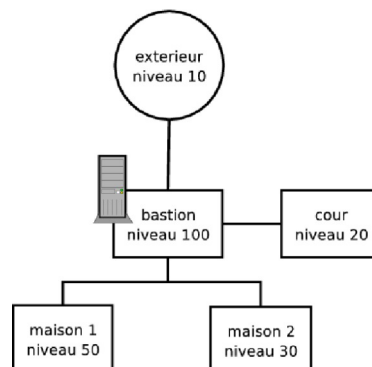
Le pare-feu lui-même étant une zone à part, appelée par convention bastion.

Les zones sont ensuite ordonnées par niveau de sécurité^[p.555] sous forme d'entiers de 0 à 100.

100 est le niveau de sécurité maximal et correspond à la zone bastion. Cela permet de "cartographier" tout le réseau.

Par convention, le niveau de sécurité le plus faible de toutes les zones est affecté à la zone "extérieur".

Les machines de la zone ont un accès complet aux zones de niveau inférieur et aucun accès à celles de niveau supérieur.



Les niveaux de sécurités des différentes zones (vue centrée sur le bastion)

Une zone correspond à un réseau et dans cette zone, on retrouve des sous-réseaux et des machines, correspondant à la notion d'extrémité^[p.547] utilisée dans ERA.

Une extrémité est un sous-ensemble d'une zone :

- Elle est définie par un ensemble d'adresses IP ou une adresse réseau.
- Elle hérite du niveau de sécurité de la zone à laquelle elle appartient.

Ajouter une zone

Il est possible à tout moment, même après la conception initiale du modèle, d'ajouter une zone de sécurité. L'ajout d'une zone de sécurité se fait en cliquant sur le bouton **Ajouter Zone** de la barre d'icônes.



Ajouter une zone au tableau des flux

Les cases des noms des zones sont cliquables.

Un clic droit dans une case des noms de zones permet d'afficher les zones ainsi que les extrémités^[p.547] qui y sont associées.

Fenêtre d'édition de zone

🔗 les trigrammes (préfixes) de zones

Dans le choix des noms de zone :

- les trois premières lettres (trigramme) du nom de la zone sont discriminantes, par exemple : statistique et station sont des noms de zone incompatibles (c'est la même zone sta) ;
- le mot clef bastion est réservé (pour la zone du bastion lui-même) ;
- le mot clef extérieur est également réservé (pour la zone extérieure, internet).

★ la gestion des VLAN

Une zone peut aussi représenter un VLAN.

C'est une bonne pratique de créer une nouvelle zone pour gérer un VLAN.

Il n'est pas possible de créer une zone pour tous les VLAN.

S'il y en a plusieurs il faut les créer un à un manuellement.

Syntaxe Creole pour la création des VLAN

Il est fréquent que les valeurs des IP des VLAN soient stockées dans une variable Creole, et que cette variable soit multiple (une variable multiple au sens Creole est une variable qui contient une liste de valeurs). Il faut alors manier correctement la syntaxe Creole pour créer une zone de VLAN.

Exemple de création d'un VLAN de eth1

Dans la widget de création d'une zone, il faut mettre une IP et un netmask variable :

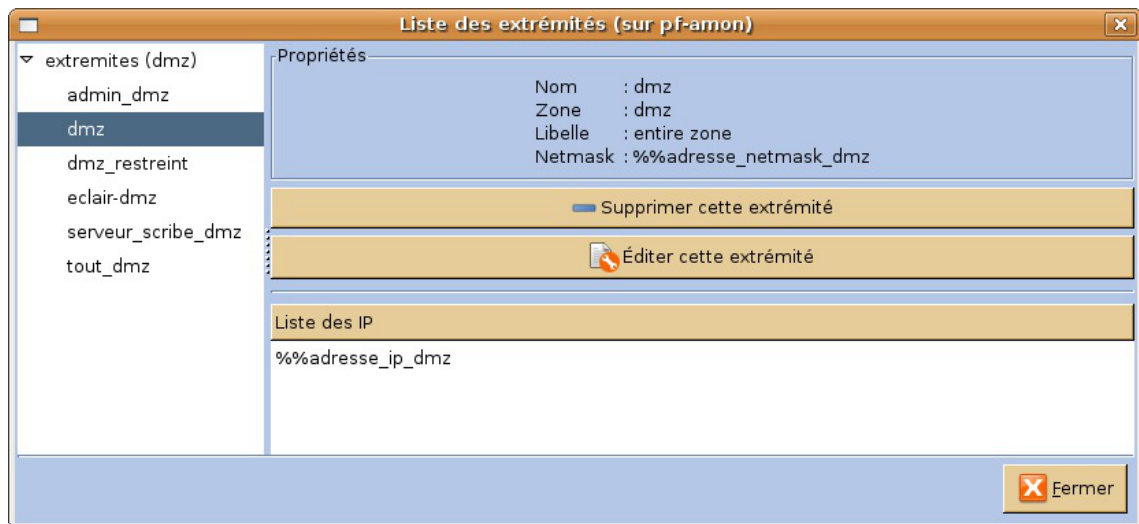
```
ip variable : %%id_vlan_eth1[0].adresse ip_vlan_eth1
```

```
netmask variable : %%id_vlan_eth1[0].adresse_netmask_vlan_eth1
```

Ajouter une extrémité

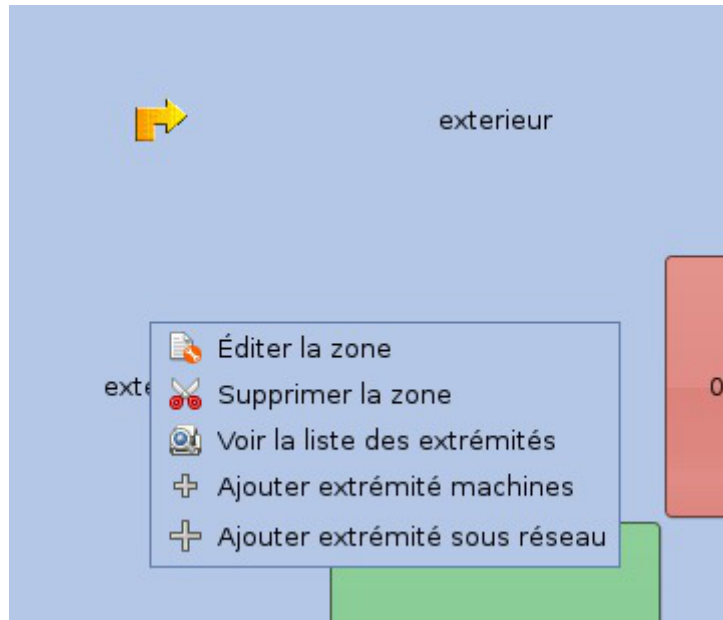
La liste des extrémités est disponible dans le menu `bibliothèque / extrémités`.

Il est également possible de lister les extrémités d'une zone, en cliquant droit sur le bouton de la zone et en sélectionnant `voir la liste des extrémités`.

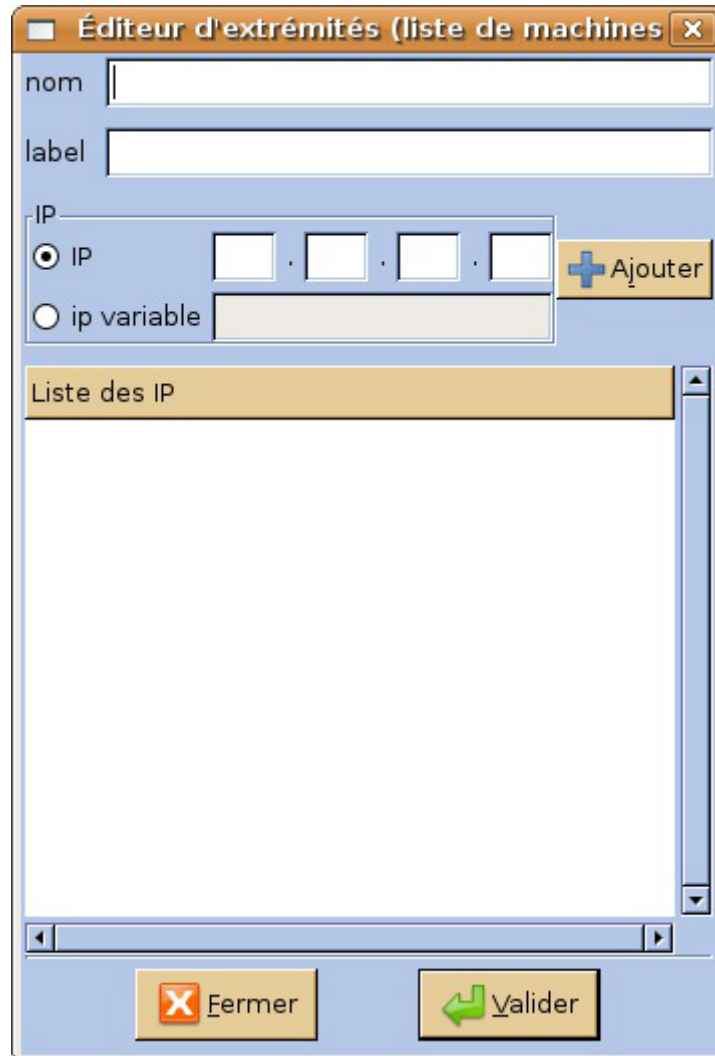


Liste des extrémités

Pour créer une nouvelle extrémité, faire un clic droit dans la zone dans laquelle vous voulez l'inclure. Ensuite, choisir `définir un ensemble de machines` ou `définir un sous-réseau` suivant que vous voulez inclure un groupe d'IP ou un sous-réseau.



Un clic droit sur le nom d'une zone affiche le menu contextuel relatif à cette zone



Ajout d'une extrémité dans le cas d'une liste de machines

Nom

Description

Propriétés du réseau

Adresse du réseau

network variable

Masque du réseau

netmask variable

Ajout d'une extrémité de type sous réseau



Les alias IP doivent être gérés **comme des extrémités** et non comme une zone : **un alias n'est pas une zone.**

Pour ajouter une extrémité de type alias, il faut spécifier le type "alias" dans l'éditeur d'extrémité :

Éditeur d'extrémités (liste de machines) (su

nom

label

IP

IP

ip variable

Liste des IP

Type

Il est fréquent que les valeurs des IP des alias soient stockées dans une variable Creole, et il est fréquent aussi que cette variable soit multiple (une variable multiple au sens Creole est une variable qui contient une liste de valeurs). Il faut alors manier correctement la syntaxe Creole pour créer une extrémité qui est un alias.

Dans la widget de création d'une extrémité, il faut alors mettre une IP et un netmask variable.

Dans la zone correspondant à la carte, créer une extrémité (clic droit sur la case de la zone).



Un alias de eth2 doit être créé de la façon suivante :

```
ip variable : %%alias_ip_eth2[0]
```

```
network variable : %%alias_network_eth2[0]
```

Il sera possible ensuite de créer une directive avec cette extrémité plutôt qu'avec l'extrémité correspondant à l'IP de la zone elle-même.



Les mauvaises fausses bonnes idées pour créer un alias

- créer une zone supplémentaire avec une carte eth0:X ;
- aller de suite dans les inclusions statiques ;
- utiliser la variable eth0 de Creole comme IP multivaluée.

Les extrémités de type conteneur

Il est possible également de créer une extrémité dans la zone **bastion**. Dans la zone bastion il y a depuis la version 2.4 un nouveau type d'extrémité, le type **conteneur**. Ce type d'extrémité permet de créer des directives à destination des conteneurs (directives de type INPUT).

Une extrémité de type conteneur est à destination du conteneur. Elle nécessite deux informations : le nom de l'interface (typiquement : "br0", "eth1", ...), et le nom du conteneur (typiquement : "bdd", "internet"...)

3.2.2. Les flux

Présentation


Dans ERA, les règles sont systématiquement classées d'après la zone d'origine et la zone de destination. ERA est donc conçu autour du concept de flux^[p.547] plutôt que centré sur la notion de règle. Par voie de conséquence, chaque zone est reliée à une autre zone par des flux.

A l'intérieur d'un flux, on trouve deux flux orientés, le "flux montant^[p.548]" et le "flux descendant^[p.548]".

Les "flux montants^[p.548]" concernent les zones^[p.565] d'un niveau de sécurité plus faible vers un niveau de sécurité plus élevé, et réciproquement pour les "flux descendants^[p.548]".


Pour pouvoir ordonner les flux en vue d'une cohérence globale, il convient ensuite de modéliser le "tableau des flux^[p.562]".

Ce tableau correspond à l'ensemble des flux du modèle de sécurité à l'intérieur duquel seront rangées les règles (ou directives).

	10	20	100
10		Montant	Montant
20	Descendant		Montant
100	Descendant	Descendant	

Directives montantes et descendantes dans la matrice de flux

Lorsque les flux montants et les flux descendants sont définis, une politique par défaut est automatiquement spécifiée. Ici, la politique de sécurité par défaut qui résulte de la matrice de flux est :

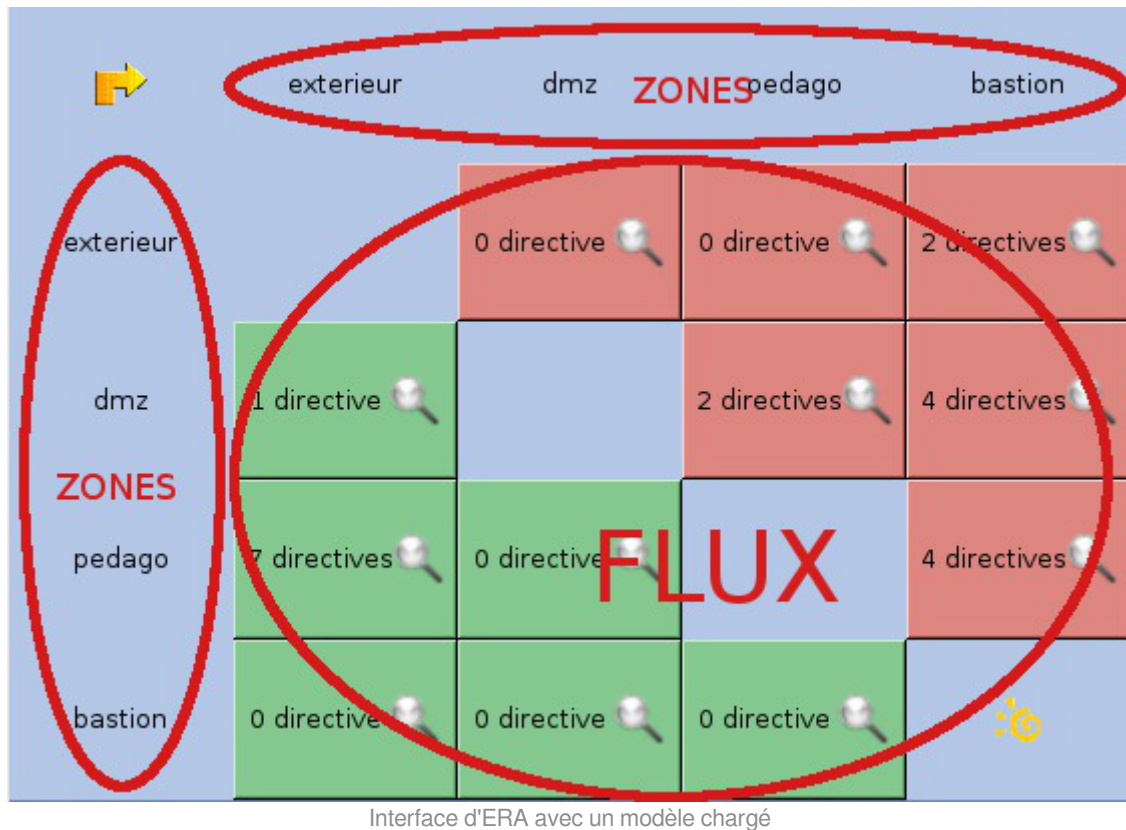
	10	20	100
10		Interdit	Interdit
20	Autorisé		Interdit
100	Autorisé	Autorisé	

Repérage des types de directives (autorisation ou interdiction) dans la matrice de flux

- 💡 **Niveaux de sécurité égaux**
 Lorsque deux zones ont deux niveaux de sécurité égaux, alors la politique par défaut est une interdiction des deux côtés (flux montants et descendants).
- ⚠️ **Changement de la politique par défaut**
 Il est possible d'inverser le comportement de la politique par défaut. On peut choisir d'interdire les flux d'une zone vers une autre par défaut.

L'interface de conception

La fenêtre principale représente un tableau composé de cases de zones et de cases de flux.



Les cases des flux sont colorés. Les cases de couleur verte sont en "autorisation" par défaut et les cases de couleur rouge sont en "interdiction" par défaut.

La couleur rouge indique que le flux orienté est interdit, tandis que la couleur verte montre que le flux orienté est autorisé.

3.2.3. Les directives

3.2.3.a. Présentation

Une directive^[p.554] est une règle concernant un service ou un groupe de services entre deux extrémités. Cette règle peut être de type "interdiction", "redirection", "source NET" ou "destination NAT".

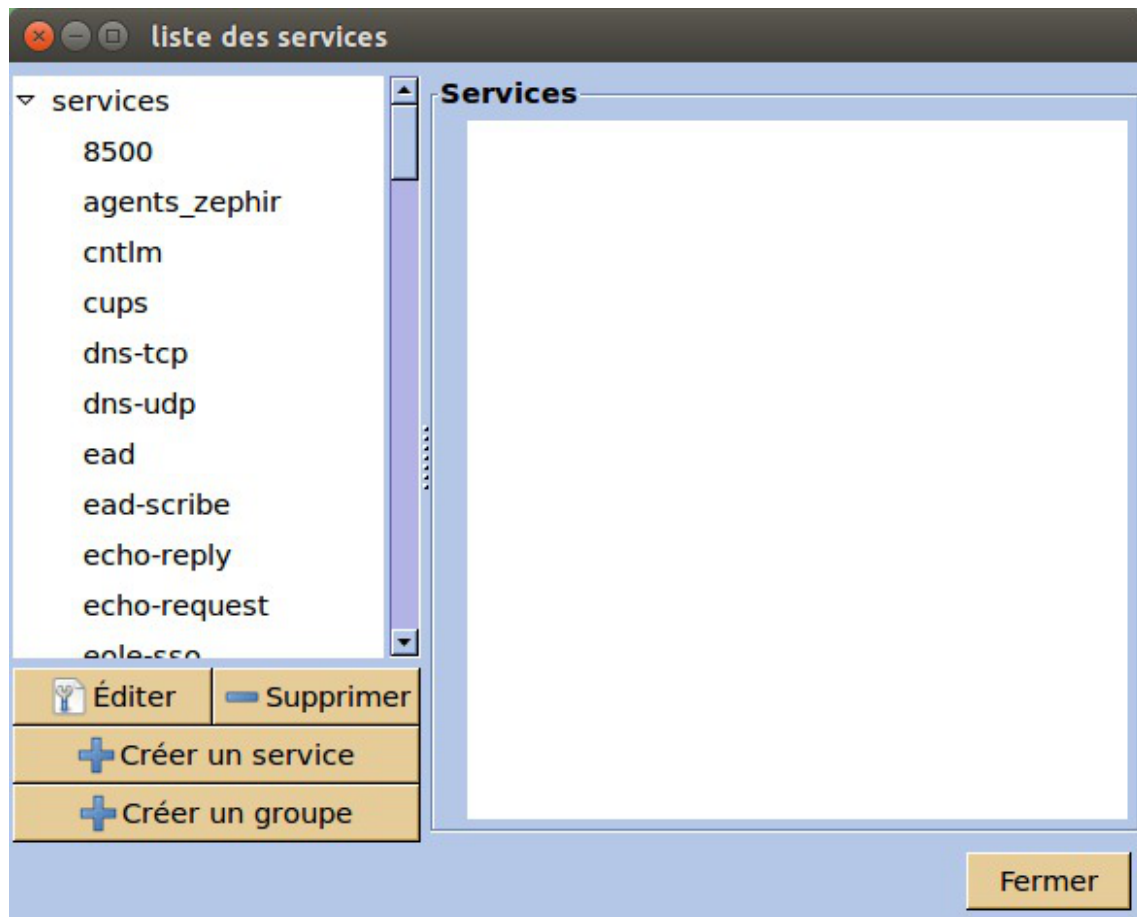
3.2.3.b. Les services et les groupes de services

Avant de pouvoir créer une directive, il faut d'abord créer un service^[p.560].

Par exemple, le service "serveur web" est défini par le protocole HTTP sur le port 80.

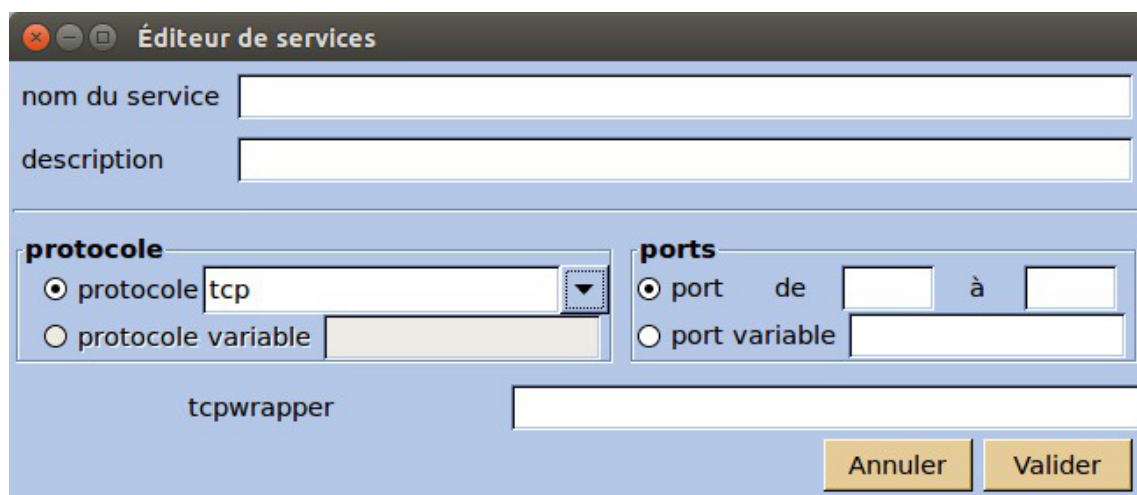
Il y a déjà une bibliothèque de services prédéfinis dans ERA.
Pour lister ces services, aller dans le menu : Bibliothèque > services .

Pour créer un service, aller dans le menu : **Bibliothèque > services** .



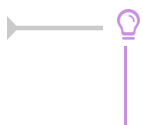
Liste et édition des services

Créer ou modifier un service signifie renseigner les noms, descriptions, protocoles et ports.



Ajout d'un service

Remarquons que si on choisit un port égal à 0, cela équivaut à saisir de 0 à 65535.



Si on veut que le service ne concerne qu'un seul port, il faut mettre deux fois le même numéro de port.

- ⚠ Depuis EOLE 2.4, l'utilisation d'une variable Creole pour définir le type de protocole à utiliser n'est plus fonctionnelle.
Cette fonctionnalité n'est plus disponible dans l'interface à partir d'EOLE 2.6.

💡 implémenter un service avec tcpwrapper

Pour prendre en compte le tcpwrapper avec ERA, ça se passe au niveau des services. Il suffit de renseigner le nom tcpwrapper du service (le nom tel qu'il doit apparaître dans le fichier **hosts.allow**) et le tcpwrapper sera pris en compte dès qu'une directive utilisant ce service sera créée.

Éditeur de services (sur amonecole)

nom du service : 8500

description : service 8500

protocole : tcp

ports : port de 8500 à 8500

tcpwrapper : []

Buttons: [] [Valider]

💡 le tcpwrapper en mode conteneur

Remarquons que ERA va générer un fichier tcpwrapper, classiquement le fichier **/etc/hosts.allow**, mais que en mode conteneur autant de fichiers seront générés que de conteneurs.

3.2.3.c. L'éditeur de directives

Un clic droit ou un double clic dans une case de flux du tableau permet de visualiser la liste des directives de façon synthétique.

Les directives sont triées par ordre croissant. C'est l'ordre dans lequel seront appliquées les règles sur le pare-feu cible.

- ⚠ Les directives de nat et redirection sont appliquées forcément avant les autres. Ceci est le comportement de Netfilter^[p.555].

Depuis cette fenêtre, il est possible d'éditer une nouvelle directive (en double-cliquant dessus) ou d'en ajouter une si nécessaire.

Pour construire une directive, il faudra au moins deux extrémités (entre deux zones) et un service (ou groupe de services), qui doit être renseigné par glisser-déplacer.



Si vous ne renseignez pas les extrémités, c'est la zone entière qui est prise (plus précisément l'extrémité désignant la zone entière).



Différence entre zone entière et zone restreinte

La zone entière est le réseau correspondant à une carte réseau du pare-feu. Cela correspond au réseau local ainsi que d'éventuels sous-réseaux derrière une passerelle. Elle est nommée *<nom de la zone>*.

La zone restreinte ne correspond qu'au sous-réseau. Elle est nommée *<nom de la zone>_restreint*.

A chaque directive est associé un service ou un groupe de services qu'il est nécessaire de renseigner par glisser-déposer.

> Les types de directives

Les types de directives

Il y a plusieurs types de directives :

- autorisation
- interdiction
- redirection
- SNAT
- DNAT
- FORWARD

Les directives d'autorisation et d'interdiction

Une directive est dans une case de flux et elle s'oppose à la politique par défaut du flux. Si le flux est en autorisation, la directive propose une interdiction et inversement.

En plus du filtrage simple, d'autres fonctionnalités sont proposées.

Les directives de redirection

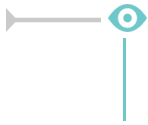
Une directive de type redirection permet de rediriger une requête d'un port déterminé vers un port de la machine elle-même (bastion).



Cette fonctionnalité est particulièrement intéressante dans le cas du proxy transparent. Toutes les requêtes destinées à des serveurs web seront redirigées automatiquement vers le service proxy installé sur le serveur.

Les directives de DNAT/SNAT

Le NAT permet de modifier l'adresse source (SNAT) ou destination (DNAT) d'une requête.



Le SNAT est utilisé pour toutes les requêtes provenant de la zone pédago vers l'extérieur. Cela permet de transformer les adresses source locales en adresses source extérieures.



Le DNAT et le SNAT ne sont pas autorisés si la directive est authentifiée.

Les directives FORWARD

Le FORWARD permet d'autoriser la translation un réseau vers un autre

> Les plages horaires

Création d'une plage horaire

Les plages horaires sont définies depuis le menu **Bibliothèque > plage horaire** .

Il y a trois manières de définir une plage horaire :

- les heures de début et de fin ;
- les dates de l'année de début et de fin ;
- les jours de la semaine.

Les informations indispensables sont : le nom et une ou plusieurs de ces trois manières.

Affectation d'une plage horaire à une directive

Il est possible de définir une plage horaire à l'intérieur de laquelle la directive sera activée.

Depuis l'éditeur de directives, glisser-déposer une plage horaire. Affecter une plage horaire à une directive.

> La journalisation

La case "journaliser" permet de tenir un journal des événements (logs) de la directive (grâce à ULOG).

> Gérer des exceptions

Dans l'éditeur de directives il est possible d'ajouter des exceptions.

L'éditeur d'exceptions permet :

- d'ajouter une exception ;
- d'éditer une exception ;
- de supprimer une exception.

nom	source	destination

L'exception peut se faire :

- sur une adresse IP ;
- sur un nom de domain ;
- sur une variable Creole.

> Le marquage

Le marquage est une fonctionnalité avancée de iptables^[p.550] permettant d'identifier un paquet grâce à une marque spécifiée dans l'interface.

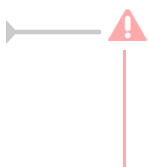
> Les directives optionnelles

Présentation

Une directive optionnelle^[p.544] est une directive qui va être activable ou désactivable depuis l'interface EAD^[p.545].

Pour cela, il est indispensable d'affecter un libellé optionnel à cette directive. Il est aussi possible de choisir un libellé optionnel préexistant dans la liste des libellés affectés aux directives, ce qui crée une notion de groupe de directives optionnelles.

La directive est étiquetée comme optionnelle



Un libellé optionnel sert de tag (d'identifiant). Il peut être composé de caractères alphanumériques [1-9] [a-z] [A-Z] et éventuellement de "_" ou d'espaces. Il est impératif de ne pas utiliser d'autres caractères accentués.

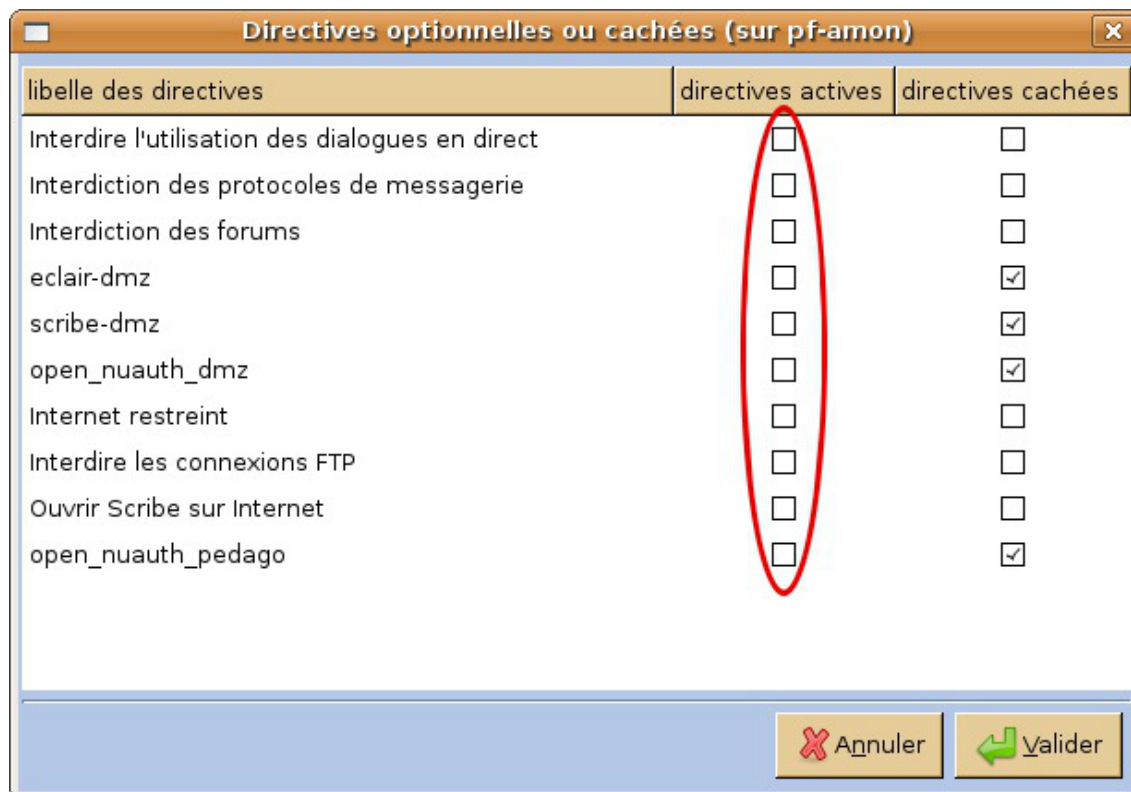
Directive optionnelle active

Une directive optionnelle n'est pas active par défaut dans ERA, c'est-à-dire que la directive ne sera pas appliquée sur le serveur cible. Pour l'appliquer, il faut aller la cocher comme active dans l'interface EAD.

Mais il est possible de rendre une directive active par défaut dans ERA. Dans ce cas, il faudra aller dans l'interface EAD pour la désactiver.

L'état actif et la possibilité de marquer une directive comme optionnelle sont deux notions différentes.

Pour activer une directive, aller dans **Bibliothèque / Directives optionnelles**.



Fenêtre de la bibliothèque permettant d'étiqueter une directive comme optionnelle

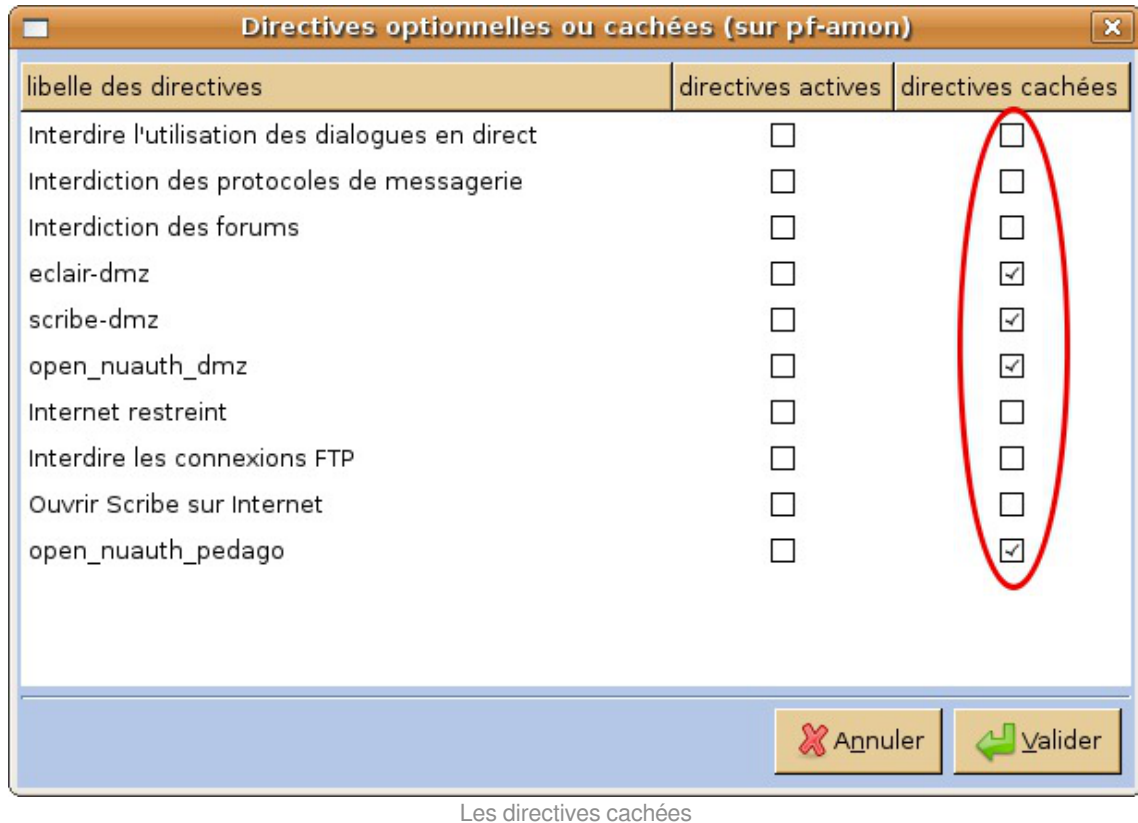
⚠ Directive optionnelle active et inactive

Dans le cas de l'activation/désactivation d'une directive optionnelle, il faut bien comprendre que c'est l'EAD qui prime par rapport à ERA. À la première instanciation du serveur, ERA détermine si la directive optionnelle est active ou inactive, mais une fois le serveur est instancié c'est depuis l'interface EAD qu'il faut renseigner le statut actif/inactif de la directive optionnelle en question.

Les directives optionnelles cachées

Une directive optionnelle cachée est une directive optionnelle qui n'apparaîtra pas dans l'EAD. Elle est activable uniquement par une procédure particulière.

Pour créer une directive optionnelle cachée, aller dans **Bibliothèque / Directives Optionnelles** et cocher **directives cachées**.



Une directive cachée est désactivée par défaut. Pour l'activer, il faut patcher le template `active_tags` afin d'y ajouter le libellé optionnel de la directive (un libellé par ligne).

⚠ Il est préférable d'utiliser un libellé optionnel court (par exemple "`ActiverProxy`" plutôt que "activer le proxy.").
 Dans le template `active_tags`, ne pas mettre de commentaire.

Voir aussi...

Directives optionnelles ERA depuis l'EAD [p.355]

3.2.4. La qualité de service

La qualité de service ne concerne que les flux des zones internes vers l'extérieur. C'est une QOS^[p.559] *externe*.

Le qualité de service est un système de **minimum garanti**.

Elle n'entraîne pas de sous-utilisation de la bande passante, car si une zone n'atteint pas son minimum d'utilisation, ce qui reste est réparti dynamiquement entre les autres zones.

Il est possible d'accéder à la fenêtre de gestion de la QOS^[p.559] de deux manières :

- depuis le menu `Bibliothèque` / `Qualité de service (QOS)` ;
- en cliquant sur la zone *Extérieur* depuis le tableau des flux.

Dans cette boîte de dialogue, il faut :

- fixer des valeurs de bande passante en *upload* et en *download* (c'est-à-dire les flux globaux disponibles entre l'intérieur et l'extérieur), en kilo bits par seconde (soit un débit de 1000 bits par seconde) ;
- à l'aide des poignées de manipulation des différentes boîtes représentant chaque zone, affecter un pourcentage de flux relatif à chaque zone.

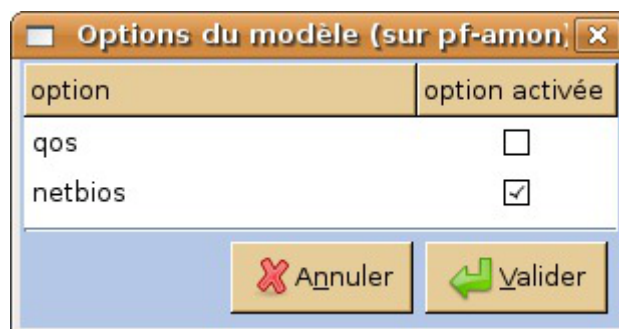
Remarquons que il est tout-à-fait possible de mettre des variables Creole comme valeurs possibles de QOS en upload et en download

La QOS peut être définie dans un modèle sans être activée !
Pensez à l'activer dans les options du modèle (**Bibliothèque->Options du modèle**).

La désactivation de la QOS n'est effective que si le fichier `/etc/qoseole.conf` est supprimé.

3.2.5. Les options du modèle

Il est possible d'ajouter des règles spécifiques à netbios et à la QOS depuis le menu **Bibliothèque / Options du modèle** .



Fenêtre des options du modèle

Activer netbios permet d'ajouter des règles permettant de bloquer les requêtes du réseau Microsoft vers l'extérieur. Cette règle est activée par défaut.

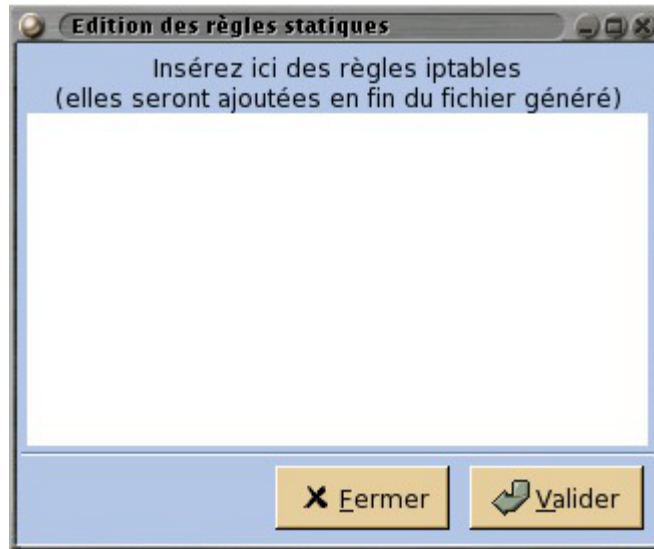
Si vous voulez utiliser les règles de Qualité de Service (QOS), il est indispensable de l'activer dans cette fenêtre. Par défaut, les règles de QOS ne sont pas actives.

3.2.6. L'inclusion statique

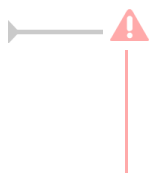
Il est possible d'insérer des règles iptables personnalisées. Ces règles vont venir s'insérer à la fin du fichier généré.

On accède à la fenêtre des inclusions statiques par le menu **Bibliothèque / Inclusion Statique** .

Il s'agit d'une zone de saisie de texte.



Fenêtre d'insertion des inclusions statiques



Aucune validation n'est faite par ERA sur ces règles insérées directement par l'utilisateur. Précisons que cette possibilité est réservée à un utilisateur avancé, qui maîtrise parfaitement la syntaxe iptables.

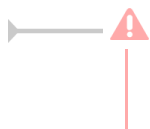
3.2.7. Imbriquer des modèles :l'héritage

Il est possible d'imbriquer des modèles, c'est-à-dire de faire dépendre des modèles les uns des autres. Un modèle devient un modèle père, les autres modèles héritent de toutes ses caractéristiques (directives, bibliothèques, flux, zones, ...).

Pour imbriquer des modèles, créez d'abord un modèle de manière habituelle. Ce modèle deviendra le modèle père. Ensuite, créez un nouveau fichier dans l'éditeur, et choisissez dans le menu **Fichier / importer un modèle**.

Le modèle est chargé comme d'habitude mais les directives importées ne sont plus éditables (elles sont grisées).

Ne seront éditables que les directives que vous allez rajouter. En plus de l'existant, vous pouvez faire toute modification utile (ajout de zone, création de directives, etc...).



Vous ne pouvez plus changer le fichier père de place ni le renommer, le chemin du fichier père est enregistré comme attribut.



L'héritage multiple entre modèles

L'héritage d'un modèle XML est donc la possibilité de d'utiliser plusieurs fichiers XML liés entre eux par référence. Le fichier référencé dans un autre fichier est appelé le fichier père. On peut voir si on édite le fichier XML avec un éditeur de texte, que le chemin du fichier XML père est renseigné dans l'attribut ****model**** à la racine de la balise ****firewall****.

Il est possible, mais ce n'est pas une action qui est accessible depuis l'interface gtk, d'hériter de plusieurs fichiers. Il suffit dans ce cas de mentionner dans l'attribut ****model**** une liste de noms longs de fichiers, séparés par des virgules. Pour des exemples de ces fonctionnalités,

regarder dans le dossier **template** dans les sources du projet ERA, car les modèles XML eux-mêmes sont générés à partir de templates qui sont imbriqués entre eux avec cette fonctionnalités de l'héritage multiple.

3.2.8. Communication avec Zéphir

La connexion au Zéphir est possible depuis le menu **Zéphir**.

Connexion à Zéphir

Importer un modèle

ERA intègre la possibilité d'échanger des modèles avec un serveur Zéphir.

Lors de la première utilisation des fonctions d'importation Zéphir, des informations de connexion vous seront demandées.

Vous devez spécifier ici l'adresse du serveur Zéphir, et le nom et le mot de passe d'un utilisateur ayant les droits nécessaires (lecture pour l'import et écriture pour l'export). Une fois connecté, vous pourrez saisir l'identifiant du serveur.

Le modèle est alors téléchargé et ouvert dans ERA. Cette procédure n'est valable que si vous avez déjà remonté le modèle de pare-feu dans Zéphir.

Importation d'un modèle XML depuis le Zéphir

A l'enregistrement, il vous sera demandé si vous voulez remonter le modèle sur Zéphir.

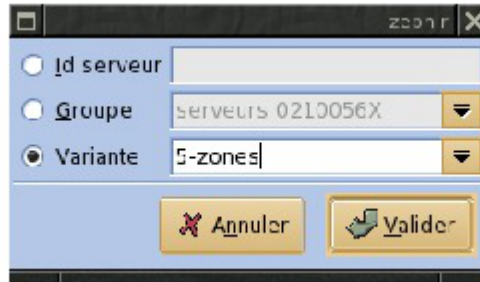
Exporter un modèle Zéphir

Lorsque vous avez construit un modèle de pare-feu, vous pouvez l'envoyer directement sur un serveur Zéphir avec le menu **Envoi à zephir**. Si vous ne les avez pas encore renseignées, ERA vous demandera les informations nécessaires à la connexion.

Les options suivantes vous sont proposées pour la sauvegarde sur Zéphir :

- pour un serveur : sauvegarde le modèle sur le serveur et change le modèle actif dans la configuration du serveur ;
- pour une variante : le fichier est ajouté à la liste des fichiers de la variante ;

- pour un groupe : idem que pour un seul serveur, mais sur tous les Amon présents dans le groupe choisi.



Exportation vers Zéphir

3.3. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles^[p.544].

Une règle peut être :

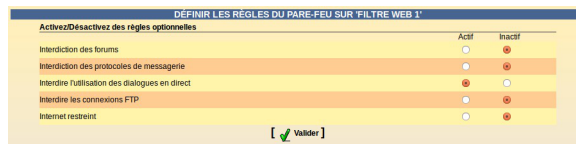
- générale, si elle concerne l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone.

La configuration générale est accessible par le menu EAD : Configuration générale / Règles du pare-feu .

La configuration spécifique est accessible par le menu EAD : Filtre web X / Règles du pare-feu :

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



Activation des directives optionnelles dans l'EAD

⚠ Lien entre ERA et les directives optionnelles de l'EAD

Pour les règles optionnelles, l'EAD prime sur l'ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comme étant active par défaut dans ERA et ne pas être active car désactivée dans l'interface EAD.

Voir aussi...

Les directives optionnelles ^[p.397]

3.4. Compléments techniques

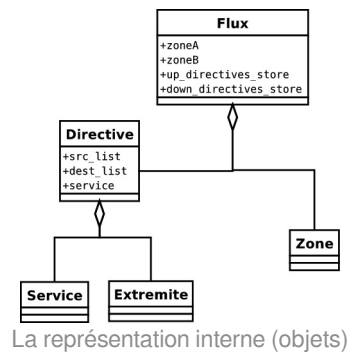
3.4.1. Le format XML interne

Les composants du tableau des flux sont :

- les flux ;
- les zones ;
- les directives montantes et descendantes.

Le format XML interne suit une DTD qui correspond à la modélisation par flux. Les noms des balises correspondent aux noms des objets ERA. Il y a la liste des zones, puis les extrémités et les services, les groupes de services, et enfin les flux contenant les directives.

La représentation interne en objets est la suivante :



- Directive(FwObject) : directive ;
- Service(FwObject), ServiceGroupe(FwObject) : service et liste de services ;
- Zone(FwObject), Extremite(FwObject) ;
- Flux(FwObject).

Les directives optionnelles

Dans le fichier `era.noyau.constants.py` il y a deux constantes intéressantes ici

- `DIRECTIVE_OPTIONAL = 1`
- `DIRECTIVE_ACTIVE = 2`

Ces filtres permettent de savoir si une directive est optionnelle ou non. Pour cela, il faut regarder l'attribut `attrs` de la directive.

Si `directive.attrs = 0`, alors la directive n'est ni optionnelle, ni active.

- `attrs=0` : pas optionnelle
- `attrs=1` : optionnelle mais pas active
- `attrs=3` : optionnelle et active
- la valeur 2 correspond à non optionnelle mais active, ce qui n'a pas de sens. Les valeurs autorisées sont donc `[0,1,3]`
- `ACTION_DENY = 1` : barrage
- `ACTION_ALLOW = 2` : pont
- `ACTION_FORWARD = 4` : redirect
- `ACTION_DNAT = 8` : dnat
- `ACTION_MASK = 16` : masque



Exemple d'une directive de type masque :

```
action="16" attrs="0" nat extr="exterieur bastion" nat port="0"
```

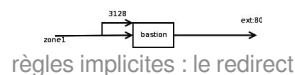
Exemple d'une directive de type dnat :

```
action="8" attrs="0" nat extr="serveur web" nat port="80"
```

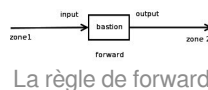
3.4.2. Comportement du Backend

Règles implicites : le REDIRECT

Un redirect doit inclure aussi une chaîne input chaîne xxx-bas. A une règle de forward vient donc se greffer une règle de type input.



Il y a une règle de forward (une redirection) :



la chaîne input qui vient se greffer sur le redirect (sur le forward) est implicite. un forward z1->z2 doublé d'une redirection, ajoute une règle de type input vers le bastion.

Une directive de redirection génère donc deux règles :

- une règle input vers le bastion
- une règle forward z1->z2

La règle dite "implicite" est la règle de type INPUT. Une règle implicite se place en fin de pile pour chaque flux (elle n'est pas placée directement à côté de sa règle de FORWARD dans le fichier de règles générées).

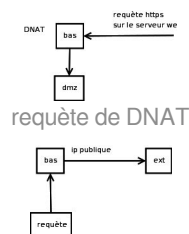
Règles implicites : Le DNAT et le SNAT

Lors d'un DNAT, une règle de type input est doublée d'un forward (elle s'ajoute à un FORWARD).

Même chose pour le masque de SNAT.

Exemple : un serveur de la DMZ répond à une requête sur le port 80 du bastion.

Un INPUT est transformé en FORWARD.



Un poste de travail peut surfer sur le web avec l'IP publique du bastion. Cela permet de surfer masqué.

3.4.3. Intégration avec Creole

Creole propose un concept de variables multivaluées qui peuvent être utilisées dans ERA. ERA utilise bien-sûr les variables de dictionnaire Creole "simples", mais la fonctionnalité d'utilisation des variables de

dictionnaires dans ERA peut-être étendue aux fonctionnalités Creole.

Si une variable `%%variable` est multi-valuée (au sens de Creole, c'est-à-dire que ça peut-être une liste), et que cette variable est présente dans une règle iptables, alors la règle iptables sera répétée autant de fois que de valeurs dans `%%variable` cette fonctionnalité génère du code avec une boucle for :

```
%for %%v in %%variable /sbin/iptables bla bla %%v bla bla %end for
```

3.4.4. Le compilateur

La génération des règles iptables

A la compilation du fichier XML, un certain nombre d'actions sont effectuées. Ce sont des règles iptables :

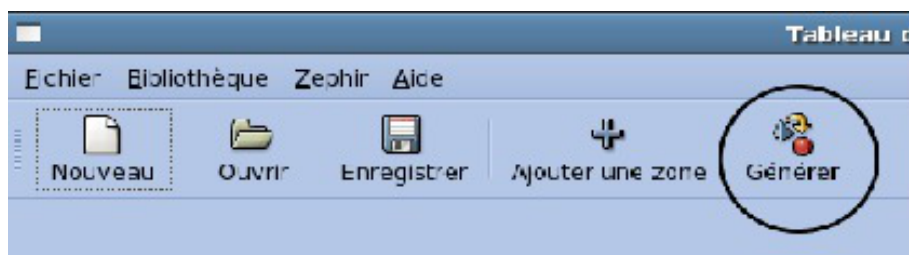
- définition d'une sous-chaîne pour chaque flux (liaison entre zone/extrémité) ;
- création de la politique par défaut (en fonction du niveau des zones) ;
- ajout des règles correspondant aux directives ;
- ajout de règles implicites liées aux directives ;
- insertion des inclusions statiques (règle iptables de bas niveau).

Sur Amon, le compilateur gère aussi l'affichage des règles optionnelles dans l'EAD et récupère leur configuration en cas de mise à jour, et contrôle l'activation des directives cachées.

Le script iptables peut-être généré depuis l'interface ERA ou bien depuis un utilitaire ligne de commande plus complet.

Le bouton **générer**, bouton de génération des règles iptables n'est utile que si l'on n'est pas sur un Amon.

Il est donc possible depuis l'interface de transcrire directement en règles iptables ce qui est enregistré dans le fichier XML.



Bouton de génération de la sortie au format iptables

C'est aussi au moment de la compilation que sont gérées les directives cachées. Elles sont activées ou désactivées selon ce qui a été spécifié.

Utilisation en ligne de commande

Aller dans le répertoire era `/usr/share/era` et lancer le compilateur avec le fichier de modèles adapté

```
[era] $ ./backend/compiler --help
compiler [options] era_model_file.xml
```

par exemple :

```
[era] $ ./backend/compiler modeles/3zones.xml
```

différentes options sont possibles, taper `--help` pour les détails ou regarder le fichier

`/usr/share/era/bastion.sh` qui correspond à ce qui est lancé par le service **bastion**
`service bastion restart` est lancé

3.5. Quelques références

- Site officiel du logiciel (présentation, téléchargement) : <http://eole.orion.education.fr>
- Code source du logiciel (versions, branches, tags) : <https://dev-eole.ac-dijon.fr/projects/era/repository>

4. Gestion des tunnels : RVP

Pré-requis

Le réseau virtuel privé (RVP)^[p.559] est activé au moment de la configuration et de l'instanciation du module.

Sur le module Amon, il faut au préalable avoir activé et configuré le réseau virtuel privé dans l'interface de configuration du module. Sur le module Sphynx, ce paramètre est forcé et n'apparaît pas.

Le mode de configuration de strongSwan (database ou fichier plat) doit être le même que sur le serveur ARV qui a généré la configuration IPsec.

ARV^[p.541] permet de gérer les RVP de plusieurs serveurs Sphynx. Un serveur Sphynx autre que le serveur Sphynx-ARV sera appelé Sphynx distant. Sur un serveur de ce type, la mise en place du RVP se fera comme sur un serveur Amon.

Activation du RVP au moment de l'installation du serveur Amon

La configuration du Réseau Virtuel Privé peut se faire avec un serveur Zéphir ou manuellement.

Dans le cas d'une configuration manuelle il faut préparer la configuration avant l'instanciation :

- copier le répertoire `/home/data/vpn/<UAI>/<UAI>-amon.tar.gz` présent sur le module Sphynx sur le module Amon dans `/tmp/sphynx.tar.gz` ;
- sur le module Amon créer le répertoire `ConfIpsec` : `# mkdir -p /root/tmp/ConfIpsec` ;
- se rendre dans le répertoire `/root/tmp/ConfIpsec` : `# cd /root/tmp/ConfIpsec` ;
- désarchiver sphynx.tar.gz : `# tar xzf /tmp/sphynx.tar.gz`

Au lancement de la première instanciation, la question suivante vous sera posée :

`Voulez-vous configurer le Réseau Virtuel Privé maintenant ? [oui/non]`
`[non] :`

Vous devez répondre oui à cette question.

Puis le choix `1.Manuel` ou `2.Zéphir` est proposé.

- Le choix `1.Manuel` permet de prendre en compte la configuration RVP présente sur le serveur, attention cette opération doit être effectuée avant d'exécuter l'instanciation ;
- Le choix `2.Zéphir` active la configuration RVP présente sur le serveur Zéphir. Cela suppose que le

serveur est déjà enregistré sur le serveur Zéphir. Il sera demandé un utilisateur et mot de passe Zéphir et l'identifiant Zéphir du serveur Sphynx.

Dans les deux cas, la phrase de passe (passphrase) de la clé privée est demandée. Si le mot de passe est correct le RVP est configuré pour cette machine et l'instanciation peut se poursuivre...

Activation du RVP sur des modules Amon déjà en exploitation

Pour activer un RVP sur un module Amon déjà instancié, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp init`.



Lors de cette phase de configuration du VPN sur Amon, les tunnels peuvent se couper dans les secondes qui suivent et dans certaines circonstances uniquement. Le problème est corrigé à partir de la version strongSwan 5.5.0 qui n'est pas disponible sur cette version d'EOLE.

Toutefois, le problème est très ponctuel et les tunnels seront relancés automatiquement par l'agent Zéphir assez rapidement.

Suppression du RVP

Pour supprimer un RVP, il faut lancer en tant qu'utilisateur `root` la commande `active_rvp delete`.

5. Résoudre des dysfonctionnements liés au MTU

Le PMTUd (Path MTU^[p.554] discovery), activé par défaut sur les modules EOLE, est une technique permettant de déterminer, dans un réseau informatique, la taille du MTU^[p.554] sur le chemin entre deux hôtes IP, afin d'éviter la fragmentation des paquets.



Cette configuration peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP^[p.549] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTUd est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Il est possible de forcer la valeur du MTU pour une interface donnée dans l'onglet `Réseau avancé` de l'interface de configuration du module en mode expert.



Les commandes `ping`, `ip route` et `tracert` sont utilisées pour ajuster les valeurs.

Utilisation de la commande `ping`

La commande `ping` permet de réaliser des tests en forçant la taille des paquets :

- ping OK avec une taille forcée à la valeur 1400 :

```
1 root@amon:~# ping -M do -s 1400 pcell.ac-dijon.fr -c1
2 PING listeseole.ac-dijon.fr (194.167.18.17) 1400(1428) bytes of data.
3 1408 bytes from platon.ac-dijon.fr (194.167.18.17): icmp_seq=1 ttl=62 time=1.38 ms
4
5 --- listeseole.ac-dijon.fr ping statistics ---
6 1 packets transmitted, 1 received, 0% packet loss, time 0ms
7 rtt min/avg/max/mdev = 1.380/1.380/1.380/0.000 ms
```

- ping KO avec une taille forcée à la valeur 1500 :

```
1 root@amon:~# ping -M do -s 1500 pcell.ac-dijon.fr -c1
2 PING listeseole.ac-dijon.fr (194.167.18.17) 1500(1528) bytes of data.
3 ping: local error: Message too long, mtu=1500
4
5 --- listeseole.ac-dijon.fr ping statistics ---
6 1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Utilisation de la commande `ip route`

La commande `ip route get to` permet de visualiser les problèmes de MTU.

```
1 # ip route get to 172.X.Y.Z
2 172.X.Y.Z dev eth0 src 10.67.V.W
3 cache expires 508sec mtu 1400
```

La commande `ip route flush cache` permet quant à elle de vider le cache.

Utilisation de la commande `tracpath`

La commande `tracpath` permet d'identifier où se trouvent les limitations du MTU.

```
1 # tracpath 172.X.Y.Z
2 1?: [LOCALHOST] pmtu 1500
3 1?: [LOCALHOST] pmtu 1438
4 1: 192.168.A.B 1.353ms
5 1: 192.168.C.D 1.972ms
6 2: 192.168.E.F 2.014ms
7 3: 192.168.G.H 1.657ms
8 4: 192.168.I.J 3.026ms
9 5: 192.168.K.L 2.543ms pmtu 1400
10 5: 172.M.N.O 9.930ms
11 6: no reply
12 ...
```

Voir aussi...

Onglet Réseau avancé [p.186]

Chapitre 9

Personnalisation du module

Les modules EOLE peuvent être personnalisés et adaptés afin de prendre en compte les spécificités rencontrées en production.

1. Panorama des services

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complètement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. Services liés aux bases de données

1.1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un serveur OpenLDAP.

L'installation d'`eole-annuaire` entraîne celle d'`eole-client-annuaire`.

Logiciels et services

Le paquet `eole-annuaire` s'appuie principalement sur le service slapd.

<http://www.openldap.org/>

Historique

L'annuaire LDAP est la brique centrale de plusieurs modules EOLE.

Grâce au paquet `eole-annuaire`, la configuration de base est identique sur les modules Horus, Scribe, Zéphir, Seshat et Thot bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `annuaire (id=10)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`.

1.1.2. eole-client-annuaire

Le paquet `eole-client-annuaire` permet de configurer l'utilisation d'un annuaire OpenLDAP distant (ou local dans le cas où le paquet `eole-annuaire` est également installé).

Logiciels et services

Le paquet `eole-client-annuaire` fournit les outils de base pour interroger et s'authentifier sur un annuaire OpenLDAP.

<http://www.openldap.org/>

Historique

Ce paquet est présent sur tous les modules fournissant un annuaire (Horus, Scribe, Zéphir, Seshat et Thot) et également sur ceux utilisant un annuaire comme base d'authentification (Eclair, Hâpy).

Conteneurs

Par défaut, la configuration LDAP cliente est déployée sur le maître mais les templates EOLE fournis par ce paquet sont également utilisés dans les conteneurs en fonction des besoins.

1.1.3. eole-db

Le paquet `eole-db` permet de configurer les bases de données utilisées sur un module EOLE.

Logiciels et services

Le paquet `eole-db` permet de configurer l'outil EoleDB.

Historique

EoleDB est une re-implémentation de l'ancien gestionnaire des bases de données EOLE (`eole-sql`).

Il est disponible depuis la version 2.5.2 d'EOLE.

Il est désormais utilisé par la majorité des applications web empaquetés par EOLE et Envole (OCS, GLPI, Roundcube, POSH, WordPress, Cdt, Taskfreak...).

De ce fait, il est automatiquement installé sur les serveurs possédant au moins l'une des applications utilisant cet outil.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.1.4. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de base de données Interbase^[p.550].

Logiciels et services

Le paquet `eole-interbase` s'appuie principalement sur le service xinetd.

Historique

Historiquement ce service est uniquement utilisé sur le module Horus.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `interbase (id=16)`.

Sur les modules Horus/AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`

1.1.5. eole-mysql

Le paquet `eole-mysql` permet la mise en place d'un serveur de base de données MySQL.

Logiciels et services

Le paquet `eole-mysql` s'appuie principalement sur le service mysql-server.

<http://www.mysql.fr/>

Historique

Utilisé à la base sur les modules Horus, Scribe et Sentinelle, le paquet `eole-mysql` est installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mysql (id=14)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `bdd (id=50)`

1.1.6. eole-postgresql

Le paquet `eole-postgresql` permet la mise en place d'un serveur de base de données PostgreSQL.

Logiciels et services

Le paquet `eole-postgresql` s'appuie principalement sur le service postgresql.

<http://www.postgresql.org>

Historique

Uniquement utilisé sur Zéphir, le paquet `eole-postgresql` est installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `postgresql (id=11)`.



À ce jour, aucun module EOLE n'implémente l'utilisation de ce service en mode conteneur.

1.2. Services liés aux serveurs de fichiers

1.2.1. eole-fichier-primaire

Le paquet `eole-fichie-primaire` permet la mise en place d'un serveur de fichiers complet.

Logiciels et services

Le paquet `eole-fichie-primaire` permet de gérer les services suivants :

- `smbd`, `nmbd` et `Scannedonly`^[p.560] (serveur de fichiers) ;
- `nscd` (cache).

<http://www.samba.org/>

Historique

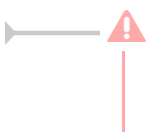
Les services fournis sont spécifiques aux modules Horus et Scribe.

Grâce au paquet `eole-fichier-primaire`, la configuration de base est identique sur les deux modules bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `partage (id=52)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.2. eole-fichier-membre

Le paquet `eole-fichier-membre` permet la mise en place d'un serveur de fichiers membre d'un domaine.

Logiciels et services

Le paquet `eole-fichier` permet de gérer les services suivants :

- `smbd`, `nmbd` et `Scannedonly`^[p.560] (serveur de fichiers) ;
- `nscd` (cache) ;
- `winbind`.

<http://www.samba.org/>

Historique

Les services fournis sont spécifiques au module eSBL.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)` .



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.3. eole-cups

Le paquet `eole-cups` permet la mise en place d'un serveur d'impression.



La gestion des imprimantes fait l'objet d'une documentation dédiée : `Imprimantes` .

Logiciels et services

Le paquet `eole-cups` permet de gérer le service cups (serveur d'impression).

<http://www.cups.org/>

Historique

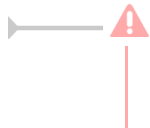
Les services fournis sont spécifiques aux modules Horus, Scribe et eSBL.

Grâce au paquet `eole-fichier`, la configuration de base est identique sur tous les modules bien que chacun conserve des spécificités et des scripts qui lui sont propres.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `fichier (id=12)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `partage (id=52)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.4. eole-proftpd

Le paquet `eole-proftpd` permet la mise en place d'un serveur FTP.

Logiciels et services

Le paquet `eole-proftpd` permet de gérer le service proftpd (serveur FTP).

<http://www.proftpd.org/>

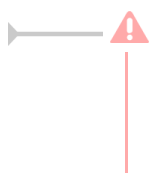
Historique

Les services fournis sont spécifiques aux modules Horus, Scribe et eSBL.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `ftp (id=25)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `partage (id=52)`.



En mode conteneur, couplé à l'un des paquets `eole-fichier`, l'accès à ce service nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_fichier_link`).

1.2.5. eole-dhcp

Le paquet `eole-dhcp` permet la mise en place d'un serveur DHCP local et/ou d'un serveur PXE.

Logiciels et services

Le paquet `eole-dhcp` s'appuie sur les services dhcp3-server et tftpd-hpa.

<http://www.isc.org/software/dhcp>

Historique

A la base, les services DHCP et TFTP étaient pré-installés uniquement sur les serveurs de fichiers (module Scribe et module Horus) ainsi que sur le serveur de clients légers Eclair, ceci avec des configurations hétérogènes et très limitées.

La mise en commun des configurations permet de bénéficier de toutes les options sur chaque module. Ce paquet peut désormais être installé sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dhcp (id=17)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `partage (id=52)`.

Sur le module Eclair 2.3 et AmonEcole+, il est installé dans le groupe de conteneurs : `ltspserver (id=54)`.

Remarques

Ne pas confondre ce paquet avec le paquet `eole-dhcrelay` qui est pré-installé sur le module Amon.

1.2.6. eole-nfs

Le paquet `eole-nfs` permet la mise en place d'un serveur NFS (partage de fichiers en réseau).

Logiciels et services

Le paquet `eole-nfs` s'appuie sur le service `nfs-kernel-server`.

<http://nfs.sourceforge.net/>

Historique

L'installation et l'activation de ce service sur le module Scribe 2.5 est obligatoire si l'on souhaite accéder aux partages par le biais d'un serveur Eclair.

Conteneurs

Le service s'installe sur système hôte (maître) et non dans un conteneur.

Remarques

Le protocole NFS étant peu sécurisé, il est recommandé de ne pas ouvrir ce service sur l'intégralité du réseau.

1.3. Services web

1.3.1. eole-web

Le paquet `eole-web` permet la mise en place d'un serveur web.



L'installation d'`eole-web` entraîne celle d'`eole-mysql`.

Logiciels et services

Le paquet `eole-web` s'appuie principalement sur le service `apache2`.

<http://httpd.apache.org/>

Il permet également d'activer l'application `phpMyAdmin`.

<http://www.phpmyadmin.net/>

Historique

À la base uniquement disponible sur les modules `Scribe/AmonEcole`, le paquet `eole-web` est désormais installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `web (id=15)`.

Sur les modules `AmonEcole` et `AmonHorus`, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Ce paquet sert de brique de base pour toutes les applications web packagées par les équipes des projets EOLE et Envole.

1.3.2. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, `Nginx`^[p.555], peut aussi faire office de serveur web.

<http://nginx.org/>

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur `Nginx`.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.3.3. eole-wpad

Le paquet `eole-wpad` permet la mise en place du service de découverte automatique du proxy par les navigateurs (WPAD^[p.564]).

Le logiciel utilisé, Nginx^[p.555], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

<http://nginx.org/>

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

Historique

Ce service étaient auparavant inclus dans le paquet `eole-reverseproxy`. Il peut désormais être installé de façon indépendante.

Le paquet `eole-wpad` est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.4. Services liés à la messagerie

1.4.1. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP Exim.

Logiciels et services

Le paquet `eole-exim` s'appuie principalement sur le service exim4.

<http://www.exim.org/>

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais utilisé sur tous les modules.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur le module AmonEcole et ses variantes, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.2. eole-spamassassin

Le paquet `eole-spamassassin` permet la mise en place d'un serveur anti-spam.

Logiciels et services

Le paquet `eole-spamassassin` s'appuie principalement sur le service spamassassin.

<http://spamassassin.apache.org/>

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-spamassassin` est désormais installable sur n'importe quel module EOLE.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.4.3. eole-courier

Le paquet `eole-courier` permet la mise en place d'un serveur POP/IMAP.

Logiciels et services

Le paquet `eole-courier` s'appuie principalement sur les services courier-imap et courier-pop.

<http://www.courier-mta.org/>

Historique

Historiquement ces services sont uniquement utilisés sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`

Remarques

Le greffon `authProg` fourni par le paquet `courier-eolecas` permet au serveur IMAP d'être compatible avec une authentification CAS.

1.4.4. eole-sympa

Le paquet `eole-sympa` permet la mise en place d'un serveur de listes de diffusion.

La gestion des listes de diffusion fait l'objet d'une documentation dédiée : `ListesDeDiffusion`.

Logiciels et services

Le paquet `eole-sympa` s'appuie principalement sur le service `sympa`.

Son interface d'administration nécessite un serveur web `apache2`.

<http://www.sympa.org/>

L'installation d'`eole-sympa` entraîne celle d'`eole-exim`.

Historique

Historiquement ce service est uniquement utilisé sur les modules Scribe/AmonEcole.

Conteneurs

Les services sont configurés pour s'installer dans le conteneur : `mail (id=13)`.

Sur les modules Scribe/AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`

1.5. Proxy et authentification

1.5.1. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

La gestion du proxy et du filtrage web fait l'objet d'une documentation dédiée : `Proxy`.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- e2guardian : filtrage web ;
- Lightsquid : analyseur de logs ;
- smb, nmbd, winbind, krb5 : authentification NTLM/KERBEROS.

<http://www.squid-cache.org/>

<http://e2guardian.org>

<http://lightsquid.sourceforge.net/>

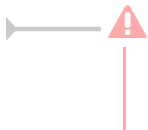
Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.



En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse ip proxy link`).

Remarques

Afin d'assurer l'authentification en mode NTLM/KERBEROS, ce paquet fournit des configurations Samba incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

1.5.2. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur RADIUS^[p.559].

Logiciels et services

Le paquet `eole-radius` s'appuie sur le projet FreeRADIUS.

<http://freeradius.org/>

Historique

Ce paquet est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le serveur maître.

1.6. Autres services réseau

1.6.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.



Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro.

<http://dev-eole.ac-dijon.fr/projects/eole-antivir>

<http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf>

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services `clamav-daemon` [<http://www.clamav.net/>] et `clamav-freshclam`.

Historique

À la base, les services `clamav` et `freshclam` étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirales (`freshclam`) s'installe sur le maître.

Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.

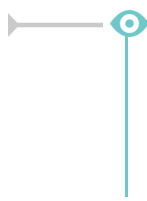
Sur les modules `AmonEcole` et `AmonHorus`, le service `clamav-daemon` est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.



C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation,

sa configuration et son démarrage dans le conteneur souhaité.



Activation de clamav dans un conteneur

```
1 <container name='xxx'>
2   <package>eole-antivirus-pkg</package>
3   <service>clamav-daemon</service>
4   <file filelist='clamav' name='/etc/clamav/clamd.conf' />
5 </container>
```

1.6.2. eole-apt-cacher-ng

Le paquet `eole-apt-cacher-ng` permet d'installer et de configurer un service de mise en cache des paquets Debian.

Logiciels et services

Le paquet `eole-apt-cacher-ng` s'appuie sur le service apt-cacher-ng.

<https://www.unix-ag.uni-kl.de/~bloch/acng/>

Historique

Ce service est pré-installé et obligatoire sur le module AmonEcole où il est utilisé par le maître et les conteneurs LXC.

Il est envisageable de l'installer sur n'importe quel module, afin, par exemple de fournir un service de mise en cache des paquets au niveau d'un établissement.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.3. eole-bareos

Le paquet `eole-bareos` permet d'installer et de configurer la solution de sauvegarde Bareos.



La gestion des sauvegardes fait l'objet d'une documentation dédiée : [Sauvegardes](#).

Logiciels et services

Le paquet `eole-bareos` s'appuie sur les services :

- bareos-dir (service directeur)
- bareos-fd (service de lecture/écriture)
- bareos-sd (service de stockage)

<http://www.bareos.org> [<http://net-snmp.sourceforge.net/>]

Historique

Ce service est pré-installé sur les modules hébergeant un serveur de fichiers (Horus, Scribe, AmonEcole).

Il est utilisable sur tous les modules EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.4. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service `bind9`^[p.542].

Historique

À la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dns (id=18)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.6.5. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP.

Logiciels et services

Le paquet `eole-dhcrelay` s'appuie sur le service `dhcp3-relay`.

<http://www.isc.org>

Historique

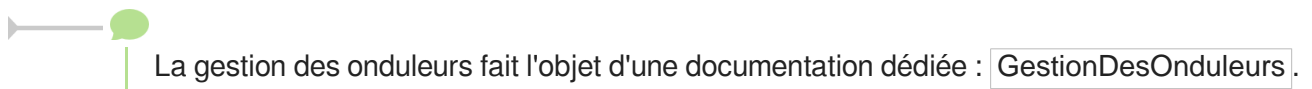
Ce service est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le maître.

1.6.6. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.



Logiciels et services

Le paquet `eole-nut` s'appuie sur le service upsd.

<http://www.networkupstools.org/>

Historique

Ce paquet est pré-installé sur tous les modules depuis la version 2.3 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.7. eole-pacemaker

Le paquet `eole-pacemaker` permet la mise en place d'un service de haute disponibilité^[p.549].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync^[p.543].

Historique

A la base, le service de haute disponibilité était uniquement disponible sur le module Sphynx via le service Heartbeat. Celui-ci se fait maintenant via les logiciels Corosync^[p.543] et Pacemaker. Le service a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service s'installe sur le serveur maître.

1.6.8. eole-snmpd

Le paquet `eole-snmpd` permet d'installer et de configurer un serveur SNMP.

Logiciels et services

Le paquet `eole-snmpd` s'appuie sur le service snmpd.

<http://net-snmp.sourceforge.net/>

Historique

Ce service n'est pré-installé sur aucun module.

Il a été créé et mis à disposition pour répondre à un besoin exprimé par plusieurs académies.

Conteneurs

Le service s'installe sur le maître.

1.6.9. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN^[p.559].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan^[p.562].

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés ainsi que sur le module Sphynx.

Conteneurs

Le service s'installe sur le serveur maître.

2. Personnalisation du serveur à l'aide de Creole

Creole^[p.544] est un ensemble d'outils permettant de mettre en œuvre un serveur suivant une configuration définie.

Il offre des possibilités de personnalisation, permettant à l'utilisateur d'ajouter des fonctionnalités sur le serveur sans risquer de créer une incohérence avec la configuration par défaut et qui ne seront pas écrasées par les futures mises à jour.

Pour personnaliser un serveur, les outils suivants sont à disposition :

- le **patch**^[p.558] : permet de modifier un template^[p.562] fourni par EOLE ;
- le **dictionnaire**^[p.544] **local** permet d'ajouter des options à l'interface de configuration, d'installer de nouveaux paquets ou de gérer de nouveaux services ;
- le **template**^[p.562] reprend le fichier de configuration d'une application avec, éventuellement, une personnalisation suivant des choix de configuration.

2.1. Répertoires utilisés par EOLE

Répertoires liés au logiciel Creole

Dictionnaires

- `/usr/share/eole/creole/dicos/` : contient les dictionnaires fournis par la distribution ;
- `/usr/share/eole/creole/dicos/local/` : contient les dictionnaires créés localement pour le serveur ;
- `/usr/share/eole/creole/dicos/variante/` : contient les dictionnaires fournis par une variante Zéphir.

Templates

- `/usr/share/eole/creole/distrib/` : contient tous les templates (distribution, locaux et issus de variantes) ;
- `/usr/share/eole/creole/modif/` : répertoire à utiliser pour créer des patch avec l'outil `gen_patch` ;
- `/usr/share/eole/creole/patch/` : contient les patch réalisés localement (avec ou sans l'outil `gen_patch`) ;
- `/usr/share/eole/creole/patch/variante/` : contient les patch fournis par une variante Zéphir ;
- `/var/lib/eole/` : répertoire recommandé pour le stockage des fichiers templatisés nécessitant un traitement ultérieur ;
- `/var/lib/creole/` : contient la copie des templates après la phase de patch (traitement interne à Creole).

Autres répertoires spécifiques

- `/etc/eole/` : contient les fichiers de configuration majeurs du module ;
- `/var/lib/eole/config/` : contient les fichiers de configuration de certains outils internes ;
- `/var/lib/eole/reports/` : contient des fichiers de rapport (pour affichage dans l'EAD, par exemple) ;
- `/usr/lib/eole/` : bibliothèques shell EOLE (remplacent *FonctionsEoleNg*) ;
- `/usr/share/eole/sbin/` : scripts EOLE ;
- `/usr/share/eole/diagnose/` : scripts *diagnose*.

2.2. Création de patch Creole

Si le fait de renseigner correctement les options de configuration n'offre pas une souplesse suffisante, il faut envisager des adaptations complémentaires.

Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à chaque `instance/reconfigure`.

Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch.

L'outil `gen_patch` vous permet de générer facilement un nouveau patch. Pour ce faire il suffit de copier le fichier de configuration depuis `/usr/share/eole/creole/distrib/` vers `/usr/share/eole/creole/modif/`, de le modifier et de lancer la commande `gen_patch`.



Copie du fichier du template d'origine :

```

root@scribe:~# cp /usr/share/eole/creole/distrib/php.ini
/usr/share/eole/creole/modif/
Changement des paramètres :
root@scribe:~# vim /usr/share/eole/creole/modif/php.ini
Exécution de la commande gen_patch :
root@scribe:~# gen_patch
** Génération des patches à partir de modif **
Génération du patch php.ini.patch
** Fin de la génération des patch **
root@scribe:~#

```

Une fois le patch créé, il faut lancer la commande `reconfigure` pour que les nouvelles options soient prises en compte.

La commande `diagnose` renvoie un diagnostic sur les patch :

```

[... ]
*** Patches
. patches => Ok
[... ]

```

Sont concernés par la procédure de patch uniquement les fichiers déjà présents dans le répertoire des templates et référencés dans les dictionnaires fournis par l'équipe EOLE.

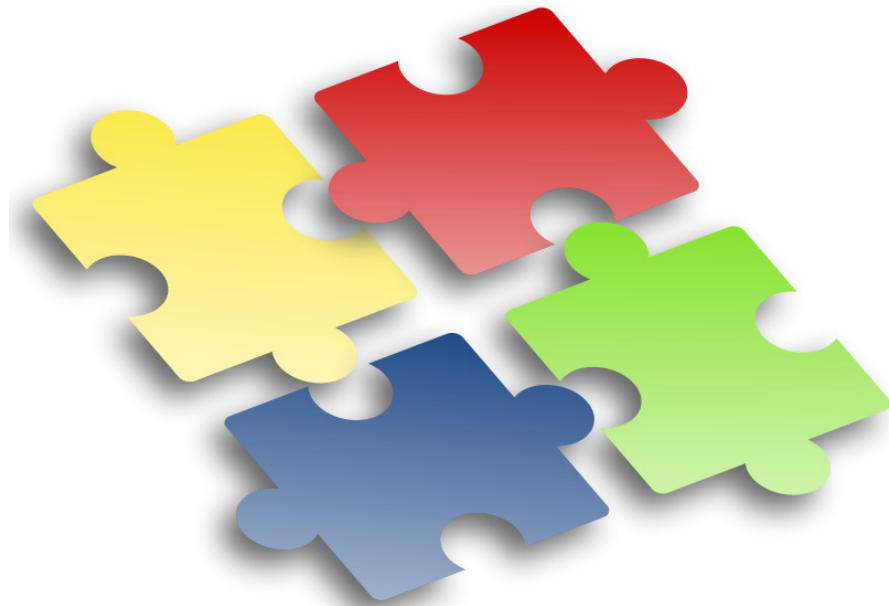
Pour les autres fichiers, l'utilisation de dictionnaires locaux et de templates personnalisés est recommandée.

Le répertoire `/usr/share/eole/creole/` contient les répertoires suivants :

- **./distrib/** : templates originaux fournis principalement par le paquet conf d'un module ;
- **./modif/** : endroit où doivent être copiés et modifiés les templates souhaités ;
- **./patch/** : fichiers patch générés à partir des différences entre les deux répertoires précédents.

Le répertoire `/var/lib/creole/` comprend les templates finaux, c'est à dire les templates initiaux avec éventuellement des patches.

Pour désactiver un patch, il suffit de supprimer ou de déplacer le fichier patch.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptibles d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

2.3. Les dictionnaires Creole

En cas d'ajout de templates^[p.562] et de variables supplémentaires, il est nécessaire de créer un dictionnaire local.

Ce dictionnaire peut également comprendre des noms de paquet supplémentaire à installer ainsi que des services à gérer.

Un dictionnaire local est un dictionnaire personnalisé permettant d'ajouter des options à Creole.

Un dictionnaire Creole contient un en-tête XML suivi d'une balise racine `<creole></creole>`.

Structure générale d'un dictionnaire XML Creole

```
<?xml version='1.0' encoding='utf-8'?>
<creole>
  <files>
</files>
  <containers>
```

```

</containers>
<variables>
</variables>
<constraints>
</constraints>
<help>
</help>
</creole>

```



Il est toujours intéressant de regarder dans les dictionnaires déjà présents sur le module pour comprendre les subtilités des dictionnaires Creole.



Vous pouvez également vous référer à la DTD^[p.545] :
<https://dev-eole.ac-dijon.fr/projects/creole/repository/revisions/master/entry/data/creole.dtd>

2.3.1. Ajouter un en-tête XML

L'en-tête est standard pour tous les fichiers XML :

```
<?xml version="1.0" encoding="utf-8"?>
```

Cet en-tête est nécessaire pour que le fichier soit reconnu comme étant au format XML.

Afin d'éviter les problème d'encodage, il est conseillé de créer le fichier sur un module EOLE (avec l'éditeur de texte vim).



Ajouter la configuration suivante en bas de votre fichier pour forcer l'indentation :

```

<!-- vim: ts=4 sw=4 expandtab
-->

```

Voir aussi...

L'éditeur de texte Vim ^[p.286]

2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu

Maître ou conteneur : <files> ou <containers>

Creole propose un système de conteneurs permettant d'isoler certains services du reste du système.

C'est dans le dictionnaire que les conteneurs sont définis et associés à des services.

Si le conteneur n'est pas spécifié, les services seront installés sur le serveur hôte, le maître.

Pour distinguer les fichiers templates, les paquets et les services de l'hôte de ceux mis dans le conteneur, il faut utiliser deux balises différentes.

Sur le serveur hôte, les fichiers templates, les paquets et les services sont dans une balise **<files>**.

Dans le cas des conteneurs, il faut spécifier un ensemble de balises **<container>** à l'intérieur d'une balise **<containers>**. L'utilisation de la balise **<all>** permet d'appliquer des balises à tous les **<container>**. En mode non conteneur cette balise s'applique sur le maître. Pour inhiber ce comportement il faut rajouter l'attribut **instance_mode='when_container'**.

La balise **<container>** doit obligatoirement contenir l'attribut **name** pour renseigner le nom du conteneur.

Lors de la première déclaration d'un conteneur l'attribution d'un identifiant unique (attribut **id**) est obligatoire.

La valeur de cet identifiant permettra de calculer l'adresse IP du conteneur.

Les groupes de conteneurs permettent de réunir des services afin de limiter le nombre de conteneurs.

Ils se déclarent de la même manière que les autres conteneurs. L'affectation d'un conteneur existant à un groupe de conteneurs s'effectue en utilisant l'attribut **group**.

Les ID de groupes de conteneurs de 50 à 99 sont réservés pour les groupes de conteneurs EOLE.

ID	Nom du groupe conteneur	Conteneurs inclus (AmonEcole/Eclair)
50	bdd	annuaire, mysql
51	reseau	web, mail
52	partage	fichier, dhcp, ftp
53	internet	proxy, dns
54	ltspserver	dhcp, ltsp
55	ltspapps	application

Les identifiants de conteneur supérieurs à 100 sont utilisables par les contributeurs.

La liste des identifiants des conteneurs et des groupes de conteneurs déjà affectés est actuellement maintenue sur le wiki EOLE à l'adresse : <http://dev-eole.ac-dijon.fr/projects/creole/wiki/ContainersID>

```

1 <creole>
2   <files>
3   </files>
4   <containers>
5     <all>
6       <host hostlist='web' name='web_url' ip='adresse_ip_br0'
7 instance_mode='when_container' comment="Serveur web sur l'IP eth0" />
8       <file filename='/etc/fichier_cible' instance_mode=
9 'when_container' />
10      </all>
11     <container name='web' id='15'>
12       [...]

```



```

11         </container>
12         <container name='reseau' id='51' />
13         <!-- affectation du conteneur web au groupe de conteneurs reseau
-->
14         <container name='web' group='reseau' />
15     </containers>
16     [...]

```

Paquets : <package>

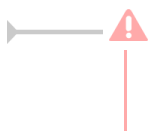
Creole permet de spécifier les paquets à installer pour profiter d'un nouveau service.

A l'instanciation de la machine, les paquets spécifiés seront installés.

Pour cela, il faut utiliser la balise <package> avec comme contenu le nom du paquet.

Les attributs de la balise <package>

- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : *when_container*, *when_no_container*, *always* (par défaut).



Pour spécifier plusieurs paquets, il faut obligatoirement écrire une balise <package> par paquet.

Fichiers templates : <file>

Les fichiers templates sont définis dans la balise <file>.

Les attributs de la balise <file>

- l'attribut **name** (obligatoire) indique l'emplacement où sera copié le fichier ;
- l'attribut **source** permet d'indiquer un nom de fichier source différent de celui de destination ;
- l'attribut **mode** permet de spécifier des droits à appliquer au fichier de destination ;
- l'attribut **owner** permet de forcer le propriétaire du fichier ;
- l'attribut **group** permet de forcer le groupe propriétaire du fichier ;
- l'attribut **filelist** permet de conditionner la génération du fichier suivant des contraintes ;
- si l'attribut **rm** vaut *True*, le fichier de destination sera supprimé si il est désactivé via une *filelist* ;
- si l'attribut **mkdir** vaut *True*, le répertoire destination sera créé si il n'existe pas ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : *when_container*, *when_no_container*, *always* (par défaut) ;
- l'attribut **del_comment** engendre la suppression des lignes vides et des commentaires dans le fichier cible afin d'optimiser sa templatisation (exemple : `del_comment='#'`).



Renommage d'un template

L'attribut **name** contient toujours le chemin complet du fichier de destination (par exemple `/etc/hosts`).

Par défaut, le fichier template doit s'appeler de la même façon que le fichier de destination (ici : `hosts`).

Si deux templates ont le même nom, il faudra spécifier le nom du template renommé avec l'attribut **source**.

Services : <service>

Les dictionnaires Creole intègrent un système de gestion de services GNU/Linux (scripts d'init) qu'il est possible d'utiliser pour activer/désactiver des services non gérés par le module EOLE installé.

Services non gérés : services non référencés dans le système de gestion des services de Creole. Ils ne sont jamais modifiés. Ils restent dans l'état dans lequel Ubuntu les a installés ou dans celui que leur a donné l'utilisateur. Les services non gérés sont généralement les services de base Ubuntu (rc.local, gpm, ...) et tous ceux pour lesquels le module ne fournit pas de configuration spécifique (mdadm, ...).

Services désactivés : services systématiquement arrêtés et désactivés lors des phases d'instance et de reconfigure. Les services concernés sont généralement liés à une réponse à "non" dans l'interface de configuration du module.

Services activés : services systématiquement activés et (re)démarrés lors des phases d'instance et de reconfigure. Les services concernés sont ceux nécessaires au fonctionnement du module.

Les services à activer/désactiver se définissent dans le dictionnaire grâce à la balise **<service>**.

Les attributs de la balise <service>

- l'attribut **startlevel** (entier) permet de spécifier le niveau de démarrage ;
- l'attribut **stoplevel** (entier) permet de spécifier le niveau d'arrêt ;
- l'attribut **servicelist** (chaîne de caractères alphanumériques) permet de conditionner le démarrage ou l'arrêt d'un service suivant des contraintes ;
- l'attribut **method** permet de définir la façon de gérer le service : `initd`, `upstart` ou `service` (par défaut) ;
- l'attribut **hidden** (booléen) indique si le service doit être activé ou non, cet attribut est particulièrement utile lors de la redéfinition d'un service, en particulier pour forcer sa désactivation ;
- si l'attribut **pty** vaut `False`, le pseudo-terminal ne sera pas utilisé (nécessaire pour certains services) ;
- si l'attribut **redefine** vaut `True`, cela permet de redéfinir un service déjà défini dans un autre dictionnaire ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence ou non du mode conteneur : `when_container`, `when_no_container`, `always` (par défaut).

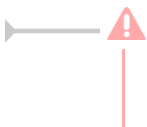
La balise `service` peut également être utilisée pour activer/désactiver des configurations de site web apache2 (commandes : `a2ensite` / `a2dissite`).

Comme pour les services système, l'activation d'un site peut être conditionnée par une `servicelist`.

On peut ainsi gérer le lien symbolique suivant : `/etc/apache2/sites-enabled/monsite` avec :

```
<service method='apache' servicelist='siteperso'>monsite</service>
```

Le fichier de configuration `monsite` étant stocké dans `/etc/apache2/sites-available/`.



Pour spécifier plusieurs services, il faut obligatoirement écrire une balise **<service>** par service.

Une règle `eole-firewall` peut être liée à un service, ainsi quand un service sera désactivé la règle le sera également.

Hôtes : <host>

La balise `<host>` permet de déclarer des hôtes à ajouter dans le fichier `/etc/hosts` du maître et/ou des conteneurs.

Les attributs de la balise <host>

- l'attribut **name** contient le nom d'une variable contenant des noms d'hôtes (FQDN), simple ou multi, obligatoire ;
- l'attribut **ip** contient le nom d'une variable contenant les adresses IPs associées aux noms, obligatoire ;
- l'attribut **hostlist** permet d'exclure cette entrée suivant des contraintes, optionnel ;
- l'attribut **crossed** combine toutes les adresses avec tous les noms d'hôtes. L'utilisation de `False` génère une association 1 nom d'hôte/1 adresse IP. Doit être `False` dans le cas d'utilisation de variables ayant une relation maître/esclave, `False`, `True` (par défaut) ;
- l'attribut **instance_mode** permet de définir un comportement en fonction de la présence du mode conteneur ou non : `when_container`, `when_no_container`, `always` (par défaut) ;
- l'attribut **comment** permet l'ajout d'une ligne de commentaire avant la(les) entrée(s), optionnel.

```
<containers>
<container name="proxy" id='20'>
<package>eole-proxy-pkg</package>
<service startlevel='30' stoplevel='30'>squid3</service>
<host hostlist='auth smb' name='nom_serveur_smb'
ip='ip_serveur_smb' instance_mode='when_container' crossed='False'
comment='serveurs d'authentification SMB'/>
</container>
</containers>
```

Montage d'une partition <disknod>

La balise `<disknod>` permet de le montage d'une partition du maître à l'intérieur d'un conteneur. Par exemple, le montage de la partition `/home` dans le conteneur fichier.

Les attributs de la balise <disknod>

La balise `<disknod>` ne possède pas d'attribut spécifique.

```
<containers>
<container name='fichier' id='12'>
```

```
<disknod>/home</disknod>
</container>
<containers>
```



Pour être pris en compte il faut nécessairement arrêter le conteneur avec la commande `CreoleService lxc stop` avant de faire un `gen_conteneurs`.

Montage d'un répertoire <fstab>

La balise <fstab> sert à déclarer le montage d'un répertoire (qui n'est pas une partition) à l'intérieur d'un conteneur.

Par exemple, le montage du répertoire `/home/mail/` du maître dans le conteneur mail.

Les attributs de la balise <fstab>

- l'attribut **name** contient le chemin du répertoire à monter ou le nom d'une variable fournissant cette information ;
- si l'attribut **name_type** vaut *SymLinkOption* cela indique que le chemin sera défini dans la variable indiquée dans l'attribut **name** ;
- l'attribut **fstablist** (chaîne de caractères alphanumériques) permet de conditionner le montage du répertoire suivant des contraintes.



```
<containers>
<container name='mail' id='13'>
<fstab name='/home/mail' />
</container>
</containers>
```



Pour être pris en compte il faut nécessairement arrêter le conteneur avec la commande `CreoleService lxc stop` avant de faire un `gen_conteneurs`.

Autorisations pour le pare-feu eole-firewall : <service_access> et <service_restriction>

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper^[p.562] et l'activation de modules noyau.

⚠ eole-firewall et ERA

Pour les modules Amon et AmonEcole, les règles d'`eole-firewall` ne s'appliquent pas. Seules les règles ERA du modèle choisi s'appliquent.

Les doublons

S'il y a plusieurs règles sur une interface/port, c'est la dernière règle qui est appliquée .

Par exemple, dans le dictionnaire `20_apache.xml`, on redirige le port `80` dans le conteneur mais dans `25_nginx.xml`, on ouvre le port `80`. Si ces deux dictionnaires sont installés simultanément, c'est l'ouverture du port qui est appliquée.

L'activation des règles

Si le nom du service correspond a un service déclaré dans le conteneur et que celui-ci est désactivé, alors les accès/restrictions ne s'appliquent pas.

Si `ip` est une variable et que cette variable n'existe pas ou qu'elle est désactivée, la règle ne s'applique pas.

De la même façon pour un port/tcpwrapper avec une variable qui n'existe pas, aucune règle ne s'applique.

Malgré son nom, l'attribut `service` des balises `service_access` et `service_restriction` doit être renseigné avec le nom de la `servicelist` associée au service et non avec le nom du service lui-même.

Si aucune `servicelist` permettant de désactiver le service n'existe, l'attribut peut être rempli librement.

Autoriser un port (XXX) pour un service donné (YYY) :

```
<service_access service='YYY'>
  <port>XXX</port>
</service_access>
```

Dans la balise `port` il est également possible de spécifier le protocole (par défaut c'est TCP).

Par exemple :

```
<service_access service='ntp'>
  <port protocol='udp'>123</port>
</service_access>
```

Avec tcpwrapper :

```
<tcpwrapper>YYY</tcpwrapper>
```

Port avec variable (ZZZ) :

```
<port port type="SymLinkOption">ZZZ</port>
```

List (WWW) pour port/tcpwrapper :

```
<port service accesslist="WWW">XXX</port>
```

```
<tcpwrapper service accesslist="WWW">YYY</tcpwrapper>
```

➤ Règles `eole-firewall` extraites du dictionnaire

`/usr/share/eole/creole/dicos/01_network.xml` pour le service `sshd`

```

1 <service_access service='sshd'>
2   <port>22</port>
3   <tcpwrapper>sshd</tcpwrapper>
4 </service_access>
5 <service_restriction service='sshd'>
6   <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type=
7   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
8   <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type=
9   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
10  <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type=
11  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
12  <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type=
13  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
14  <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type=
15  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
16 </service_restriction>
```

Si on ne définit que les `service_access`, le port est ouvert pour tout le monde sur toutes les interfaces.

Pour ajouter des restrictions il faut mettre :

```
<service_restriction service='YYY'>
```

```
  <ip interface='eth0'>1.1.1.1</ip>
```

```
</service_restriction>
```

Dans ce cas, seule l'adresse IP `1.1.1.1` peut accéder à ce service.

Il est possible d'utiliser des variables :

```
<ip interface='auto' ip_type='SymLinkOption'>variable</ip>
```

Il est possible d'utiliser un netmask :

```
<ip interface='eth0' netmask="255.255.255.0" ip_type='SymLinkOption'>variable</ip>
```

```
<ip interface='eth1' netmask="variable_netmask" netmask_type='SymLinkOption' ip_type='SymLinkOption'>variable</ip>
```

Le paramètre `interface` peut être :

- `ethX` (pour une interface donnée) ;
- `all` (pour toutes les interfaces) ;
- `auto` (calcul de l'interface via la route) ;
- une variable (avec l'ajout de `interface_type="SymLinkOption"`).

Il est aussi possible d'ajouter une `service_restrictionlist` aux balises `ip`.

➤ Règles `eole-firewall` extraites du dictionnaire `/usr/share/eole/creole/dicos/01_network.xml` pour le service `genconfig`

```

1 <service_access service='genconfig'>
2   <port>7000</port>
3 </service_access>
4 <service_restriction service='genconfig'>
5   <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type=
6   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
7   <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type=
8   'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
9   <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type=
10  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
11  <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type=
12  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
13  <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type=
14  'SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
15 </service_restriction>

```

Complément sur les attributs

instance_mode

L'attribut `instance_mode` remplace les anciens attributs `in_container` et `container_only`.

Une ressource, qu'elle soit sur le maître ou dans un conteneur, peut n'être à générer que si le mode conteneur est activé ou désactivé :

instance_mode	mode conteneur	mode non conteneur
when_container	✓	
when_no_container		✓
always (default)	✓	✓

Les balises acceptant l'attribut `instance_mode` sont actuellement :

- package ;
- file ;
- service ;
- host.

Exemple récapitulatif

➤ Fichiers templates, paquets et services locaux ou dans un conteneur

```

1 <containers>
2   <!-- dans le conteneur mon_reverseproxy -->
3   <container name="mon_reverseproxy" id='101'>
4     <package>nginx</package>
5     <service servicelist="myrevprox" startlevel='91'>nginx</service>
6     <file filelist='myrevprox' name='/etc/nginx/sites-enabled/default'
7     source='nginx.default' />
8     <file filelist='myrevprox' name='/var/www/nginx-default/nginx.html' rm
9     ='True' />
10  </container>
11 </containers>
12 <files>

```



```

11 <!-- sur le maître-->
12 <service>ntp</service>
13 <file name='/etc/ntp.conf/>
14 <file name='/etc/default/ntpdate' owner='ntp' group='ntp' mode='600' />
15 <file name='/etc/strange/host' source='strangehost.conf' mkdir='True' />
16 </files>

```

Voir aussi...

Choisir le mode du module [p.58]

2.3.3. Utiliser des familles, variables et des séparateurs

Variables : <variables>

L'ensemble des familles et, ainsi, des variables sont définies dans un nœud <variables></variables>.

Familles : <family>

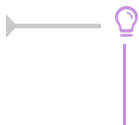
Un conteneur famille permet d'avoir des catégories de variables. Celle-ci correspond à un onglet dans l'interface. Les familles sont incluses obligatoirement dans une balise <variables>.



Une famille **Squid** pour gérer toutes les variables relatives a *Squid*.

Les attributs de la balise *family* sont les suivants :

- l'attribut **name** (obligatoire) est à la fois le nom et l'identifiant de la famille ;
- l'attribut **mode** permet de définir le mode d'affichage de la famille :
 - mode basic par défaut ;
 - mode normal ;
 - mode expert.
- l'attribut **icon** définit une image associée à l'onglet ;
- l'attribut **hidden** indique si la famille doit être affichée ou non, sa valeur pouvant être modifiée via une condition (voir plus bas).



Une famille dont toutes les variables sont cachées (hidden) ou désactivées (disabled) ne sera pas affichée sauf en mode debug.



Les icônes utilisés proviennent des bibliothèques de polices et d'icônes libres :

- Font Awesome : <http://fontawesome.github.io/Font-Awesome/icons> ;
- Font Mfizz : <http://fizzed.com/oss/font-mfizz>.

Pour choisir une icône, il faut se rendre sur les pages ci-dessus et recopier le nom de l'icône. Pour la font Mfizz il faut enlever le préfixe `icon-`.

```
<family name='messagerie' mode='basic' icon='enveloppe'>
  <variable name='system_mail_from' type='mail' description="Adresse
  électronique d'envoi pour le compte root"/>
</family>
```

Variable : <variable>

Une variable contient une description et, optionnellement, une valeur EOLE par défaut.

Les variables peuvent être à valeur unique ou multi-valuées.

Les balises <variable> sont incluses obligatoirement dans une balise <family>.

Les attributs de la balise *variable* sont les suivants :

- l'attribut **name** (obligatoire) est le nom de la variable ;
- l'attribut **type** (obligatoire) permet d'utiliser un type EOLE avec des vérifications automatiques (fonctions de vérifications associées à chaque type de variable) ;
- l'attribut **description** permet de définir le libellé à afficher dans l'interface de configuration du module ;
- l'attribut **multi** permet de spécifier qu'une variable pourra avoir plusieurs valeurs (par exemple pour un DNS, on aura plusieurs adresses IP de serveurs DNS) ;
- l'attribut **mode** permet de définir le mode d'affichage de la variable (*basic*, *normal* ou *expert*) ;
- si l'attribut **hidden** vaut *True*, la variable ne sera pas affichée dans l'interface de configuration (on peut par exemple souhaiter masquer des variables dont la valeur est calculée automatiquement) ;
- si l'attribut **disabled** vaut *True*, la variable sera déclarée comme désactivée.
- si l'attribut **mandatory** vaut *True*, la variable sera considérée comme obligatoire, cet attribut remplace l'ajout d'un *check obligatoire* au niveau des conditions ;
- si l'attribut **redefine** vaut *True*, cela permet de redéfinir une variable déjà définie dans un autre dictionnaire ;
- si l'attribut **exists** vaut *False*, cela permet de définir une variable si et seulement si elle n'a pas déjà été définie dans un autre dictionnaire.
- si l'attribut **remove_check** vaut *True* pour une variable redéfinie, alors toutes les validations (*check*) associées à cette variable sont réinitialisées ;
- si l'attribut **remove_condition** vaut *True* pour une variable redéfinie, alors toutes les conditions associées à cette variable sont réinitialisées (attention, **remove_condition** n'est disponible qu'à partir de la version **EOLE 2.5.2**) ;
- si l'attribut **auto_freeze** vaut *True*, la variable devient à verrouillage automatique. Sa valeur est verrouillée dès le premier enregistrement de la configuration. Dans l'interface de configuration du module, ces variables sont identifiées par la présence d'un cadenas. Ce dernier apparaît verrouillé une fois le serveur instancié ;
- si l'attribut **auto_save** vaut *True*, la variable devient à enregistrement obligatoire. Sa valeur est obligatoirement enregistrée dans le fichier de configuration et elle n'est donc pas automatiquement modifiée si sa valeur par défaut change au niveau des dictionnaires. On retrouve ainsi un fonctionnement équivalent à celui disponible sur EOLE 2.3.

Les principaux types de variables Creole sont les suivants :

- *number* : la valeur de la variable doit être du type "int". La fonction python `int(value)` ne doit pas retourner d'erreur ;
- *string* : la valeur de la variable doit être du type "unicode" ;
- *ip* : valeur de type IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *local_ip* : la même chose que IP, sauf que les adresses réservées et privées soulèvent un warning (voir IPy pour des informations sur les adresses réservées et privées) ;
- *netmask* : adresse de masque réseau. La valeur doit passer ce test : `IPy.IP('0.0.0.0/{0}'.format(value))` ;
- *network* : adresse réseau. La valeur doit passer ce test : `IPy.IP(value)` ;
- *broadcast* : adresse de broadcast. : La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))` ;
- *netbios* : alphanumérique autorisé sauf pour le 1er caractère qui doit forcément être du type alpha, minimum 2 et maximum 15 caractères ;
- *domain* :
 - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`
 - ou
 - alphanumérique et '.' autorisé sauf pour le 1er caractère qui doit forcément être du type alpha. Le '.' est obligatoire. Minimum 2 et maximum 255 caractères ;
- *domain_strict* : nom DNS uniquement (adresse IP interdite) ;
- *unix_user* : nom d'utilisateur ou de groupe Unix ;
- *web_address* : adresse Internet. Doit débuter par `http://` ou `https://` ;
- *hostname* :
 - adresse IP. La valeur doit passer ce test : `IPy.IP('{0}/32'.format(value))`
 - ou
 - alphanumérique autorisé sauf pour le 1er caractère qui doit forcément être du type alpha. Minimum 2 et maximum 63 caractères ;
- *hostname_strict* : nom d'hôte uniquement (adresse IP interdite) ;
- *mail* : adresse e-mail ;
- *port* : entier compris entre 1 et 65535 ;
- *filename* : tout chemin Unix (fichier ou répertoire) ;
- *oui/non* : seules valeurs possibles : "oui" et "non" ;
- *yes/no* : seules valeurs possibles : "yes" et "no" ;
- *on/off* : seules valeurs possibles : "on" et "off" ;

Comportement avec `redefine='True'` et `remove_check='False'`

- si la nouvelle variable fournit une valeur par défaut, elle remplace l'ancienne ;

- si la nouvelle variable fournit un ou plusieurs des attributs suivants : *description*, *hidden*, *mandatory*, *auto_freeze*, *mode*, les valeurs des nouveaux attributs remplacent les anciennes ;
- les attributs *type* et *multi* ne sont pas modifiables ;
- si un nouveau *valid_enum* est défini dans les fonctions *checks*, il remplace l'ancien ;
- si de nouveaux *disabled_if(_not)_in* sont définis, ils remplacent les anciens ;
- les autres conditions et contraintes sont ajoutées à celles qui étaient déjà définies.

Valeur : <value>

A l'intérieur d'une balise <variable>, il est possible de définir une balise <value> permettant de spécifier la valeur par défaut de la variable.

Séparateurs : <separators> et <separator>

Les séparateurs permettent de définir des barres de séparation au sein d'une famille de variable dans l'interface de configuration.

Les séparateurs définis dans un dictionnaire sont placés dans la balise <separators></separators> dans la balise <variables>.

A l'intérieur de la balise <separators> il faut spécifier autant de balises <separator> que de séparateurs souhaités.

Les attributs de la balise *separator* sont les suivants :

- l'attribut **name** (obligatoire) correspond au nom de la variable suivant le séparateur ;
- si l'attribut **never_hidden** vaut *True*, le séparateur sera affiché même si la variable associée est masquée.

Dans le cas où il n'y a aucune variable à afficher dans le bloc défini par le séparateur, celui-ci est forcément masqué.

Exemple

Variables, familles et séparateurs

```
<variables>
  <family name='services'>
    .. <variable name='activer_esu' type='oui/non'
      description="Utiliser le logiciel ESU" hidden='True'>
    .. <value>oui</value>
    .. </variable>
  .. </family>
  <family name='esu'>
    .. <variable name='esu_proxy' type='oui/non'
      description="Activer le proxy ESU">
```

```

    <value>non</value>
  </variable>
  <variable name='esu proxy server' type='domain'
description='Adresse du proxy ESU' mandatory='True' />
  <variable name='esu proxy port' type='port' description='Port
du proxy ESU' mandatory='True'>
    <value>3128</value>
  </variable>
  <variable name='esu proxy bypass' type='string'
description='Ne pas utiliser le proxy ESU pour' multi='True'>
    <value>127.0.0.1</value>
  </variable>
</family>
<separators>
  <separator name='esu proxy'>Proxy ESU</separator>
</separators>
</variables>

```

2.3.4. Comportement des variables

En plus des propriétés décrites explicitement dans les dictionnaires Creole, certaines variables se voient ajouter des contraintes ou des modifications de propriétés en fonction de certains paramètres.

Les variables possédant la propriété `auto freeze='True'` sont obligatoirement affichées en mode basique lors de la saisie initiale, ceci afin d'attirer l'attention de l'utilisateur sur le fait qu'elles ne seront plus modifiables ultérieurement.

Une exception a été ajoutée à cette règle, si la propriété `expert='True'` est explicitement ajoutée sur la variable, celle-ci apparaîtra uniquement dans le mode expert.

Les variables obligatoires (`mandatory='True'`) ne possédant pas de valeur par défaut (calculée ou non) sont obligatoirement affichées en mode basique, puisque l'utilisateur devra forcément les renseigner.

Les variables non obligatoires (`mandatory='False'`) possédant une valeur par défaut (balise `<value>`) deviennent obligatoires.

2.3.5. Mettre en place des contraintes

Des fonctions (contraintes) peuvent être utilisées pour grouper / tester / remplir / conditionner des variables.

L'ensemble des contraintes d'un dictionnaire se place à l'intérieur d'un nœud XML

<constraints></constraints>.

Lien entre variables : <group>

Il est possible de lier des variables sous la forme d'une relation maître-esclave(s).

La variable maître doit obligatoirement être multi-valuée (`multi='True'`).

Elle se définit dans l'attribut **master**.

Les variables esclaves sont définies entre les balises <slave>.

Les variables esclaves deviennent automatiquement multi-valuées.

```
<group master='adresse_ip_eth0'>
  <slave>adresse_netmask_eth0</slave>
  <slave>adresse_network_eth0</slave>
</group>
```

Calcul automatique modifiable <fill> ou non <auto>

Le calcul automatique permet d'associer automatiquement (par le calcul) une valeur par défaut à une variable.

Cette valeur peut être :

- éditable par l'utilisateur : balise <fill> ;
- non éditable par l'utilisateur (exemple : l'IP d'un serveur en DHCP) : balise <auto>.

Contrairement aux versions précédentes si l'utilisateur a choisi de conserver la valeur par défaut d'une variable affectée par un *fill*, le calcul de la valeur sera réalisé à chaque fois, comme pour les variables *auto* sauf si la variable possède l'attribut `auto_save='True'`.

Les calculs *auto* ne sont pas compatibles avec les variables à verrouillage automatique (`auto_freeze`) ou à enregistrement obligatoire (`auto_save`).

L'attribut *name* correspond au nom de la fonction qui sera utilisée pour le calcul.

Les fonctions utilisées peuvent être :

- des fonctions natives de Tiramisu^[p.562] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

L'attribut de la balise *param* : `optional='True'` : indique que le paramètre sera ignoré si la variable associée n'existe pas. Cela permet de contourner les erreurs du type : Utilisation de la variable <param var name> non présente dans un calcul

L'attribut de la balise *param* : `hidden='False'` : indique que le paramètre sera ignoré si la variable possède des propriétés incompatibles avec le calcul (variable désactivée, variable obligatoire sans

valeur, ...). Cela permet de contourner les erreurs du type : `impossible d'effectuer le calcul, l'option <target var name> a les propriétés : ['disabled'] pour : <param var name>`

Les principales fonctions de calcul utilisables avec les balises fill et auto sont les suivantes :

- **calc_network** : calcule l'adresse réseau par défaut à partir d'une IP et d'un masque de sous-réseau


```
<fill name='calc_network' target='my_network'>
  <param type='eole' name='ip'>my_ip</param>
  <param type='eole' name='netmask'>my_netmask</param>
</fill>
```
- **calc_broadcast** : calcule l'adresse de broadcast à partir d'une adresse IP et d'un masque de sous-réseau


```
<fillname='calc_broadcast' target='my_broadcast'>
  <param type='eole' name='ip'>my_ip</param>
  <param type='eole' name='netmask'>my_netmask</param>
</fill>
```
- **calc_val** : renvoie la valeur passée en paramètre (généralement la valeur d'une autre variable)


```
<fill name='calc_val' target='nom_machine'>
  <param type='eole' name='valeur'>eole module</param>
</fill>
```
- **calc_val_first_value** : renvoie la valeur de la première variable définie


```
<fill name='calc_val_first_value' target='eolesso_adresse'>
  <param type='eole' optional='True' hidden='False'>web_url</param>
  <param type='eole'>adresse_ip_eth0</param>
</fill>
```
- **calc_multi_val** : renvoie les valeurs passées en paramètre en supprimant les doublons


```
<fill name='calc_multi_val' target='ssl_organization_unit_name'>
  <param>110 043 015</param>
  <param type='eole'>nom_academie</param>
  <param type='eole'>numero_etab</param>
</fill>
```
- **concat** : concaténation de plusieurs valeurs


```
<fill name="concat" target='bacula_dir_name'>
  <param type='eole' name='valeur1'>nom_machine</param>
  <param name='valeur2'>-dir</param>
</fill>
```
- **calc_multi_condition** : la valeur est déterminée en fonction d'une ou de plusieurs autres variables. Le résultat peut être une chaîne de caractères ou la valeur d'une autre variable multi ou non (si type='eole')


```

<auto name='calc_multi_condition' target='variable_calculée'>
  <param>oui</param>
  <param type='eole' name='condition_1'>activer_logiciel1</param>
  <param type='eole' name='condition_2'
  hidden='False'>activer_logiciel2</param>
  <param name='match'>oui</param>
  <param name='mismatch' type='eole'>variablemiss</param>
  <param
  name='default_mismatch'>valeur_si_variablemiss_disabled</param>
</auto>

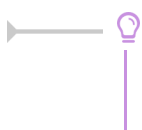
```

Il est possible d'utiliser des `calc_multi_condition` avec des variables non déclarées ou désactivées mais uniquement si toutes les variables testent la même condition.

A *contrario*, il est possible de spécifier une condition différente pour chacune des variables en en fournissant la liste dans la première balise `param` : `<param>['non', 'oui']</param>`. Dans ce cas, il faut exactement le bon nombre de variables et que celles-ci soient accessibles.

Validation et/ou liste de choix : `<check>`

La valeur renseignée pour une variable est validée par une fonction.



La déclaration de nombreuses validations peut être évitée en affectant un type adapté à chacune des variables.

L'attribut `name` correspond au nom de la fonction qui sera utilisée pour le calcul.

Les fonctions utilisées peuvent être :

- des fonctions natives de Tiramisu^[p.562] ;
- des fonctions déclarées dans le fichier `eosfunc.py` ;
- des fonctions ajoutées en tant que fonctions personnalisées (voir ci-dessous).

L'attribut de la balise `param` : `optional='True'` : indique que le paramètre sera ignoré si la variable associée n'existe pas. Cela permet de contourner les erreurs du type : Utilisation de la variable `<param var name>` non présente dans un calcul

L'attribut de la balise `param` : `hidden='False'` : indique que le paramètre sera ignoré si la variable possède des propriétés incompatibles avec le calcul (variable désactivée, variable obligatoire sans valeur, ...). Cela permet de contourner les erreurs du type : impossible d'effectuer le calcul, l'option `<target var name>` a les propriétés : `['disabled']` pour : `<param var name>`

La présence de l'attribut `level="warning"` indique que le test de validation n'est pas bloquant.

En cas d'échec de la validation un message d'alerte apparaîtra mais la valeur sera tout de même acceptée.

```

<check name="valid_ipnetmask" target="adresse_netmask_eth0"
level="warning">
  <param type='eole'>adresse_ip_eth0</param>
</check>

```

Les principales fonctions de validation disponibles sont les suivantes :

- *valid_enum* : la valeur doit être choisie parmi celles de la liste, si *checkval* est à False, l'utilisateur est autorisé à entrer la valeur de son choix (liste ouverte)

```

<check name="valid_enum" target="lettre">
  <param>['a','b','c']</param>
  <param name="checkval">False</param>
</check>

```

- *valid_regexp* : la valeur doit être conforme à une expression rationnelle

```

<check name='valid_regexp' target='code ent'>
  <param>^[A-Z][0-9]${</param>
  <param name='err_msg'>L'identifiant doit etre compose d'une lettre
et d'un chiffre</param>
</check>

```

- *valid_differ* : la valeur doit être différente de celle passée en paramètre

```

<check name='valid_differ' target='smb_workgroup'>
  <param type='eole' hidden='False'>smb_netbios_name</param>
</check>

```

- *valid_entier* : la valeur doit être un entier sur lequel on peut définir un minimum et/ou un maximum

```

<check name='valid_entier' target='nombre'>
  <param name='mini'>0</param>
  <param name='maxi'>50</param>
</check>

```

- *valid_networknetmask* : vérifie la cohérence entre une variable de type *network* et la variable de type *netmask* associée

```

<check name="valid_networknetmask" target="netmask_ssh_eth0">
  <param type='eole'>ip_ssh_eth0</param>
</check>

```

- *valid_ipnetmask* : vérifie la cohérence entre une variable de type *ip* et la variable de type *netmask* associée

```

<check name="valid_ipnetmask" target="adresse_netmask_eth0"
level="warning">
  <param type='eole'>adresse_ip_eth0</param>
</check>

```

- `valid_in_network` : vérifie la cohérence entre une variable de type `ip` et les variables de type `network` et `netmask` associées

```
<check name="valid_in_network" target="adresse_ip_gw">
  <param type='eole'>adresse_network_eth0</param>
  <param type='eole'>adresse_netmask_eth0</param>
</check>
```

Autre fonction de validation disponible mais non utilisée dans les dictionnaires livrés :

- `valid_broadcast`

Contrainte entre variables : `<condition>`

`disabled_if_in` et `disabled_if_not_in`

Les conditions `disabled_if_in` et `disabled_if_not_in` permettent :

- d'activer/désactiver une variable (`type='variable'`)
- d'activer/désactiver une famille (`type='family'`)
- d'activer/désactiver des services (`type='servicelist'`)
- d'activer/désactiver la templatisation de fichiers (`type='filelist'`)

en fonction d'un ensemble de conditions.

```
<condition name='disabled if not in' source='port_rpc'>
  <param>0</param>
  <param>7080</param>
  <target>ip_eth0</target>
  <target type='family' optional='True'>net</target>
  <target type='filelist'>ldap</target>
  <target type='servicelist'>ldap</target>
</condition>
```

Si l'attribut **optional** de la balise `target` vaut **'True'**, la cible sera ignorée si elle n'existe pas.

Cela permet de contourner les erreurs du type : `Variable <target var name> inexistante mais avec condition`

Si l'attribut **fallback** de la balise `condition` vaut **'True'**, les cibles seront automatiquement désactivées si le calcul de la condition est impossible (variable source inconnue ou désactivée).

Cela permet de contourner les erreurs du type : `Variable <src var name> inexistante mais utilisée dans une condition`

Son utilisation évite d'avoir à déclarer explicitement la variable source avec l'attribut `exists='False'` dans le dictionnaire courant.

```
<condition name='disabled if in' source='activer spamassassin'
fallback='True'>
  <param>non</param>
  <target type='variable'>exim spam score</target>
</condition>
```

! hidden_if_in et hidden_if_not_in

Les anciennes conditions *hidden_if_in* et *hidden_if_not_in* sont toujours supportées mais leur comportement est désormais calqué sur celui des *disabled_if_in* et *disabled_if_not_in* par lesquelles elles doivent être remplacées.

frozen_if_in et frozen_if_not_in

Les conditions *frozen_if_in* et *frozen_if_not_in* permettent de passer une variable en mode automatique (valeur non modifiable par l'utilisateur) en fonction d'un ensemble de conditions.

```
<condition name='frozen if not in' source='eth0 method'>
  <param>statique</param>
  <target type='variable'>adresse ip eth0</target>
  <target type='variable'>adresse netmask eth0</target>
  <target type='variable'>adresse ip gw</target>
</condition>
```

Ajout de fonctions personnalisées

Il est possible d'ajouter des librairies de fonctions personnalisées dans le répertoire `/usr/share/creole/funcs`.

Les librairies doivent posséder l'extension `.py` et contenir des fonctions python.

```
# -*- coding: utf-8 -*-
def to_iso(data):
    """ encode une chaine en ISO """
    try:
        return unicode(data, "UTF-8").encode("ISO-8859-1")
    except:
        return data
```



Si vous devez importer des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul

elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptibles d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

2.3.6. Afficher de l'aide

Il est possible d'afficher de l'aide dans l'interface :

- affichée au survol de l'onglet : **<family>** ;
- affichée au survol du libellé de la variable : **<variable>**.

L'ensemble des aides d'un dictionnaire est dans la balise **<help>**.

```
<help>
```

```
  <variable name='adresse_ip_eth0'>
```

```
    Adresse IP de la première carte réseau (ex: 10.21.5.1)
```

```
  </variable>
```

```
</help>
```

```

<help>
  <family name='messagerie'> Paramétrage du serveur de
  messagerie (MTA) Exim :
    - Paramétrage d'Exim selon 5 modèles ;
    - Paramétrage du domaine de messagerie suivant le modèle
  Exim ;
    - Paramétrage des réécritures d'adresses ;
    - Paramétrage des logs Exim ;
    - Paramétrage du relais des mails ;
    - Paramétrage d'activation de spamassassin ;
    - Paramétrage d'activation de Sympa.
  </family>
</help>

```

2.4. Le langage de template Creole

Les variables du dictionnaire Creole sont accessibles en les préfixant par la chaîne de caractères : `%%`.

Si dans le dictionnaire Creole :

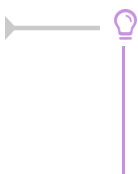
```
adresse_ip_eth0 vaut 192.168.170.1
```

Et qu'on a dans un template source le contenu suivant :

```
bla bla bla %%adresse_ip_eth0 bla bla bla
```

Après instanciation, le fichier cible contiendra :

```
bla bla bla 192.168.170.1 bla bla bla
```



Dans les cas où une variable est susceptible d'être confondue avec le texte qui l'entoure, il est possible d'encadrer son nom par des accolades :

```
%%{adresse_ip_eth0} est identique à %%adresse_ip_eth0.
```

2.4.1. Déclarations du langage Creole

Creole fournit un langage de template complet.

Il est possible de créer des boucles, des tests, de gérer les lignes optionnelles, de réaliser des inclusions répétées, ...

La déclaration de test : if

Syntaxe :

```
%if EXPRESSION |code if %else |code else %end if
```

Dans les tests il est possible d'utiliser les opérateurs du langage python : `==`, `!=`, `>`, `<`, `>=`, `<=`, `not`, `and`, `or`, ...

```

%if %%size > 500
  c'est grand .
%elif %%size >= 250
  c'est moyen
%else
  c'est petit
%end if

```

```

%if %%toto == 'yes' and ( %%titi != "" or %%tata not in
  ['a','b','c'] ) :
  la condition a été validée
%end if

```

La déclaration d'itération : for

Syntaxe :

```

%for %%iterateur in EXPRESSION
  CODE avec %%iterateur
%end for

```

La boucle `%for` est particulièrement intéressante lorsque l'on souhaite effectuer des traitements sur une **variable multi-valuée**.

```

%for %%i in range(4)
  itération %%i
%end for

%for %%valeur in %%variable multivaluee
  %%valeur
%end for

```

Pour des traitements simples, la fonction prédéfinie `%custom_join` (voir section suivante) peut avantageusement éviter la mise en place d'une boucle `%for`.

La notation pointée

Si une variable Creole est **multivaluée** et **maître** (*master d'un groupe de variable*) alors, il est possible de faire appel à ses variables **esclaves** à l'intérieur de la boucle `%for`.

Si `.netmask_admin_eth0` est esclave de `ip_admin_eth0` alors, il est possible d'appeler cette variable en notation pointée.

Par exemple : dans le dictionnaire Creole figurent les variables suivantes.

`ip_admin_eth0` est la variable maître et :

- `ip_admin_eth0 = ['1.1.1.1', '2.2.2.2']`
- `netmask_admin_eth0 = ['255.255.255.255', '255.255.255.255']`

Le template suivant :

```
%for %%ip admin in %%ip admin_eth0
%%ip admin/%%ip admin.netmask admin_eth0
%end for
```

donnera comme résultat :

`1.1.1.1/255.255.255.255`

`2.2.2.2/255.255.255.255`

Il est également possible aussi d'accéder à l'index (la position dans la liste) de la variable en cours de boucle :

```
%for %%idx, %%val in %%enumerate(%%ip admin_eth0)
L'index de %%val est : %%idx
%end for
```

Le template généré sera le suivant :

`l'index de : 1.1.1.1 est : 0`

`l'index de : 2.2.2.2 est : 1`

Il est également possible (mais déconseillé) d'utiliser une "notation par item" (notation entre crochets).

Par exemple pour accéder à l'item numéro 5 d'une variable, il faut écrire :

`variable[5]`

La variable doit être évidemment être **multivaluée** et comporter au minimum (*item+1*) valeurs.

`ip_admin_eth0 = ['1.1.1.1', '2.2.2.2', '3.3.3.3']`

et si un template a la forme suivante :

```
bla bla
%%ip_admin_eth0[2]
bla bla
```

alors l'instanciation du template donnera comme résultat :

`bla bla`

`3.3.3.3`

`bla bla`


⚠ .value et .index

Les attributs `.value` et `.index` ne sont plus supportés et ne doivent plus être utilisés dans les templates.

Les déclarations spéciales echo et set


L'instruction `%echo` permet de déclarer une chaîne de caractères afin que celle-ci apparaisse telle quelle dans le fichier cible.

Cela est utile lorsqu'il y a des caractères spéciaux dans le template source et, en particulier, les caractères `%` et `\` qui sont susceptibles d'être interprétés par le système de template.

—  `%echo "- deux barres obliques : \\\n- un pourcentage : %"`

L'utilisation de l'instruction `%echo` ne rend pas les templates très lisibles d'autant plus que, généralement, on souhaite intercaler des variables au milieu des caractères spéciaux.

En pratique, il est donc préférable de passer par des variables locales que l'on peut déclarer avec `%set`.

—  `%set %%slash='\\'`
`%set %%double_slash='\\\\'`
`%%double_slash%%machine%%{slash}partage`

Autres déclarations

La déclaration while

Syntaxe : `%while EXPR contenu`

`%end while`

Exemple :

`%while %someCondition('arg1', %%arg2)`

`The condition is true.`

`%end while`

La déclaration repeat

Syntaxe : `%repeat EXPR`

`%end repeat`

La déclaration unless

`%unless EXPR`

`%end unless`

peut être utile si une variable est dans le dictionnaire Creole pour "ne pas" exécuter une action : `%`

`%unless %%alive`

`do this`

`%end unless`

La syntaxe d'inclusion

il est possible d'inclure des fichiers à l'aide de la déclaration suivante :

`%include "includeFileName.txt"`

ou bien à partir du nom long du fichier à inclure (le nom de fichier étant ici renseigné dans une variable Creole :

```
%include source=%%myParseText
```

Effacement des retours chariots : slurp

Exemple d'utilisation :

```
%for %%i in range(15)
```

```
%%i-%slurp
```

```
%end for
```

donnera :

```
1-2-3-4-5-6...
```

sur une seule ligne (gobe les retours chariots)

remarquons que dans ce cas là, `slurp` n'est pas nécessaire et il est possible d'écrire le end sans sauter de ligne :

```
%for %%i in range(15)
```

```
%%i-%end for
```

exemple 2 :

```
%if %%dns nameservers != ['']
```

```
dns nameservers %slurp
```

```
%for %%name server in %%dns nameservers %%name server %slurp
```

```
%end for
```

```
%end if
```

```
#
```

générera :

```
dns nameserver toto titi #
```

2.4.2. Fonctions prédéfinies

Il est possible d'accéder à des fonctions prédéfinies, provenant du module : `eosfunc.py`.

Ces fonctions peuvent être utilisées dans un template de la manière suivante (exemple) :

```
[...] %%fonction predefinie(%%variable) [...]
```

Variable "optionnelle" : `is_defined`

Il peut arriver qu'on ne soit pas sûr que la variable que l'on souhaite tester soit définie dans les dictionnaires présents sur le module ou que la variable soit désactivée.

C'est le cas lorsque l'on veut traiter un cas particulier dans un template qui est commun à plusieurs modules.

Hors, si une variable est utilisée dans le template cible sans avoir été définie, le processus d'instanciation sera stoppé.

Pour tester si une variable est définie, il faut utiliser la fonction `%%is_defined`.

```

%if %%is_defined('ma_variable')
%%ma_variable
%else
la variable n'est pas définie
%end if

```

Contrairement à toutes les autres fonctions, *is_defined* nécessite comme argument le nom de la variable fourni sous forme d'une **chaîne de caractères**.

Si une variable non définie est placée dans un bloc qui n'est pas traité (conditionné par une fonction ou d'autres variables), ça n'est pas bloquant.



Dans de nombreux cas, la fonction *is_defined* peut avantageusement être remplacée par la fonction *getVar* à laquelle on aura pris soin d'indiquer une valeur par défaut à renvoyer en cas d'indisponibilité de la variable (voir ci-dessous).

Variable "vide" : *is_empty*

Il n'est pas toujours évident, en particulier lorsque l'on manipule des variables multi-valuées, de trouver le test adéquat afin de déterminer si une variable est vide.

Pour tester si une variable est vide, il est désormais recommandé d'utiliser la fonction *%%is_empty*.

```

%if not %%is_empty(%%ma_variable)
%%ma_variable[0]
%else
la variable est vide
%end if

```

Concaténation des éléments d'une liste : *custom_join*

La fonction *%%custom_join* permet de concaténer facilement les éléments d'une variable multi-valuée.

Cela permet d'éviter le recours à une boucle *%for* et l'utilisation de l'instruction *%slurp* qui est souvent source d'erreurs.

Il est possible de spécifier le séparateur à utiliser en le passant comme paramètre à la fonction.

En l'absence de ce paramètre, le séparateur utilisé est l'espace.

```

%%custom_join(%%ma_variable, ':')

```

Si *ma_variable* vaut ['a', 'b', 'c'], cela donnera :

```

a:b:c

```

Variable "dynamique" : getVar

Une variable dynamique prend comme nom (ou partie du nom) la valeur d'une autre variable.

```
%for %%interface in range(0, %%int(%%nombre interfaces))
L'interface      eth%%interface      a      pour      adresse
%%getVar('adresse ip eth'+str(%%interface))
%end for
```

La fonction *getVar* peut également être utilisée lorsque l'on n'est pas certain qu'une variable est disponible (inexistante ou désactivée) car il est possible de lui spécifier une valeur par défaut à renvoyer en cas d'indisponibilité.

```
%if %%getVar("activer mon logiciel", "non") == 'oui'
Activation du logiciel
%end if
```

Variable esclave "dynamique" : getattr

Lorsque le nom de la variable esclave doit être calculé, on peut utiliser `%%getattr` à la place de la notation pointée.

```
%set %%num='0'
%for %%ip ssh in %%getVar('ip ssh eth'+%%num)
SSH      est      autorisé      pour      %%ip_ssh/%%getattr(%%ip_ssh,
'netmask ssh eth'+%%num)
%end for
```

La fonction *getattr* peut également être utilisée lorsque l'on n'est pas certain qu'une variable esclave est disponible (inexistante ou désactivée) car il est possible de lui spécifier une valeur par défaut à renvoyer en cas d'indisponibilité.

```
%for %%iterator %%var master
%%getattr(%%iterator, 'var slave', 'default')
%end for
```

Autres fonctions

Fonctions de traitement des chaînes de caractères

- transformation d'une chaîne en majuscules : `%%upper(%%ma_chaine)` ;

- transformation d'une chaîne en minuscules : `%%lower(%%ma chaîne)` ;
- encodage d'une chaîne en ISO-8859-1 (au lieu d'UTF-8) : `%%to_iso(%%ma chaîne)` ;
- transformation d'un masque réseau (ex : 255.255.255.0) en classe d'adresse (ex : 24) : `%%calc_classe(%%mask)` ;

Fonctions de tests

- vérification que la variable est une adresse IP (et pas un nom DNS) : `%%is_ip(%%variable)` ;
- vérification de l'existence d'un fichier : `%%is_file(%%fichier)`.

Déclaration de fonctions locales

Pour un traitement local et répétitif, il peut être pratique de déclarer une fonction directement dans un template avec `%def` et `%end def`.

Cependant, la syntaxe à utiliser dans ces fonctions est assez complexe (on ne sait jamais quand mettre le caractère `%` !) et ce genre de déclaration ne facilite pas la lisibilité du template.

Les fonctions déclarées localement s'utilisent de la même façon que les fonctions déjà prédéfinies.



```
%def nombre_points(chaine)
.. %return chaine.count('.')
%end def
Il y a %%nombre_points(%%ma variable) points dans ma variable.
```

Ajout de fonctions personnalisées

Il est possible d'ajouter des bibliothèques de fonctions personnalisées dans le répertoire `/usr/share/creole/funcs`.

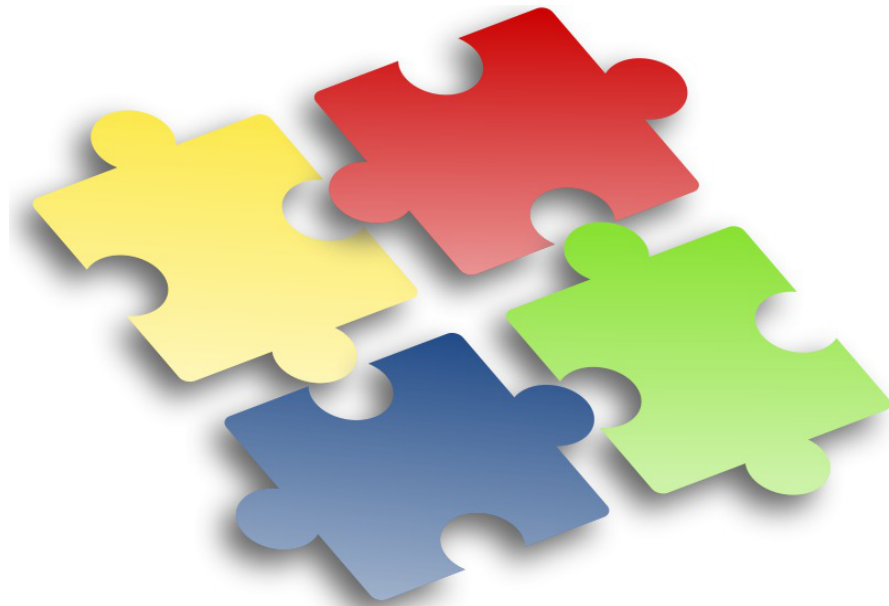
Les bibliothèques doivent posséder l'extension `.py` et contenir des fonctions python.



```
# -*- coding: utf-8 -*-
def to_iso(data):
    """ encode une chaîne en ISO """
    try:
        return unicode(data, "UTF-8").encode("ISO-8859-1")
    except:
        return data
```



Si vous devez importer des bibliothèques python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptibles d'intéresser d'autres utilisateurs. Elles peuvent faire l'objet d'une intégration dans le projet EOLE par l'équipe de développement.

Les avantages sont multiples :

- pérennité de vos modifications ;
- diffusion sur l'ensemble de vos serveurs ;
- optimisé par l'équipe ;
- diffuser à tous les utilisateurs.

Aussi n'hésitez pas à proposer votre travail. Pour se faire vous pouvez vous référer à la documentation pour apprendre comment contribuer.

2.4.3. Utilisation avancée

Modification des méta-caractères utilisés

Dans le cas où il y a trop de % dans le template, il est possible de changer carrément de méta-caractères, en ajoutant une section `compiler-settings` en en-tête du template.

Cette méthode est, par exemple, utilisée pour la génération du fichier de configuration du logiciel `eJabberd` qui est en déclaré en Erlang^[p.546].



Utilisation de @ et @@ à la place de % et %%

```
%compiler-settings
directiveStartToken = @
cheetahVarStartToken = @@
%end compiler-settings
```

Utilisation de `creole_client`

Les fonctionnalités de *creole_client* sont utilisables directement dans les templates.

Il est par exemple possible de lister toutes les variables et leurs valeurs :

```
%for %%var, %%value in %%creole client.get creole().items()
. %%var : %%value .
%end for
```

Donnera le résultat suivant (notez que le nom des variables esclaves est précédé de celui de la variable maître associée) :

```
ssl_organization_name : Ministere Education Nationale (MENESR) .
https_port : .
check_passwd_min_len_two_type : 9 .
container_ip_proxy : 127.0.0.1 .
nom_cache_pere_zone.options_cache_pere_zone : [] .
nom_cache_pere : [] .
ignore_expect_100 :
off_eolessa_adresse : 192.168.230.205 .
activer_dhcprelay : non
[...]
```

Plus généralement, il est possible d'accéder à toutes les informations décrites dans les dictionnaires comme celles concernant les conteneurs, les services et les tâches programmées.

Liste des conteneurs :

```
%for %%container in %%creole client.get containers()
* %%container['name']
%end for
```

Liste des services actifs :

```
%for %%srv in %%creole client.get services()
%if %%srv.has_key('activate')
* %%srv['name']
%end if
%end for
%set %%sched = %%creole client.get('schedule.schedule')
```

Les tâches programmées sont exécutées à
 %%{sched['hour']}h%%{sched['minute']}

2.4.4. Exemple

► Templatiser un nouveau fichier

Nous voulons templatiser le fichier `toto.conf` à l'aide des mécanismes Creole afin de rajouter l'`adresse_ip_eth0` (variable existante) ainsi que l'adresse de l'établissement (nouvelle variable).

- Ajouter un dictionnaire local

Dans `/usr/share/eole/creole/dicos/local/`
ajouter un fichier `.xml`

- Ajouter votre fichier template

Notre fichier `toto.conf` sera placé dans `/usr/share/eole/creole/distrib/`

Il faut ajouter les variables à l'aide de la syntaxe Creole.

exemple : l'adresse est `%%adresse_ip_eth0` et l'adresse est `%%adresse_etablissement`

- Entrer l'adresse de l'établissement

- Aller dans l'interface de configuration du module
- Dans l'onglet `Perso` renseigner l'adresse de l'établissement
- Enregistrer

- Reconfigurer

Le mécanisme de configuration a écrit votre fichier `/etc/toto.conf` avec les variables.

🗨 Commentaires généraux

Les variantes Zéphir

Cette procédure décrit comment ajouter des spécifications locales.

Dans le cadre d'un développement massif, le module Zéphir propose un mécanisme de variantes semblable.

Instancier un template avec CreoleCat

CreoleLint et CreoleCat ^[p.461]

2.5. Les scripts Creole

Creole fournit également un ensemble de scripts destinés à faciliter l'administration du serveur :

- `CreoleLint` permettant de faire des vérifications sur un dico ou sur un template ;
- `CreoleCat` permettant d'instancier un seul template indépendamment des commandes `instance` et `reconfigure` ;
- `CreoleGet` et `CreoleSet` permettant de lire et de modifier la valeur d'une variable Creole.
- `CreoleRun` et `CreoleService` permettant de lancer des commandes système et de gérer les services sur les modules EOLE, y compris à l'intérieur des conteneurs^[p.543] ;
- `CreoleLock` permettant de placer, enlever ou vérifier les verrous Creole.

2.5.1. CreoleLint et CreoleCat

`CreoleLint` et `CreoleCat` sont des utilitaires permettant de faciliter les tests sur les dictionnaires et les templates :

- `CreoleLint` permet de valider la syntaxe des dictionnaires et des templates ;
- `CreoleCat` permet d'instancier un seul template indépendamment des commandes `instance` et `reconfigure` .

Vérifier les dictionnaires et templates avec CreoleLint

La commande `CreoleLint` permet de valider la syntaxe des dictionnaires et des templates.

L'outil effectue une série de tests dans le but de détecter des erreurs dans la déclaration et l'utilisation des variables.

Sur un module installé, il est possible de lancer l'application sans option particulière :

```
# CreoleLint
```

Cette commande permet également :

- de valider un seul template avec l'option `-t` : `CreoleLint -t hostname`
- de ne lancer qu'un seul des tests lint avec l'option `-n nomDuTest` : `CreoleLint -n valid dtd`
- de ne lancer que la validation des dictionnaires avec l'option `-d` : `CreoleLint -d`

Les tests lint disponibles sont les suivants :

- `valid dtd` : validation syntaxique des dictionnaires ;
- `tabs in dicos` : recherche de tabulation dans les dictionnaires ;
- `hidden if in dicos` : recherche des conditions dépréciées `hidden if in` et `hidden if not in` ;
- `obligatoire in dicos` : recherche du validateur déprécié `obligatoire` ;
- `valid slave value` : recherche les variables esclaves avec une liste en valeur défaut (EOLE >= 2.5.2) ;
- `wrong dicos name` : validation du nom des dictionnaires ;
- `valid var label` : vérification des libellés des variables ;
- `valid separator label` : vérification des libellés des séparateurs ;
- `valid help label` : vérification des libellés de l'aide en ligne ;
- `activation var without help` : vérification des variables d'activation sans balise d'aide (EOLE >= 2.5.2) ;
- `family without help` : vérification des familles sans balise d'aide ;
- `family without icon` : vérification des familles sans icône spécifique ;
- `old fw file` : recherche des anciens fichiers eole-firewall ;
- `valid parse tmpl` : validation de tous les templates.



L'option `-l` permet de choisir le niveau des messages (info, warning ou error).

La commande `CreoleLint` suivie du paramètre `-h` permet d'obtenir de l'aide. Un manuel est également disponible :

```
# man CreoleLint
```

Instancier un template avec CreoleCat

La commande `CreoleCat` permet d'instancier un seul template indépendamment des commandes `instance` et `reconfigure`.

Cette commande permet :

- d'instancier un seule template existant sur le module en utilisant la ou les destinations déclarées dans le dictionnaire :

```
# CreoleCat -t hostname
```

- d'instancier un template existant sur le module en redirigeant le résultat dans un fichier spécifique :

```
# CreoleCat -t hostname -o /tmp/hostname.txt
```

- d'instancier un fichier template spécifique en redirigeant le résultat dans un fichier spécifique :

```
# CreoleCat -s /tmp/test.tpl -o /tmp/test.txt
```

- d'instancier un fichier template spécifique en affichant le résultat sur la console (*EOLE* >= 2.5.2) :

```
# CreoleCat -s /tmp/test.tpl
```



L'option `-l` permet de choisir le niveau des messages (info, warning ou error).

Les options `-v` (`--verbose`) ou `-d` (`--debug`) permettent de connaître le détail des opérations réalisées par le programme.

La commande `CreoleCat` suivie du paramètre `-h` permet d'obtenir de l'aide.



```
root@scribe:~# CreoleCat -d -t sympa.auth.conf
Instanciation du fichier '/etc/sympa/auth.conf' depuis
'/var/lib/creole/sympa.auth.conf'
Copy template: '/usr/share/eole/creole/distrib/sympa.auth.conf' ->
'/var/lib/creole'
Cheetah processing: '/var/lib/creole/sympa.auth.conf' ->
'/etc/sympa/auth.conf'
Changing properties: chown sympa:sympa /etc/sympa/auth.conf
Changing properties: chmod 0644 /etc/sympa/auth.conf
```



Dans le cas d'un template renommé, c'est le nom du template (défini dans l'attribut *source*) qu'il faut utiliser.

2.5.2. CreoleGet et CreoleSet

`CreoleGet` et `CreoleSet` sont des utilitaires permettant de lire et de modifier la valeur d'une variable

Creole.

Récupérer la valeur d'une variable avec CreoleGet

CreoleGet est un utilitaire très pratique pour récupérer la valeur d'une variable Creole.

Il s'utilise tout simplement en lui donnant le nom de la variable souhaitée en argument :

```
CreoleGet mavariable
```



La commande `CreoleGet --list` permet d'obtenir la liste complète des variables.

La commande `CreoleGet` supporte l'autocomplétion à partir de la version 2.5.2 d'EOLE.



```
# CreoleGet --list | grep release
eole release="2.4.2"
```

CreoleGet permet également de récupérer la liste des groupes de conteneurs :

```
CreoleGet --groups
```

Sur un serveur en mode non conteneur, cette commande renvoie uniquement `root`.



Dans le cas où l'on n'est pas certain que la variable soit disponible (variable inconnue ou désactivée), il est possible d'indiquer une valeur par défaut à renvoyer en cas d'erreur :

```
CreoleGet activer_logiciel non
```

Dans le cas contraire, une erreur pourra apparaître.



Pour accéder à une variable esclave, il faut connaître la variable maître :

```
CreoleGet lamaster.lesclave
```



Les valeurs multiples sont séparées par un saut de ligne (`\n`) :

```
root@eolebase:~# CreoleGet serveur maj
eole.ac-dijon.fr
ftp.crihan.fr
```



L'option `-h` ou `--help` ou la commande `man CreoleGet` permettent d'obtenir de l'aide.

Lister les services gérés par Creole avec CreoleGet

La commande suivante permet d'obtenir la liste des services qui sont gérés par CreoleService sur le module :

```
CreoleGet .containers.services |grep \.name=
```

```
1 root@eolebase:~# CreoleGet .containers.services|grep \.name=
2 service0.name="networking"
3 service1.name="cron"
4 service10.name="exim4"
5 service11.name="eoleflask"
6 service12.name="nginx"
7 service13.name="ead3"
8 service14.name="genconfig"
9 service15.name="bastion"
10 service16.name="z_stats"
11 service2.name="rng-tools"
12 service3.name="ntp"
13 service4.name="nut-server"
14 service5.name="salt-api"
15 service6.name="salt-master"
16 service7.name="salt-minion"
17 service8.name="ead-server"
18 service9.name="ead-web"
19 root@eolebase:~#
```

Modifier la valeur d'une variable avec CreoleSet

CreoleSet est un utilitaire très pratique pour modifier la valeur d'une variable Creole.

Il s'utilise tout simplement en lui donnant le nom de la variable et sa valeur en argument :

```
CreoleSet mon_ip 10.10.10.55
```



L'option `--default` permet de réinitialiser une variable à sa valeur par défaut :

```
CreoleSet --default serveur_ntp
```

La commande `CreoleSet` supporte l'autocomplétion à partir de la version 2.5.2 d'EOLE.



Les valeurs multiples doivent être séparées par un saut de ligne (`\n`) :

```
root@eolebase:~# CreoleSet serveur_maj "eole.ac-toto.fr
ftp.crihan.fr"
```



La modification d'une variable possédant des dépendances fortes avec d'autres variables ou familles ne sera généralement pas possible car cela cassera la consistance des données.



L'option `-h` ou `--help` ou la commande `man CreoleSet` permettent d'obtenir de l'aide.

2.5.3. CreoleRun et CreoleService

CreoleRun et **CreoleService** sont des utilitaires permettant de lancer des commandes système et de

gérer les services sur les modules EOLE, y compris à l'intérieur des conteneurs^[p.543].

Exécuter une commande avec CreoleRun

CreoleRun est un utilitaire très pratique pour exécuter une commande dans un conteneur (depuis le maître).

Le script s'utilise de la façon suivante :

```
CreoleRun "<command>" <container>
```



Si le mot clé `all` est utilisé à la place du nom du conteneur, alors la commande sera lancée dans tous les conteneurs (rien ne sera exécuté en mode non conteneur).

La commande gère un troisième argument qui si il vaut `yes` exécutera la commande uniquement si l'environnement est un conteneur (ie : si l'utilisation de SSH est nécessaire).

Gérer les services avec CreoleService

CreoleService permet de gérer les services déclarés dans les dictionnaires Creole.

Le script s'utilise de la façon suivante :

```
CreoleService [-c <container>] <service> <action>
```

Les actions possible sont :

- *configure* : configure le lancement automatique du service au démarrage du serveur en fonction de la configuration Creole du serveur ;
- *enable* : active le lancement automatique du service au démarrage du serveur ;
- *disable* : désactive le lancement automatique du service au démarrage du serveur ;
- *apply* : démarre ou arrête le service en fonction de la configuration Creole du serveur ;
- *start* : démarre le service ;
- *stop* : arrête le service ;
- *restart* : redémarre le service ;
- *reload* : recharge le service ;
- *status* : vérifie l'état du service.



L'option, `-f` (ou `--force`) permet de forcer le démarrage ou redémarrage d'un service même si celui-ci est désactivé au niveau de la configuration Creole du serveur.

2.5.4. CreoleLock

CreoleLock est un utilitaire permettant de placer, enlever ou vérifier les verrous Creole.

Il peut gérer deux niveaux (level) de verrouillage distincts.

La plupart des outils de base EOLE utilisent de verrous de niveau "système".

Verrou "normal"

Ce type de verrou permet d'éviter qu'une même application soit exécutée deux fois en parallèle. Il s'agit donc d'un verrou isolé.

En mode normal (`--level=normal`), les fichiers lock sont écrits dans le répertoire `/var/lock/eole` et il est possible d'exécuter plusieurs applications différentes en même temps tant qu'elles ne posent pas un lock ayant le même nom.

Verrou "système"

Contrairement au mode normal, les verrous "système" (`--level=system`) sont exclusifs. Cela permet d'éviter que deux applications concurrentes sont exécutées en même temps. Par exemple, il ne faut pas qu'un reconfigure soit exécuté en même temps qu'une sauvegarde : ces deux procédures utilisent des verrous "système".

Dans ce mode, mes fichiers lock sont écrits dans le sous-répertoire `/var/lock/eole/eole-system`.

Nom d'un fichier lock

Le nom d'un fichier lock est de la forme `prefixe.suffixe`, avec :

- un préfixe invariant fourni par le programme (généralement le nom de l'application) ;
- un suffixe représentant le PID^[p.558] de l'application.

Poser un verrou avec CreoleLock

Pour poser un verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock acquire --name toto
```

Si un verrou existe déjà, la commande affichera un message d'erreur et ne renverra pas le code `0`.

Vérifier la présence d'un verrou avec CreoleLock

Pour vérifier la présence du verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock is_locked --name toto
```


Cette commande retournera le code `0` si le verrou est présent.

Supprimer un verrou avec CreoleLock

Pour supprimer un verrou nommé *toto*, la commande à taper est la suivante :

```
CreoleLock release --name toto
```

Cette commande retournera le code `0` en cas de succès.

 Seul le programme (y compris la console si la commande est lancée en console) qui a posé le verrou a le droit de le supprimer.

API python

La librairie `pyeole.lock` permet de gérer les verrous Creole directement en python.

Elle fournit notamment les fonctions `acquire`, `is_locked` et `release`.



L'option `-h` permet d'afficher les paramètres de la commande `CreoleLock` :

```
# CreoleLock -h
usage: /usr/bin/CreoleLock [acquire|release|is_locked]
[options|--help]
```

2.5.5. Indications pour la programmation

Certaines fonctions ont été intégrées sur les modules afin que les scripts puissent être écrits en tenant compte des spécificités des modules EOLE, que sont les variables et le mode conteneur.

Programmation bash

- obtenir la valeur d'une variable (variables de conteneur comprises) :

```
CreoleGet <variable_name>
```

- obtenir la valeur d'une variable ou une valeur prédéfinie en cas d'erreur :

```
CreoleGet <variable name> <default value>
```

- modifier la valeur d'une variable :

```
CreoleSet <variable_name> <new value>
```

- exécution d'une commande dans un conteneur :

```
CreoleRun "<command>" <container>
```

- redémarrage d'un service dans un conteneur :

```
CreoleService -c <container> <service name> restart
```



Petit script bash

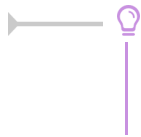
```
1#!/bin/bash
2echo "mon adresse IP est $(CreoleGet adresse_ip_eth0)"
3echo "La base Ldap est stockée dans $(CreoleGet container_path_annuaire)
4/var/lib/ldap"
4echo "Le conteneur annuaire a l'adresse : $(CreoleGet
5container_ip_annuaire)"
5CreoleRun "ls /var/lib/ldap" annuaire
6CreoleService slapd restart -c annuaire
```



Script compatible EOLE 2.3/2.4/2.5

```
1#!/bin/bash
2if [ -f /usr/bin/ParseDico ];then
3  RunCmd=RunCmd
4  . /usr/bin/ParseDico
5  . /etc/eole/containers.conf
6  . /usr/share/eole/FonctionsEoleNg
7else
8  RunCmd=CreoleRun
9  # récupération des variables nécessaires
10 container_path_web=$(CreoleGet container_path_web)
11 nom_machine=$(CreoleGet nom_machine)
12fi
```

```
13 touch ${container_path_web}/etc/${nom_machine}.conf
14 $RunCmd "chown www-data /etc/${nom_machine}.conf" web
```



CreoleGet permet également d'accéder aux variables "extra" :

```
CreoleGet schedule.schedule.hour
```

Programmation Python

- obtenir la valeur d'une variable (variables de conteneur comprises) :

```
from creole.client import CreoleClient
CreoleClient().get_creole('<variable name>')
```

- obtenir la valeur d'une variable ou une valeur prédéfinie en cas d'erreur :

```
from creole.client import CreoleClient
CreoleClient().get_creole('<variable name>', '<default value>')
```

- obtenir l'ensemble des variables dans un dictionnaire :

```
from creole.client import CreoleClient
dico = CreoleClient().get_creole()
adresse_ip_eth0 = dico['adresse_ip_eth0']
# cas particulier: pour les variables 'esclaves' d'un groupe, préfixer
par la variable maître
sso_first_base_ldap = dico['eolessso_ldap.eolessso_base_ldap'][0]
```

- obtenir la valeur d'une esclave correspond à une master :

```
master = client.get_creole('master')
slave = client.get_creole('slave')
for idx, var in enumerate(master):
    print "master : {0}, slave : {1}".format(var, slave[idx])
```

- exécution d'une commande dans un conteneur (affichage à l'écran) :

```
from pyeole.process import system code
system code([<commande sous forme de liste>], container='<conteneur>')
```

- exécution d'une commande dans un conteneur (sorties dans un tuple) :

```
from pyeole.process import system out
system out([<commande sous forme de liste>], container='<conteneur>')
```

- redémarrage d'un service dans un conteneur (avec affichage à l'écran)

```
from pyeole.log import init logging
from pyeole.service import manage_service
init_logging(level='info')
manage_service('restart', '<service>', '<conteneur>')
```



Petit script Python

```
1 #!/usr/bin/env python
```

```

2# -*- coding: UTF-8 -*-
3from creole.client import CreoleClient
4creole_client = CreoleClient()
5print "mon adresse IP est {0}".format(creole_client.get_creole(
    'adresse_ip_eth0'))
6print "La base Ldap est stockée dans {0}/var/lib/ldap".format(
    creole_client.get_creole('container_path_annuaire'))
7print "Le conteneur annuaire a l'adresse : {0}".format(creole_client.
    get_creole('container_ip_annuaire'))
8from pyeole.process import system_code
9system_code(['ls', '/var/lib/ldap'], container='annuaire')
10from pyeole.log import init_logging
11from pyeole.service import manage_service
12init_logging(level='info')
13manage_service('restart', 'slapd', 'annuaire')

```

Script compatible EOLE 2.3/2.4/2.5

```

1#!/usr/bin/env python
2# -*- coding: UTF-8 -*-
3from pyeole.process import system_code
4try:
5    from creole import parsedico
6    from creole.eosfunc import load_container_var
7    variables = parsedico.parse_dico()
8    variables.update(load_container_var())
9except:
10    from creole.client import CreoleClient
11    variables = CreoleClient().get_creole()
12fichier = open('{0}/etc/{1}.conf'.format(variables['container_path_web'],
    variables['nom_machine']), 'a')
13fichier.close()
14system_code(['chown', 'www-data', '/etc/{0}.conf'.format(variables[
    'nom_machine'])], container='web')

```

Modification de variables

Du fait des dépendances entre variables certaines modifications ne sont pas réalisables avec la commande `CreoleSet`.

C'est notamment le cas pour les variables groupées qui doivent impérativement posséder le même nombre d'éléments au moment de l'enregistrement ou pour des variables de type `oui/non` qui permettent de débloquer des variables à caractère obligatoire.

L'exemple qui suit montre comment activer l'autorisation des connexion SSH pour un couple adresse IP / masque de sous-réseau.

```

1#!/usr/bin/env python
2# -*- coding: UTF-8 -*-
3from creole.loader import creole_loader, config_save_values
4config = creole_loader(rw=True)
5config.creole.interface_0.ssh_eth0 = u'oui'
6config.creole.interface_0.ip_ssh_eth0.ip_ssh_eth0[0] = u'192.168.1.1'
7config.creole.interface_0.ip_ssh_eth0.netmask_ssh_eth0[0] =
    u'255.255.255.255'
8config_save_values(config, 'creole')

```

Pour accéder à une variable esclave, il faut connaître le nom de sa famille et celui de la

variable maître associée.

Les valeurs doivent être saisies en Unicode^[p.563], qui en python se traduit par l'ajout du caractère **u** devant la chaîne de caractères.

Cette obligation ne concerne pas les variables de type `number` qui attendent un nombre entier :

```
config.creole.systeme.bash_tmout = 3600
```

2.6. Ajout de script exécuté à l'instance ou au reconfigure

Il est parfois nécessaire d'ajouter un script qui sera exécuté à l'instanciation ou au reconfigure du module. EOLE met en place des mécanismes permettant d'exécuter des scripts avant ou après l'instanciation ou la reconfiguration.

Ces scripts doivent être dans l'un des répertoires suivants :

- `/usr/share/eole/preservice` : exécution avant l'arrêt des services ;
- `/usr/share/eole/pretemplate` : exécution avant la templatisation des fichiers ;
- `/usr/share/eole/posttemplate` : exécution entre la templatisation des fichiers et le redémarrage des services ;
- `/usr/share/eole/postservice` : exécution après le redémarrage des services.



Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.



L'ensemble de ces scripts se jouent de façon alphanumérique.

Les scripts fournis par EOLE sont préfixés par des chiffres et un tiret :

```
1 root@scribe:/usr/share/eole/preservice# ll
2 total 28
3 drwxr-xr-x  2 root root 4096 sept. 28 10:24 ./
4 drwxr-xr-x 29 root root 4096 sept. 28 10:24 ../
5 -rwxr-xr-x  1 root root  387 sept. 28 09:16 00-anetwork*
6 -rwxr-xr-x  1 root root  464 sept.  7 15:08 00-bareoswebui*
7 -rwxr-xr-x  1 root root  500 juin 26 2015 00-save-sid*
8 -rwxr-xr-x  1 root root  702 sept.  7 15:36 00-web*
9 -rwxr-xr-x  1 root root  235 sept. 28 09:16 99-ifupdown*
10 root@scribe:/usr/share/eole/preservice#
```

Le type d'appel (instance ou reconfigure) est envoyé au script sous la forme d'un argument :

```
1 #!/bin/bash
2 if [ "$1" == "instance" ]; then
3     echo "ce code n'est exécuté qu'à l'instance"
4 elif [ "$1" = "reconfigure" ] ;then
5     echo "ce code n'est exécuté qu'au reconfigure"
```

6 fi



Si le script quitte avec un autre code de retour que `0`, l'instance ou le reconfigure s'arrête immédiatement.

Il est donc préférable que le script soit de la forme :

```
1 #!/bin/bash
2 # <<< SCRIPT >>>
3 exit 0
```

Voir aussi...

Indications pour la programmation [p.468]

2.7. Ajout d'un test diagnose

Les scripts diagnose personnalisés peuvent être placés dans le répertoire `/usr/share/eole/diagnose`

Ces fichiers sont généralement écrits en bash et permettent de se connecter au service voulu pour tester l'état de celui-ci.



Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.

Un certain nombre de fonctions sont disponibles dans les bibliothèques EOLE, mais vous pouvez créer vos propres fonctions pour vos besoins spécifiques.

Généralement, le test affiche *Ok* si le service est fonctionnel et *Erreur* en cas de problème.

Voici quelques fonctions disponibles dans la bibliothèque `/usr/lib/eole/diagnose.sh` :

- *TestIP* et *TestIP2* : testent si une IP répond au ping ;
- *TestARP* : teste si l'adresse MAC associée à une IP répond ;
- *TestService* : teste la connexion TCP sur une IP et un numéro de port ;
- *TestUDP* : teste si un port est ouvert localement en UDP ;
- *TestPid* : teste la présence du PID d'une application locale ;
- *TestDns* : teste la résolution de nom sur un serveur DNS particulier ;
- *TestNTP* : teste un serveur NTP ;
- *TestHTTPage* : teste l'ouverture d'une session HTTP ;
- *TestWeb* : teste le téléchargement d'une page HTTP ;
- *TestCerts* : teste des valeurs du certificat TLS/SSL.



```
#!/bin/bash
# utilisation des fonctions EOLE
. /usr/lib/eole/diagnose.sh
# teste si le serveur web local est fonctionnel
# en vérifiant la variable Creole "activer apache"
# et en utilisant la fonction TestHTTPage
if [ $(CreoleGet activer apache) = "oui" ];then
    TestHTTPage "Web local" "http://$(CreoleGet
adresse ip eth0)/"
fi
```

Voir aussi...

Indications pour la programmation [p.468]

2.8. Gestion des noyaux Linux

Noyau Linux utilisé

Les modules EOLE 2.5 utilisent par défaut le noyau le plus récent de la distribution Ubuntu.

Si le noyau utilisé est différent du noyau conseillé, les commandes `instance` et `reconfigure` vous proposeront de redémarrer le serveur ou le redémarreront automatiquement en fonction de la situation.



Sur les dernières versions d'Ubuntu 14.04, le noyau utilisé est `linux-image-generic-lts-vivid`.

Pour plus d'informations, consulter la page : <http://doc.ubuntu-fr.org/ltsenablementstack>



La commande `uname -r` permet de connaître le noyau en cours d'utilisation.

En-tête du noyau

Plusieurs outils nécessitent la présence des en-têtes du noyau (headers) sur le serveur.

Les en-têtes du noyau courant sont pré-installés sur les modules.



Les en-têtes des anciens noyaux sont purgés automatiquement lorsque le noyau associé est supprimé.

Purge des anciens noyaux

Tous les noyaux sont purgés à l' `instance` et au `reconfigure` à l'exception :

- du noyau en cours d'utilisation ;
- du noyau précédent le noyau utilisé ;
- du noyau le plus récent installé ;
- d'un éventuel noyau personnalisé (voir ci-dessous).

Personnalisation du noyau

Dans certains cas (prise en charge de matériels, tests,...), il peut être nécessaire d'utiliser un autre noyau (compilé ou non par vos soins) que le noyau courant.

Créer le fichier `/usr/share/eole/noyau/local` avec le numéro de version du noyau à utiliser permet de forcer l'utilisation d'un noyau antérieur ou d'un noyau compilé.



Pour utiliser le noyau **linux-image-4.4.0-112-generic** il faut ajouter le numéro de version du noyau 4.4.0-112 dans le fichier `/usr/share/eole/noyau/local` :

```
# echo 4.4.0-112 > /usr/share/eole/noyau/local
```

Mettre à jour Grub :

```
# update-grub
```

Pour réutiliser le noyau courant il faut supprimer le fichier `/usr/share/eole/noyau/local` et mettre à jour Grub à l'aide de la commande `update-grub` .



Cette facilité est à utiliser à titre exceptionnel.

Aucun signalement lié à l'utilisation d'un noyau différent de celui préconisé par EOLE ne sera pris en compte.

2.9. Gestion des tâches planifiées eole-schedule

Présentation

Sur les modules EOLE, les tâches planifiées (comme par exemple les mises à jour, les sauvegardes, la purge de certaines informations, l'exportation de l'annuaire, des bases de données et des quotas disque ou encore les mises à des listes noires pour le filtrage proxy) sont gérées par `eole-schedule` .

Contrairement à l'utilisation de cron, `eole-schedule` permet de maîtriser les tâches planifiées même si la sauvegarde est activée.

En version 2.5, `eole-schedule` est géré depuis Tiramisu^[p.562].

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est cron^[p.544] qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bareos^[p.541] qui lance `eole-schedule` .

Il existe 4 types de tâches planifiées :

- les tâches journalières : *daily* ;
- les tâches hebdomadaires : *weekly* ;
- les tâches mensuelles : *monthly* ;
- les tâches uniques : *once*.

Ces tâches sont découpées en *pre*-sauvegarde et *post*-sauvegarde.

Si aucune sauvegarde n'est prévue : le *cron* lance *pre* puis *post* à l'heure qui a été tirée au hasard.

Si une sauvegarde est prévue : Bareos lance *pre* avant la sauvegarde et *post* à l'heure qui a été tirée au hasard (sauf si celle-ci est prévue avant la sauvegarde ou si la sauvegarde n'est pas terminée, dans ce cas les tâches *post* sont exécutées après la sauvegarde).

Les sauvegardes "post" sont obligatoirement marquées en `Full` même si cela ne correspond à rien (pas de sauvegarde, exécution des scripts uniquement). Elles sont réalisées à l'heure qui a été tirée au hasard.

Par contre, les sauvegardes "pre" sont bien lancées à l'heure des sauvegardes définie par l'administrateur.

Différences par rapport à Schedule 2.3

La liste des scripts à activer est décrite dans un fichier XML^[p.564] (dictionnaire). Ce système permet de mettre en place des valeurs par défaut. Ainsi, l'activation ou la désactivation d'un script n'est plus réalisée à l'installation du paquet ce qui est à la fois plus simple et plus sûr.

La description n'est plus dans le script. Elle est directement dans le fichier XML.

Les scripts *pre/post* sont maintenant mélangés dans le répertoire `/usr/share/eole/schedule/scripts`.

Gestion des tâches planifiées

Lister ce qui est programmé

```
# manage_schedule -l
```

Ajouter une tâche planifiée

```
# manage_schedule -a daily -s majblacklist -m post
```

Supprimer une tâche planifiée

```
# manage_schedule -d majblacklist
```

Appliquer la configuration (génération des liens symboliques)

```
# manage_schedule --apply
```



L'ajout et la suppression n'appliquent pas la configuration. Il faut :

- soit l'appliquer à la main (`manage_schedule --apply`) ;
- soit effectuer un `reconfigure` .

Gestion des tâches uniques (once)

Les scripts lancés pour une nuit sont gérés totalement différemment et les informations associées ne sont pas conservées dans Tiramisu.

⚡ Ajouter une tâche planifiée unique

```
# manage_schedule -a once -s majauto -m post
```

⚡ Supprimer une tâche planifiée unique

```
# manage_schedule -d once -s majauto -m post
```

La prise en compte des tâches uniques est instantanée.
L'appel à la méthode `--apply` n'est donc pas nécessaire.

Exemple de fichier XML

Les fichiers XML décrivant les tâches planifiées ont un format proche de celui des dictionnaires^[p.544] Creole.

Exemple du fichier : `/usr/share/eole/creole/extra/schedule/01_majauto.xml`

```
1 <?xml version="1.0" encoding="utf-8"?>
2
3 <creole>
4   <variables>
5     <family name='majauto'>
6       <variable name="description" type="string"><value>Mise à jour
7 du serveur</value></variable>
8       <variable name="day" type="schedule"><value>weekly
9 </value></variable>
10      <variable name="mode" type="schedulemod"><value>post
11 </value></variable>
12    </family>
13  </variables>
14 </creole>
```

Gestion des mises à jour avec Creole et eole-schedule

La mise à jour hebdomadaire consiste en un script `eole-schedule` nommé `majauto`. Il est configuré pour être lancé une fois par semaine (`weekly`) après la sauvegarde (`post`).

Sa gestion dans les scripts python est facilitée par la librairie `creole.maj`.

⚡ Savoir quand est prévue la mise à jour

```
# python -c "from creole import maj; print maj.get_maj_day()"
```

⚡ Activer/désactiver la mise à jour hebdomadaire

Activation de la mise à jour hebdomadaire :

```
# manage_schedule -a weekly -s majauto -m post
```

ou :

```
# python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
# manage_schedule -d majauto
```

ou :

```
# python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

Forcer l'exécution des tâches planifiées

Il est possible de forcer l'exécution des tâches planifiées avec la commande `/usr/share/eole/schedule/schedule cron`.

```
1 root@amon:~# /usr/share/eole/schedule/schedule cron
2 Démarrage de pre schedule daily
3 pre schedule daily accompli
4 Démarrage de post schedule daily
5 . Test de http://eole.orion.education.fr/maj/blacklists => Ok
6 Téléchargement des bases
7 Rien à faire pour blacklists.tar.gz
8 Rien à faire pour le fichier weighted
9 eole-schedule - run-parts: executing
  /usr/share/eole/schedule/daily/post/majblacklist daily
10 post schedule daily accompli
11 Démarrage de pre schedule once
12 pre schedule once accompli
13 Démarrage de post schedule once
14 post schedule once accompli
15 root@amon:~#
```

Lire les journaux de l'exécution des tâches planifiées

Les journaux de l'exécution des tâches planifiées se trouvent dans le répertoire `/var/log/rsyslog/local/eole-schedule/`.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
1 root@eole:~# manage_schedule -l
2 Tâches planifiées EOLE :
3 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
4 - après sauvegarde
5 + Mise à jour du serveur (majauto)
6 root@eole:~#
```



Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
1 root@eole:~# rm /etc/eole/extra/schedule/config.eol
2 rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
3 root@eole:~# manage_schedule -l
```

```

4 Tâches planifiées EOLE :
5 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
6 - après sauvegarde
7 + Mise à jour du serveur (majauto)
8 root@eole:~#

```

2.10. Gestion du pare-feu eole-firewall

Introduction

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper^[p.562] et l'activation de modules noyau.

`eole-firewall` ne gère que des "autorisations", des règles en INPUT sur un port déterminé.

Les flux sont bloqués en entrée depuis l'extérieur. En interne (entre le maître et les conteneurs et entre conteneurs) il n'y a pas de restriction.

Si un conteneur possède une seconde interface (variable du type : *adresse_ip_link*), les flux sont bloqués en entrée.

eole-firewall avec ERA

Pour les modules avec ERA, Amon et AmonEcole, les règles d'`eole-firewall` ne s'appliquent pas. Seules les règles ERA du modèle choisi s'appliquent.

eole-firewall sans ERA

`eole-firewall` ne gère que des "autorisations", des règles en INPUT sur un port déterminé. Ces autorisations peuvent être affinées avec des "restrictions".

Les flux sont bloqués en entrée depuis l'extérieur. En interne (entre le maître et les conteneurs et entre conteneurs) il n'y a pas de restriction.

Si un conteneur possède une seconde interface (variable du type : *adresse_ip_link*), les flux sont bloqués en entrée.

Pour gérer les "autorisations" il faut créer des dictionnaires personnalisés. Pour cela il faut se référer à la rubrique traitant des dictionnaires dans la personnalisation du module à l'aide de Creole.

Pour des cas particuliers et exceptionnels il est possible de décrire des règles de pare-feu dans des

fichiers placés dans le répertoire `/usr/share/eole/bastion/data/`.

Ces fichiers de règles doivent respecter les critères suivants :

- commencer par `#!/bin/bash` ;
- être exécutable ;
- ne pas contenir d'extension ;
- son code retour doit être 0.



La création de règles par cette méthode doit rester exceptionnelle.



Fichier `/usr/share/eole/bastion/data/40-icmp_static_rules` sur le module Scribe

```
1 #!/bin/bash
2 /sbin/iptables -A eth0-root -p icmp --icmp-type destination-unreachable -j
  ACCEPT
3 /sbin/iptables -A eth0-root -p icmp --icmp-type network-unreachable -j
  ACCEPT
4 /sbin/iptables -A eth0-root -p icmp --icmp-type source-quench -j ACCEPT
5 /sbin/iptables -A eth0-root -p icmp --icmp-type fragmentation-needed -j
  ACCEPT
6 /sbin/iptables -A eth0-root -p icmp --icmp-type time-exceeded -j ACCEPT
7 /sbin/iptables -A eth0-root -p icmp --icmp-type parameter-problem -j
  ACCEPT
8 /sbin/iptables -A eth0-root -p icmp --icmp-type echo-reply -j ACCEPT
9 /sbin/iptables -A eth0-root -p icmp --icmp-type echo-request -j ACCEPT
```

Créer des dictionnaires personnalisés pour gérer les règles du pare-feu eole-firewall

Utiliser des fichiers templates, paquets, services et règles de pare-feu [p.430]

Chapitre 10

Résolution de problèmes

Sur les modules EOLE quelques outils sont disponibles pour aider à la résolution de problèmes. L'outil de diagnostic `diagnose` et la lecture des logs permettent l'identification de la plupart des problèmes. L'outil de génération de rapport aidera à rassembler des informations en vue d'une analyse.

1. Problèmes à la mise en œuvre

Erreur lors du partitionnement

L'outil de partitionnement affiche la question suivante : "partitionner le disques > Nom de volume déjà utilisé" :

Cela indique juste que des partitions LVM^[p.552] (issues d'une installation antérieure) ont été détectées sur le disque dur.

Vous pouvez cliquer sur "oui" pour continuer l'installation.

Erreur lors de l'installation des paquets

L'installateur s'arrête ou affiche un message d'erreur lors de l'étape : "choisir et installer des logiciels" :

C'est peut-être uniquement parce que le CD-ROM utilisé est mal gravé ou abîmé.

Pour connaître la nature exacte du problème, vous pouvez réaliser les manipulations suivantes :

- `ctrl F2` (affiche la console de débogage)
- `nano /var/log/syslog` (édite le fichier de log)
- `ctrl W` , `ctrl V` (va à la fin du fichier)

puis utilisez la *flèche du haut* pour remonter dans le fichier jusqu'à trouver les lignes contenant des erreurs.

La présence de l'expression "I/O Error" indique qu'il y a eu des erreurs de lecture, dans ce cas, il faut graver un nouveau CD.

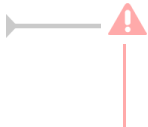
Erreur lors de la création des conteneurs

Il est possible de suivre le processus d'installation des conteneurs dans le journal d'activité

`/var/log/isolation.log`

Problèmes lors de la configuration

Pour détecter les problèmes de configuration, il faut utiliser la commande `diagnose`.



Avant de chercher un éventuel problème, il est recommandé de lancer une reconfiguration du module à l'aide de la commande `reconfigure`.

2. Problèmes à l'exploitation

La commande diagnose

Lors de la mise en œuvre d'un module, un outil de diagnostic permet de valider que la configuration est correcte et fonctionnelle.

la commande `diagnose` valide donc les points clés de la configuration des services.

L'état des services est indiqué clairement par un code couleur vert/rouge.

```
Last login: Wed Jan 27 11:15:15 2016 from 192.168.230.146
root@horus:~# diagnose

*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Cartes réseau
eth0: Link detected: yes

*** Interfaces
horus:      192.168.0.25 => Ok

*** Services distants
.   Passerelle 192.168.0.1 => Ok
.   DNS 192.168.232.2 => Ok
.   NTP pool.ntp.org => Ok
.   Accès distant => Ok

Sur l'interface réseau eth0
.   SSH => Ok
.   EAD Server => Ok
.   EAD Web => Ok

*** Pare-feu
.   Génération des règles => Ok (22:42:30 26/01/16)
.   Pare-feu => Ok

*** Validité du certificat
.   eole.crt => Ok
```

Les points importants de l'état du serveur sont vérifiés :

- la version du module installé ;
- la connectique réseau et sa configuration ;
- l'état des principaux services.

S'il apparaît que certaines sections sont en erreur, il faut revoir la configuration dans l'interface dédiée et reconfigurer le serveur.

Le diagnose, mode étendu

Si le diagnostic précédent n'est pas suffisant pour comprendre d'éventuelles erreurs, un mode étendu avec l'option `-L` permet d'obtenir plus d'informations :

```
# diagnose -L
```

```

*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Configuration matérielle du serveur

Type :
Standard PC (i440FX + PIIX, 1996) - QEMU

Processeur :
  QEMU Virtual CPU version 2.0.0

Carte réseau :
  Virtio

Disques :
  DVD reader

Appuyez sur Entrée pour continuer ...

```

Le premier écran détaille l'aspect matériel du serveur.

```

Sys. de fichiers      Taille Utilisé Dispo Uti% Monté sur
udev                  486M   4,0K  486M   1% /dev
tmpfs                  100M   5,3M   95M   6% /run
/dev/mapper/horus--vg-root 3,4G   2,0G   1,2G  64% /
none                   4,0K     0   4,0K   0% /sys/fs/cgroup
none                   5,0M     0   5,0M   0% /run/lock
none                   497M     0   497M   0% /run/shm
none                   100M     0   100M   0% /run/user
/dev/mapper/horus--vg-home  18G    75M   17G   1% /home
/dev/mapper/horus--vg-tmp  1,8G   3,4M   1,7G   1% /tmp
/dev/vda2              688M   69M   570M  11% /boot
/dev/mapper/horus--vg-var  14G   603M   13G   5% /var

Inode disques :
Sys. de fichiers      Inœuds IUtil. ILibre IUtil% Monté sur
udev                  122K   476   121K   1% /dev
tmpfs                  125K   470   124K   1% /run
/dev/mapper/horus--vg-root 220K  116K  105K  53% /
none                   125K     2   125K   1% /sys/fs/cgroup
none                   125K     5   125K   1% /run/lock
none                   125K     1   125K   1% /run/shm
none                   125K     2   125K   1% /run/user
/dev/mapper/horus--vg-home  1,2M    90   1,2M   1% /home
/dev/mapper/horus--vg-tmp  120K   152   119K   1% /tmp
/dev/vda2              45K    304   45K   1% /boot
/dev/mapper/horus--vg-var  888K   5,9K  883K   1% /var

Appuyez sur Entrée pour continuer ...

```

Le deuxième écran détaille les disques reconnus, leur partitionnement, et le taux d'occupation des partitions affichées.

***** Paquets installés**

Noyau linux : Linux 4.2.0-25-generic

Vérification des paquets installés : OK

Vérification des mises à jour...

Mise à jour le jeudi 28 janvier 2016 11:04:10

*** horus 2.5.2 (0000000A) ***

Configuration du dépôt Ubuntu avec la source test-eole.ac-dijon.fr

Configuration du dépôt EOLE avec la source test-eole.ac-dijon.fr

Action update pour root

Action list-upgrade pour root

0 nouveau, 11 mis à jour, 0 à enlever

Paquets à mettre à jour :

```

apache2 (2.4.7-1ubuntu4.9) (root)
apache2-bin (2.4.7-1ubuntu4.9) (root)
apache2-data (2.4.7-1ubuntu4.9) (root)
apt (1.0.1ubuntu2.11) (root)
apt-transport-https (1.0.1ubuntu2.11) (root)
apt-utils (1.0.1ubuntu2.11) (root)
curl (7.35.0-1ubuntu2.6) (root)
libapt-inst1.5 (1.0.1ubuntu2.11) (root)
libapt-pkg4.12 (1.0.1ubuntu2.11) (root)
libcurl3 (7.35.0-1ubuntu2.6) (root)
libcurl3-gnutls (7.35.0-1ubuntu2.6) (root)

```

Appuyez sur Entrée pour continuer ...

L'écran suivant affiche ensuite le nom du module, sa version, ainsi que l'état des mises à jour. Si comme ici, il en existe, il est conseillé de les installer pour vérifier si le problème rencontré est corrigé dans les nouveaux paquets.

Dernières actions Creole

```

2016-01-26T22:44:15.856124+01:00 horus.ac-test.lan zephir: INSTANCE => FIN : Configuration terminée
2016-01-28T11:04:10.400319+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T11:05:02.602131+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : 11 paquets à mettre à jour
2016-01-28T11:28:10.989084+01:00 horus.ac-test.lan zephir: MAJ => INIT : Début en devel
2016-01-28T11:28:12.422925+01:00 horus.ac-test.lan zephir: MAJ => MSG : Mise à jour en devel forcée par l'utilisateur
2016-01-28T11:30:44.113397+01:00 horus.ac-test.lan zephir: MAJ => FIN : 30 paquets mis à jour en devel
2016-01-28T11:30:44.117192+01:00 horus.ac-test.lan zephir: MAJ => MSG : Reconfiguration du serveur à planifier
2016-01-28T11:36:41.877030+01:00 horus.ac-test.lan zephir: RECONFIGURE => INIT : Début de configuration
2016-01-28T11:40:04.902914+01:00 horus.ac-test.lan zephir: RECONFIGURE => FIN : Configuration terminée
2016-01-28T11:56:25.998182+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T11:57:23.416706+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer
2016-01-28T14:37:48.275191+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T14:38:27.340008+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer
2016-01-28T14:42:33.432867+01:00 horus.ac-test.lan zephir: QUERY-MAJ => INIT : Début
2016-01-28T14:43:13.145804+01:00 horus.ac-test.lan zephir: QUERY-MAJ => FIN : Aucun paquet à installer

```

Appuyez sur Entrée pour continuer ...

Le dernier écran affiche la liste des dernières actions Creole réalisées sur le serveur (mise à jour, reconfigure, Query-Auto, etc.).

```

Last login: Wed Jan 27 11:15:15 2016 from 192.168.230.146
root@horus:~# diagnose

*** Test du module horus version 2.5.2 (horus 0000000A) ***

*** Cartes réseau
eth0: Link detected: yes

*** Interfaces
horus:      192.168.0.25 => Ok

*** Services distants
.   Passerelle 192.168.0.1 => Ok
.   DNS 192.168.232.2 => Ok
.   NTP pool.ntp.org => Ok
.   Accès distant => Ok

Sur l'interface réseau eth0
.   SSH => Ok
.   EAD Server => Ok
.   EAD Web => Ok

*** Pare-feu
.   Génération des règles => Ok (22:42:30 26/01/16)
.   Pare-feu => Ok

*** Validité du certificat
.   eole.crt => Ok

```

Enfin, on retrouve l'affichage standard de l'outil avec l'état des services.

Les journaux système

Lorsque des problèmes surviennent en exploitation, les journaux système (ou journaux de bord, fichiers de log, fichiers de journalisation) constituent une source incomparable d'informations. Ils contiennent la succession des événements ou des actions qui sont survenus sur un système informatique donné.

Ces fichiers sont au format texte, et sont généralement stockés en local dans le répertoire `/var/log`

L'outil de log utilisé par EOLE est `rsyslogd` et la configuration se trouve dans `/etc/rsyslog.conf`

Ce fichier définit les messages à enregistrer et le fichier cible, cela permet éventuellement de filtrer (ou répartir) les messages, par leur source et leur degré d'importance.

La plupart des logiciels disposent d'un paramètre "*log level*" permettant de régler la verbosité des informations journalisées.

En cas de problème, il est conseillé d'augmenter le niveau de journalisation du logiciel incriminé.

Les fichiers les plus couramment utilisés sont :

- `/var/log/messages` : contient tous les messages d'ordre général concernant la plupart des services et démons.
- `/var/log/syslog` : est plus complet que `/var/log/messages`, il contient tous les messages, hormis les connexions des utilisateurs.
- `/var/log/auth` : contient les connexions des utilisateurs.
- `/var/log/mail.log` : contient les envois et réception de mails.
- `/var/log/cron` : fichier log du service cron (planificateur système).



Il est possible de lire le contenu d'un fichier avec la commande `less` :

```
# less /var/log/syslog
```

Pour n'afficher que les dernières ligne d'un fichier, utiliser la commande `tail` :

```
# tail -n 50 /var/log/syslog
```


La commande `tail` permet également d'afficher en temps réelle les nouvelles entrées dans un fichier. Pour cela, ajouter l'option `-f` :

```
# tail -f /var/log/syslog
```

Accéder aux partitions du module depuis un Live Linux

Lorsqu'on a recours à un live CD ou USB, il n'est pas possible d'accéder directement aux partitions.

```
1 # mkdir /media/partition
2 # mount /dev/sda2 /media/partition
3 mount: type inconnu de système de fichiers 'LVM2_member'
```

Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
1 # vgscan
2 Reading all physical volumes. This may take a while...
3 Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
1 # vgchange -a y eolebase-vg
2 4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
1 # ll /dev/mapper/
2 total 0
3 drwxr-xr-x  2 root root    160 févr.  8 11:53 ./
4 drwxr-xr-x 19 root root   4460 févr.  8 11:53 ../
5 crw-----  1 root root  10, 236 févr.  8 11:53 control
6 lrwxrwxrwx  1 root root     7 févr.  8 11:53 eolebase--vg-home ->
  ../dm-4
7 lrwxrwxrwx  1 root root     7 févr.  8 11:53 eolebase--vg-root ->
  ../dm-0
8 lrwxrwxrwx  1 root root     7 févr.  8 11:53 eolebase--vg-swap_1 ->
  ../dm-1
9 lrwxrwxrwx  1 root root     7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
10 lrwxrwxrwx  1 root root     7 févr.  8 11:53 eolebase--vg-var -> ../dm-3
```

OU

```
1 # lvdisplay
2 --- Logical volume ---
3 LV Path                /dev/eolebase-vg/swap_1
4 LV Name                 swap_1
5 VG Name                 eolebase-vg
6 LV UUID                 0047WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
7 LV Write Access        read/write
8 LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
9 LV Status               available
10 # open                  2
11 LV Size                 1,09 GiB
12 Current LE              280
13 Segments                1
14 Allocation              inherit
15 Read ahead sectors     auto
16 - currently set to     256
17 Block device            252:1
```

18 [...]

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

3. Trouver de l'information

Plusieurs sources d'information sont disponibles pour répondre de manière autonome aux questions que l'on se pose :

- équipes d'assistance académiques ;
- les documentations EOLE ;
- la FAQ des documentations ;
- aide sur les commandes ;
- les archives des listes de discussion ;
- les listes de discussion ;
- la documentation externe ;
- les wikis de la forge.

La documentation officielle EOLE

La documentation officielle EOLE est accessible depuis la page du module sur le site internet du projet EOLE dans la rubrique Documentation ou directement à l'adresse <http://eole.ac-dijon.fr/documentations/>

La documentation EOLE est publiée en HTML et en PDF, elle est divisée sous forme :

- de documentation par module ;
- de documentation transversale et thématique.

Les questions les plus fréquentes - FAQ

Les problèmes rencontrés fréquemment ont souvent déjà trouvés une solution, des FAQ sont proposées dans la documentation de chaque module, elles recensent les interrogations les plus courantes. Ces rubriques évoluent régulièrement.



Une documentation thématique dédiée réunit les FAQ de tous les modules.

Aide sur les commandes

N'oubliez pas de consulter les pages de manuel installées sur le système avec la commande `man` :

```
# man nomDeLaCommande
```



```
# man man
```

```
# man setfacl (q pour sortir)
```

Sur un serveur les différents commandes offrent de l'aide avec l'option `--help` :

```
# nomDeLaCommand --help
```



```
# man --help
```

Certains logiciels libres manquent encore de documentation ou ne sont pas documentés du tout. Dans ce cas, pensez à consulter le contenu de leur fichier de configuration. Certains commentaires donnent des indications voire remplacent une documentation externe.

Commandes utiles sous Linux

Voici quelques commandes qui peuvent vous aider à vous faire une idée plus précise de l'état du serveur. Voici une liste de quelques commandes utiles :

- `top -d1` (q pour sortir, h pour aide)
- `mc` (éditeur de texte)
- `links` (navigateur texte que l'on peut exécuter via SSH directement sur le serveur)
- `tcpdump` (examineur de paquets)
- `nmap` (scanneur de ports)
- `tcpcheck` (testeur de port)

Les archives des listes de discussion

Les listes de discussion du projet sont archivées et mettent à disposition un moteur de recherche.

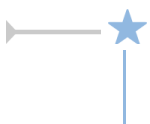
Rares sont les fils de discussion (threads ou topics) évoquant un questionnement ou un problème sans évoquer la réponse ou la solution.

<http://eole.orion.education.fr/listes/lists>

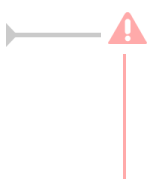
Les listes de discussion

Les listes de diffusions sont un espace d'échange qui est source d'aide et d'informations. Chaque module EOLE possède sa propre liste. Pour échanger sur les listes il faut préalablement être inscrit.

<http://eole.orion.education.fr/listes>



Avant de poser une question sur une liste de discussion ou avant d'y répondre il faut s'assurer qu'elle n'a pas déjà trouvée réponse.

- 
- Gardez toujours à l'esprit que beaucoup de gens vont lire ce que vous écrivez : ne postez jamais d'informations confidentielles sur une liste de diffusion.
 - N'activez pas de répondeur sur une liste de discussion ;-).

- N'écrivez pas en privée aux membres de l'équipe, préférez exposer remarques publiquement ;
- Ne modifiez pas le champ "Répondre à" afin que les réponses soient envoyés à la liste et non à votre adresse personnel. Consultez cet explication pour Thunderbird : <http://blogzinet.free.fr/index.php?2005/02/16/536-thunderbird-repondre-a-recurrent-dans-c>
- Pour écrire à la liste n'utilisez pas un ancien message pour en modifier le sujet, le fil de discussion serait endommagé, il faut ouvrir un nouveau fil de discussion avec un sujet parlant.
- La Nétiquette décrit un certains nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.
<http://fr.wikipedia.org/wiki/Nétiquette>

Documentation externe

La plupart des logiciels fournis avec les modules EOLE sont largement utilisés en dehors de l'Éducation nationale.

Des documentations plus spécifiques à l'utilisation de la plupart des logiciels utilisés sont disponibles sur Internet (ex. <http://doc.ubuntu-fr.org/cups>).

Dans le cas de la mise en place d'une configuration avancée de l'un des logiciels, il est tout à fait indiqué de consulter sa documentation officielle (ex. <http://www.cups.org/documentation.php>).



Les documentations externes peuvent faire état de commandes systèmes à exécuter.

Il n'est pas forcément judicieux de suivre ces instructions car les modules EOLE disposent d'un système d'auto-configuration (Creole^[p.544]) qui risque d'écraser vos modifications ou même de ne plus fonctionner correctement.



En cas de doute, n'hésitez pas à demander à l'équipe.

Les wikis de la forge

Les wiki de la forge peuvent contenir des notes diverses comme des documentations techniques, des pistes de réflexion et des informations sur la diffusion, l'évolution et le développement des logiciels et des modules.



Les notes les plus importantes sont régulièrement intégrées à la documentation.

Quelques références

- Site officiel du Pôle de Compétences Logiciels Libres : <http://pcll.ac-dijon.fr> ;
- Site web officiel de la distribution : <http://eole.orion.education.fr> ;
- Le blog : <http://pcll.ac-dijon.fr/eole/blog/> ;

- Les listes de discussion : <http://eole.orion.education.fr/listes> [<http://eole.orion.education.fr/>] ;
- La forge : <http://dev-eole.ac-dijon.fr/> ;
- Les annonces
 - Sur la forge : <http://dev-eole.ac-dijon.fr/news>
 - Flux Atom : <http://dev-eole.ac-dijon.fr/news.atom>
- La documentation : <http://eole.ac-dijon.fr/documentations/>

4. Demander de l'aide / Signaler un problème

Les problèmes rencontrés ont fréquemment déjà trouvés une solution, il existe diverses sources d'informations à disposition :

- les documentations ;
- la FAQ des documentations ;
- les archives des listes de diffusion.

Avant de demander de l'aide

- Avez-vous consulté la documentation du projet ?
- Avez-vous consulté la FAQ ?
- Avez-vous consulté les archives des listes de discussion ?
- Avez-vous effectué un reconfigure sur le serveur ?
- Avez-vous répondu oui aux 4 questions listées ci-dessus ?

Collecte d'informations

Il faut collecter des informations permettant la compréhension et le contexte du problème rencontré. Par contre il faut trouver un juste milieu entre trop peu d'information et trop d'information.

Voici des informations qui selon le contexte vont être utile à la description du problème :

- La version précise du module utilisé ainsi que le niveau des mises à jour (stable, candidat, développement) ;
- Résultat de la commande de diagnostic `diagnose -L` pour un diagnostic étendu) ;
- Les différentes étapes permettant de reproduire le problème rencontré ;
- Les extraits de fichiers de journalisation ;
- Toutes informations connexes ayant un rapport avec votre problème (les adaptations locales, patch, dictionnaires additionnels, logiciels supplémentaires, etc.) ;
- Joindre des copier/coller et/ou des captures d'écran ;
- Générer un rapport avec la commande `gen_rpt` ;

La commande `gen_rpt` permet de générer une archive incluant :

- les fichiers de configuration EOLE du serveur ;
- le diagnostic étendu ;
- la liste des processus en cours sur le serveur ;
- les règles de pare-feu appliquées sur le système ;
- l'historique des commandes système ;
- la liste des paquets installés ;
- plusieurs fichiers de journalisation ;
- le rapport d'extraction (Module Scribe) ;
- le rapport de sauvegarde (Module Scribe/Horus/Eclair).

L'archive nommée `<module>-<numéro-etab>.tar.gz` est enregistrée dans le répertoire courant au lancement de la commande.



Si une passerelle de courrier a été définie sur le serveur, l'archive pourra être directement envoyée à l'équipe EOLE (merci de ne pas en abuser) ou à l'adresse de votre choix.



Dans la collecte d'informations peuvent se trouver des informations sensibles, attention à leur diffusion sur des médias publics : IRC, liste de discussion, demande sur la forge...

Formuler une demande d'aide

Lorsque vous posez une question, gardez à l'esprit que ceux qui la liront n'auront que votre message pour se représenter votre demande. Essayez de donner une description précise du problème. Les informations précédemment collectées vous aideront à fournir des détails.



- Écrivez dans un langage clair et concis, pas de langage SMS, soignez la grammaire et l'orthographe, cela permet d'éviter certains quiproquos ;
- Soyez précis et explicite sur le contexte du problème ou de l'aide demandée.
Ne dites pas *Quand je clique sur la disquette ça marche pas.* mais dites plutôt *Dans LibreOffice, quand je clique sur l'icône en forme de disquette j'obtiens l'erreur suivante : "copiez le texte intégral de l'erreur ou faites une capture d'écran" ;*
- Décrivez les symptômes du problème, évitez les suppositions ou les interprétations.
Préférez dire *Le fond d'écran ne s'affiche pas* plutôt que *Un firewall doit sûrement bloquer mon fond d'écran ;*
- Décrivez la chronologie des événements et/ou des symptômes de votre problème ;
- Décrivez le but à atteindre, le comportement attendu ;
- Le volume d'information n'a rien avoir avec la précision des informations attendues ;
- Ne dites jamais que votre problème est URGENT même si c'est le cas, personne n'aime se sentir contraint par le caractère urgent de la demande ;
- Ne posez votre question qu'une seule fois, même si la réponse se fait attendre. Il est par

exemple possible que la réponse nécessite des recherches et donc du temps.



La Nétiquette décrit un certains nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

<http://fr.wikipedia.org/wiki/Nétiquette>



Vous trouverez le développement intégral des différents points évoqués ci-dessus dans le document présent à cette adresse : <http://www.gnurou.org/writing/smartquestionsfr>

Les listes de discussion

Les listes de diffusions sont un espace d'échange qui est source d'aide et d'informations. Chaque module EOLE possède sa propre liste. Pour échanger sur les listes il faut préalablement être inscrit.

<http://eole.orion.education.fr/listes>

La liste de diffusion est un bon endroit pour poser votre question. Cependant la quantité des messages et leur contenu demande une certaine organisation de tous afin que les échanges restent cohérents, efficaces et cordiaux.



Voici quelques points à suivre lors de l'envoi d'un message :

- Utilisez un sujet le plus explicite et le plus adapté possible ;
- Envoyez vos messages dans des formats lisibles par tous les clients de messagerie : le texte brut est très apprécié, le HTML et les images animées beaucoup moins ;
- Si votre courrier comporte une énorme pièce jointe, préférez utiliser la compression ou l'utilisation d'un dépôt de fichiers externe ;
- Ne postez jamais d'informations confidentielles sur une liste de diffusion ;
- Nouveau sujet est équivalent à un nouveau fil de discussion. N'utilisez pas la fonction **Répondre à** un ancien message en en modifiant l'objet pour lancer un nouveau sujet. Créez vraiment un **Nouveau message**. Sinon, en classant par fils de discussion votre message sera confondu avec un autre sujet et risque de ne pas être vu.
- Laissez l'historique de la conversation dans votre réponse, pour ceux qui vous aide et qui n'ont pas votre problème en tête cela constitue un aide-mémoire et permet de se replacer rapidement dans le contexte.
- N'activez pas de répondeur (message d'absence) sur une liste de discussion ;
- N'écrivez pas en privée aux membres de l'équipe, préférez exposer vos remarques publiquement pour le bénéfice de tous ;
- Ne modifiez pas le champ "Répondre à" afin que les réponses soient envoyés à la liste et non à votre adresse personnel. Consultez cet explication pour Thunderbird : <http://blogzinet.free.fr/index.php?2005/02/16/536-thunderbird-repondre-a-recurrent-dans-c>
- Pour écrire à la liste n'utilisez pas un ancien message pour en modifier le sujet, le fil de

discussion serait endommagé, il faut ouvrir un nouveau fil de discussion avec un sujet parlant.

- La Nétiquette décrit un certains nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

<http://fr.wikipedia.org/wiki/Nétiquette>

Discussion relayée par Internet

Internet Relay Chat ou IRC sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion, mais peut aussi être utilisé pour de la communication de un à un. Un canal de discussion `#eole` se trouve sur freenode.net.



- Il est demandé de mettre son nom réel dans les paramètres du client. ;
- La Nétiquette décrit un certains nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

<http://fr.wikipedia.org/wiki/Nétiquette>

Faire un signalement sur la forge

Il est possible de faire des remonter aux travers des différents listes de discussion du projet EOLE mais pour une bonne prise en charge il vous sera demandé de saisir une demande dans la forge.

Il est possible de demander des évolutions, de l'aide ou de signaler des erreurs directement sur la forge à l'adresse suivante : <http://dev-eole.ac-dijon.fr/projects/modules-eole/issues/new>



Pour se faire il est recommandé de regarder avant si la demande n'existe pas déjà à l'adresse :

<http://dev-eole.ac-dijon.fr/projects/modules-eole/issues>



Lorsque vous renseignez un signalement, veillez à suivre ces quelques recommandations :

- Soyez clairs, donnez des explications claires de façon à ce que d'autres puissent reproduire le dysfonctionnement ;
- Séparez clairement les faits des suppositions ;
- S'il n'ont rien à voir, faites un signalement par dysfonctionnement rencontré ;
- Si vous avez des informations susceptibles d'aider à résoudre le problème ou si vous avez la solution, n'hésitez pas à les joindre à votre demande.

Quelques références

- Site officiel du Pôle de Compétences Logiciels Libres : <http://pcll.ac-dijon.fr> ;
- Site web officiel de la distribution : <http://eole.orion.education.fr> ;

- Le blog : <http://pcll.ac-dijon.fr/eole/blog/> ;
- Les listes de discussion : <http://eole.orion.education.fr/listes> [<http://eole.orion.education.fr/>] ;
- La forge : <http://dev-eole.ac-dijon.fr/> ;
- Les annonces
 - Sur la forge : <http://dev-eole.ac-dijon.fr/news>
 - Flux Atom : <http://dev-eole.ac-dijon.fr/news.atom>
- La documentation : <http://eole.ac-dijon.fr/documentations/>

5. Contribuer au projet EOLE

Il est possible de contribuer au projet EOLE de différentes manières. Les contributions seront intégrées au fur et à mesure en fonction de ce qui est prioritaire dans les cycles de publication.

Les contribution peuvent aller du partage de l'astuce la plus simple jusqu'à des développements plus complexes en passant par la relecture, l'enrichissement de la documentation, l'écriture de tutoriels, le test des versions candidates, l'écriture d'un rapport de bug, la revue de code, la réponse aux demandes d'aide sur les listes de discussions...

Vous pouvez manifester votre désir de contribuer à des développements il faut s'inscrire et le signaler sur la liste dev-eole@listeseole.ac-dijon.fr.

Si votre contribution est complexe, une documentation expliquant son fonctionnement est toujours la bienvenue. Soit directement dans votre message, soit sous forme d'un fichier indépendant.

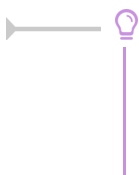
Pour permettre aux utilisateurs d'accéder à votre contribution vous pouvez :

- demander son intégration et sa diffusion directement par l'équipe ;
- fournir des ressources que nous pourrons intégrer à la documentation ou à l'espace contribution.

Demander des évolutions ou signaler des erreurs

Il est possible de faire des remonter aux travers des différents listes de discussion du projet EOLE mais pour une bonne prise en charge il vous sera demandé de saisir une demande dans la forge.

Il est possible de demander des évolutions, de l'aide ou de signaler des erreurs directement sur la forge à l'adresse suivante : <http://dev-eole.ac-dijon.fr/projects/modules-eole/issues/new>



Pour se faire il est recommandé de regarder avant si la demande n'existe pas déjà à l'adresse :

<http://dev-eole.ac-dijon.fr/projects/modules-eole/issues>

Chapitre 11

Documentations techniques

1. Les dépôts EOLE

Architecture des dépôts EOLE

Un miroir des dépôts Ubuntu est disponible à l'adresse suivante :

<http://eole.ac-dijon.fr/ubuntu>

Le miroir propose pour chaque version de la distribution Ubuntu plusieurs catégories de paquets (les fichiers *.deb) :

- **<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^[p.549] 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>

2. Gestion des journaux systèmes sur EOLE

Architecture cible

Dans un souci d'harmonisation et de centralisation de l'information, la quasi totalité des logs est désormais rassemblée sur le maître dans le répertoire : `/var/log/rsyslog/local`

Par défaut, les logs des services installés dans un conteneur et qui utilisent rsyslog sont remontés sur le maître (fichiers de configuration : `/etc/rsyslog.d/99-aggregation.conf` dans les conteneurs).

L'utilisation de rsyslog laisse la possibilité de réaliser une configuration spécifique pour chaque service.

C'est déjà le cas pour `squid` par exemple (template : `80-squid.conf`).

Le répertoire `/var/log/rsyslog/remote` est quant à lui prévu pour recevoir les journaux de serveurs distants dans le cas de la mise en place d'un serveur de log centralisé (l'équivalent du serveur 2.2 : [ZéphirLog](#)).

Exceptions connues

A l'heure actuelle, plusieurs services ne sont pas directement pris en charge par rsyslog :

- les logs de `Samba` sont toujours stockés dans le répertoire : `/var/log/samba` et ne sont pas remontés sur le maître ;
- les logs de `ltsp-cluster-lbagent` et `ltsp-cluster-lbserver` sont toujours stockés dans le répertoire `/var/log` et ne sont pas remontés sur le maître.

Un lien symbolique permet toutefois d'accéder directement aux fichiers depuis le maître.

Rotation des logs

Les programmes dont les logs sont centralisés sur le maître doivent avoir une configuration *logrotate* avec les chemins adaptés sur le maître.



Si le service est susceptible d'être installé dans un conteneur et qu'il doit être redémarré, il faut penser à adapter les commandes.

La commande `CreoleService` permet, par exemple, de gérer un service y compris si celui-ci est dans un conteneur :

```
CreoleService -c <conteneur> <service> restart
```

3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation

Note technique de l'ANSSI du 02/12/2013

Cette note technique détaille les prérequis nécessaires à la mise en œuvre d'un système de journalisation efficace et sécurisé et présente les bonnes pratiques permettant de bâtir une architecture de gestion de journaux pérenne, quelle que soit la nature du système d'information.

<http://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-jour>



Note technique de l'ANSSI du 02/12/2013 au format PDF :

http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf

3.1. Contexte juridique

Aspects juridiques et réglementaires

- les éléments juridiques doivent être pris en compte dans le cadre de la conception technique ;
- la réglementation pose un principe général d'effacement ou d'anonymisation des données de connexion ;
- il existe plusieurs régimes juridiques distincts en fonction de la nature de celui qui opère la journalisation ou du cadre dans lequel les éléments de journalisation sont générés.

Valeur probatoire des éléments de journalisation

- objectifs :

- permettre la traçabilité de l'activité d'un réseau et d'apporter la preuve de cette activité (utilisation ou non-utilisation d'une application ou d'un service par un utilisateur, accès illégitime, etc) ;
 - être en capacité à identifier directement ou indirectement un individu ou un équipement ayant participé à cette activité.
- afin d'être opposable en cas de contentieux, leur mise en œuvre doit respecter les règles relatives à l'administration de la preuve et les principes directeurs des procès civils et pénaux

Traces nominatives

Régime général de protection des données à caractère personnel

- les éléments de journalisation peuvent contenir des données à caractère personnel (données relatives à une personne identifiable directement ou indirectement) ;
- une adresse courriel, une URL ou une adresse IP sont régulièrement considérées par la CNIL comme des données à caractère personnel.

Le traitement d'éléments de journalisation impose le plus souvent le respect des dispositions notamment de la loi du 6 janvier 1978 et en particulier :

- formalités préalables auprès de la CNIL (déclaration, autorisation, etc.) ;
- définir une politique claire adaptée aux données traitées et aux finalités ;
- définir le cycle de vie des éléments de journalisation (processus de création, de conservation, de destruction, etc.) ;
- respecter les exigences relatives aux droits de la personne.

Accès aux traces nominatives

Jurisprudence CNIL

- seules des personnes spécifiquement habilitées peuvent accéder aux éléments de journalisation ;
- les personnes habilitées doivent être soumises à des obligations de confidentialité particulières ;
- l'accès doit être strictement limité à la finalité poursuivie, de la manière la moins intrusive possible pour les données à caractère personnel ;
- le personnel habilité ne doit subir aucune contrainte quant au dévoilement des informations, notamment par son employeur, sauf si la loi en dispose autrement (dans le cadre d'une procédure judiciaire) ;
- les éléments de journalisation ne peuvent être conservés que pour un temps limité ;
- les activités liées à la gestion des éléments de journalisation doivent être strictement limitées au but poursuivi ;
- les procédures liées à la gestion des éléments de journalisation doivent être décrites dans des documents de référence, permettant ainsi de s'assurer que les données à caractère personnel ne sont pas conservées de manière illégitime.

Régimes particuliers relatifs à la conservation des éléments de journalisation

- conservation des éléments de journalisation au minimum durant un an par les fournisseurs d'accès à Internet (FAI) et par les hébergeurs ;

- conservation des éléments de journalisation des opérateurs de communications électroniques.

3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation

Règles de conception technique

La prise en compte de la fonction de journalisation est primordiale et doit se faire lors de toute démarche de conception et de développement.

Les événements doivent être horodatés

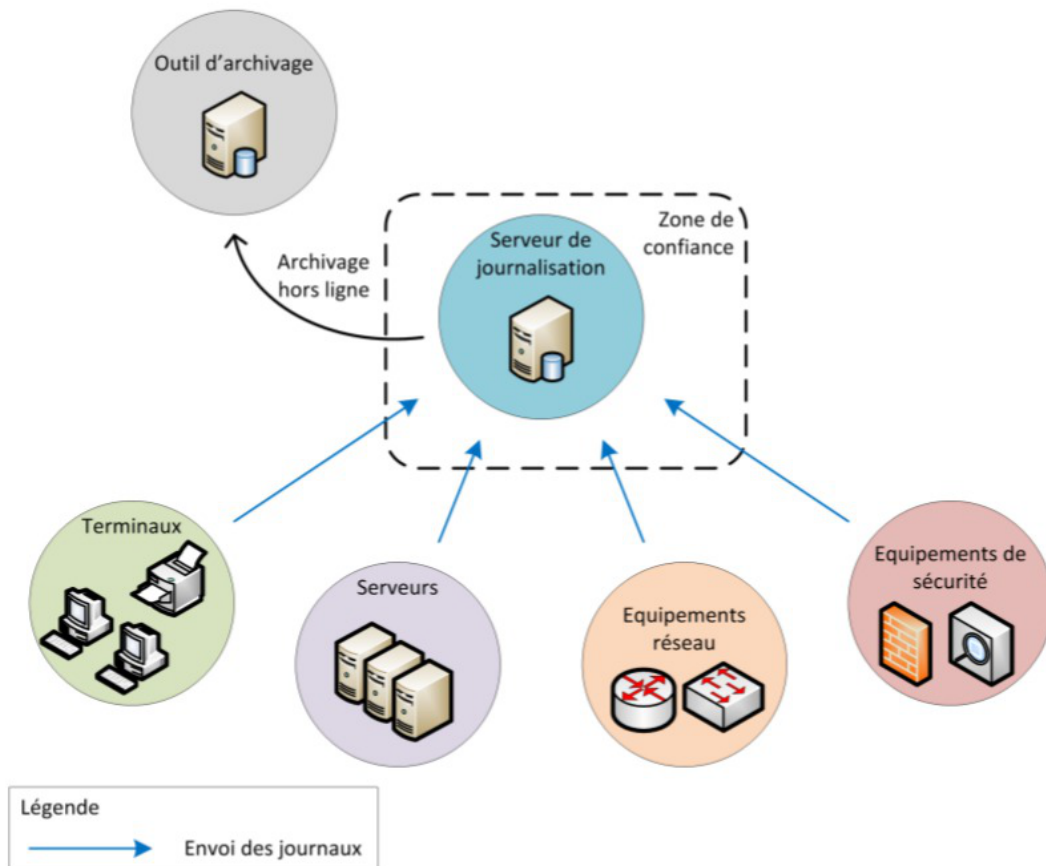
- pour l'ensemble des événements et ce afin de permettre une meilleure exploitation des journaux ;
- les horloges des équipements doivent être synchronisées sur plusieurs sources de temps internes cohérentes entre elles.

Dimensionnement

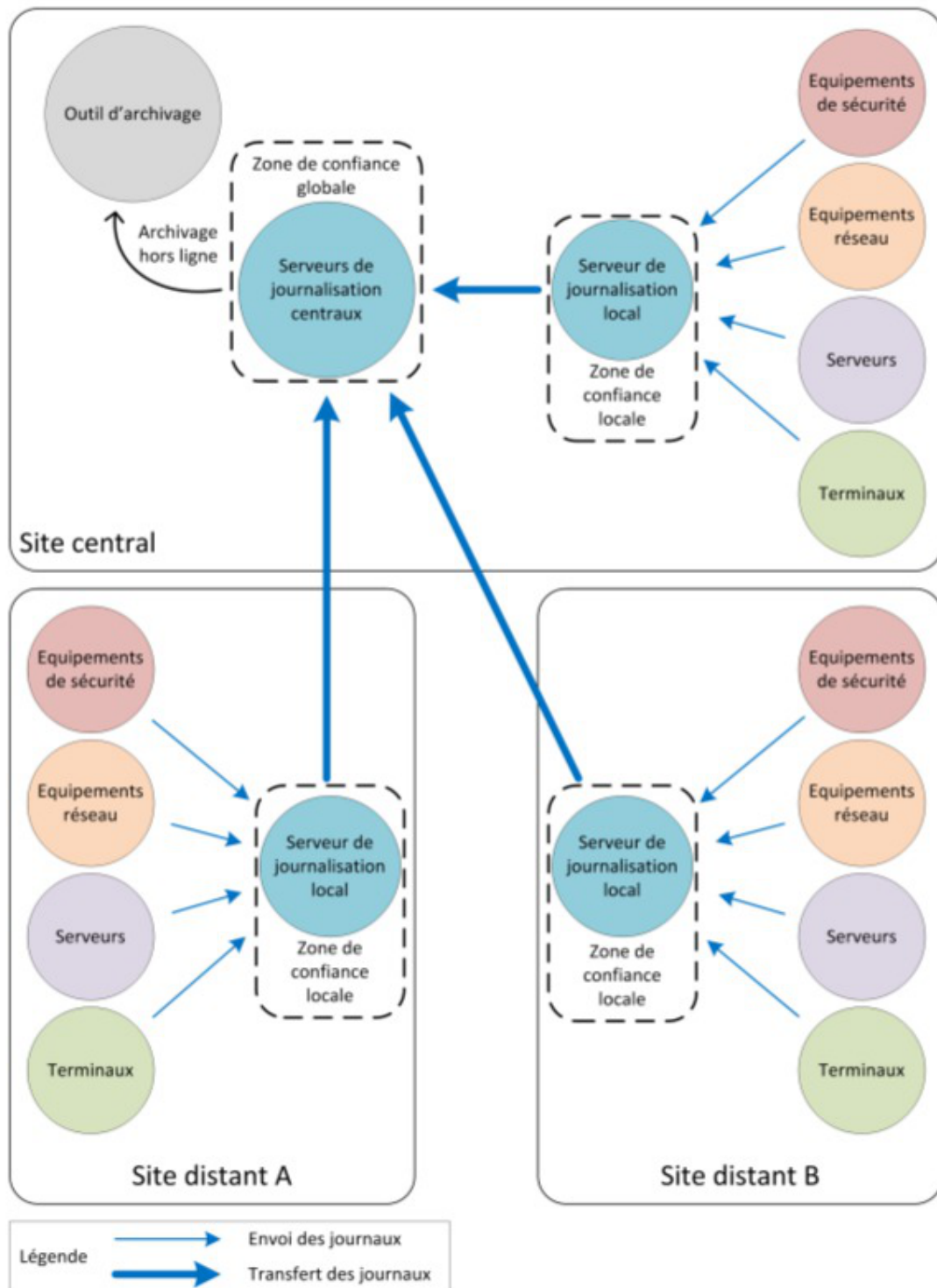
- l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux doit être prise en compte dans le dimensionnement des équipements,

Recommandations d'architecture et de conception

- Les journaux doivent être automatiquement exportés sur une machine physique différente de celle qui les a générés ;
- centralisation des journaux de l'ensemble des équipements du système d'information sur des serveurs dédiés ;
- redondance nécessaire du serveur central en cas de volume de journaux important ou selon le nombre de sites de collecte de journaux ;
- selon la taille ou la typologie du système d'information mise en place d'une approche hiérarchique pour l'organisation des serveurs de collecte.



Exemple d'architecture de journalisation simple (image du document officiel de l'ANSSI)



Exemple d'architecture de journalisation multi-sites (image du document officiel de l'ANSSI)

Protection des données échangées

- privilégier un transfert en temps réel des journaux sur les serveurs centraux ;
- ne pas effectuer de traitement sur les journaux avant leur transfert (peut conduire à dénaturer les événements et induire des pertes d'information).

Fiabilisation du transfert des journaux

- il est recommandé d'utiliser des **protocoles d'envoi de journaux basés sur TCP** pour fiabiliser le

transfert de données entre les machines émettrices et les serveurs centraux.

Sécurisation du transfert des journaux

- utiliser des protocoles de transfert de journaux qui s'appuient sur des mécanismes cryptographiques robustes ;
- contrôler la bande passante des flux réseau utilisée pour transférer les journaux d'événements ;
- en cas de besoin de sécurité, le transfert des journaux doit se faire sur un réseau d'administration dédié ;
- placer les serveurs de journalisation dans un réseau spécifique non exposé directement à des réseaux qui ne sont pas de confiance.

Stockage

- dédier une partition disque au stockage des journaux d'événements ;
- prendre en compte les durées réglementaires de stockage.

Protection des journaux

- l'accès aux journaux doit être limité en écriture à un nombre restreint de comptes ayant le besoin d'en connaître ;
- les processus de journalisation et de collecte doivent être exécutés par des comptes disposant de peu de privilèges ;
- un outil spécifique doit être utilisé pour une meilleure exploitation des journaux présents sur les serveurs centraux ;
- les comptes ayant accès à l'outil de consultation centralisée des journaux doivent être associés à des rôles prédéterminés.

Chapitre 12

Paramétrage des postes client

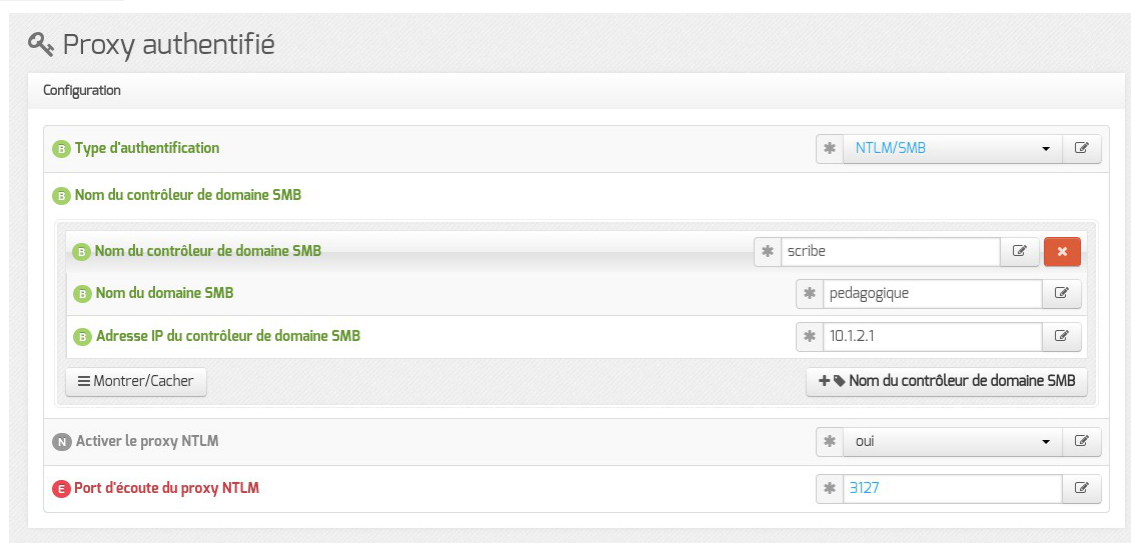
1. Authentification NTLM/SMB - NTLM/KERBEROS hors domaine

L'authentification NTLM^[p.555] pour des postes hors domaine est facilité par l'utilisation du proxy Cntlm^[p.543].

Installation et activation

Cntlm est pré-installé sur les modules Amon, AmonEcole et ses variantes.

L'activation du service se fait dans l'interface de configuration du module dans l'onglet **Proxy authentifié**. Cet onglet n'est disponible que si l'authentification web a été, elle-même, activée dans l'onglet **Authentification**.



Vue de l'onglet Proxy authentifié dans l'interface de configuration du module

Il faut choisir le type d'authentification sur le proxy NTLM/SMB ou NTLM/KERBEROS.

Ensuite il faut passer la variable Activer le proxy NTLM à oui.

Par défaut, le port de Cntlm est le 3127 mais sa valeur peut être modifiée par le biais de la variable experte intitulée : Port d'écoute du proxy NTLM.

L'activation du service est effective après une reconfiguration du serveur avec la commande :

```
# reconfigure
```



Attention, si l'authentification de type NTLM/SMB est choisie, c'est le premier domaine spécifié qui sera utilisé par Cntlm.

Configuration des clients hors domaine

L'authentification proxy NTLM/SMB et NTLM/KERBEROS nécessite une configuration particulière des postes clients Windows.

Par défaut, il est nécessaire, par exemple, de modifier la base de registre sur le poste Windows Seven.

Mais dans le cas de l'utilisation de Cntlm aucun changement n'est requis dans la base de registre pour les postes hors domaine.

Les postes nomades (hors domaine) doivent utiliser le port [3127](#) pour passer par Cntlm.

Configuration des clients du domaine

Pour continuer à profiter de l'authentification transparente, les postes intégrés au domaine ne doivent pas passer par Cntlm.

Il est donc nécessaire de configurer correctement les postes du domaine avec, par exemple, ESU^[p.547].

Les postes intégrés au domaine doivent donc utiliser le port [3128](#) pour passer par le proxy .

— Dans le cas où la découverte automatique du proxy avec WPAD est activée, le port proposé par défaut est automatiquement celui du proxy NTLM Cntlm ([3127](#) par défaut).

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD ^[p.267]

]

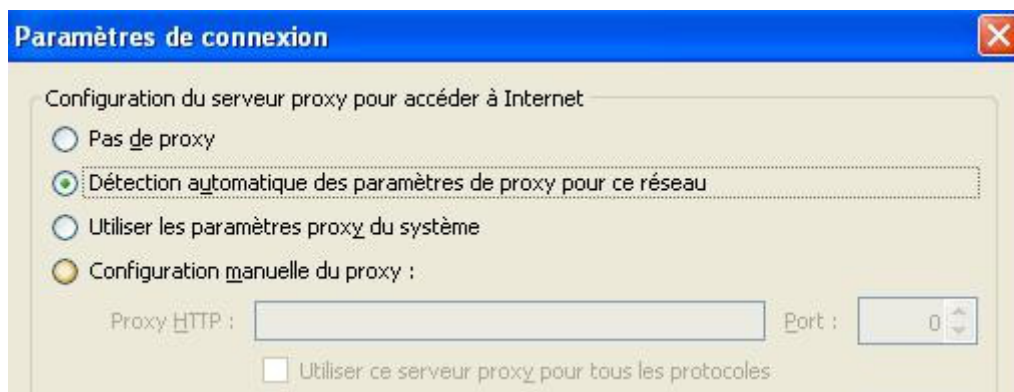
Onglet Proxy authentifié : 5 méthodes d'authentification ^[p.142]

2. Configurer la découverte automatique du proxy avec WPAD

WPAD^[p.564] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essaiera de télécharger le fichier : [wpad.<domaine local>/wpad.dat](#) ou le fichier [proxy.pac](#).

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.



La détection automatique du proxy par les navigateurs peut être imposée par des outils tels que :

- ESU/client Scribe ;
- Gaspacho.

Dans le cas de l'activation du proxy Cntlm^[p.543] le numéro de port change mais sa prise en charge est automatisée, il n'y a donc rien à faire.

Configuration côté serveur

Pour fonctionner correctement, WPAD a besoin de trois éléments qui sont pris en charge par EOLE :

- un serveur web qui diffuse le fichier, dans le cadre d'EOLE, c'est le service Nginx^[p.555] qui se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.
- un nom de domaine `wpad.<nom_domain_local>` qui pointe vers le serveur web ;
- un serveur DHCP configuré pour envoyer le chemin du fichier.

Par défaut, la configuration est correctement définie sur un AmonEcole mais dans le cadre d'un environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

Le serveur DHCP doit être activé et correctement configuré sur le module Scribe.

Dans l'interface de configuration du module en mode expert, dans l'onglet `Dhcp`, le champ `Nom de domaine du serveur WPAD` permet de configurer le nom de domaine du serveur WPAD.



Même s'il est possible d'utiliser n'importe quel domaine, il est conseillé d'utiliser la même valeur que celle utilisée pour le nom de domaine local.



Pour les postes de travail Windows c'est la valeur du champ `Nom de domaine du serveur WPAD` qui sera utiliser pour accéder au fichier WPAD tandis que pour des postes

de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.

 A screenshot of a configuration field titled "Nom de domaine du serveur WPAD" with a red error icon. The field contains the text "etb1.lan" and has a small edit icon to its right.

Dans l'interface de configuration du module, en mode expert, il faut saisir dans le Nom de domaine du serveur WPAD de l'onglet Dhcp la même valeur que celle du champ Nom de domaine privé du réseau local de l'onglet Général.

⚠ Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande reconfigure sur le module.

Configuration sur le module Amon

WPAD est mise à disposition sur les modules Amon et ses variantes (AmonEcole, ...) au travers du paquet eole-wpad mais n'est fonctionnel que si le paquet eole-proxy est installé.

Pour fonctionner correctement, il faut que l'URL wpad.<nom domaine local> corresponde à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.

 A screenshot of a configuration field titled "Activer le support de WPAD" with a blue error icon. The field contains a dropdown menu with the value "oui" and a small edit icon to its right.

Activation de WPAD dans l'onglet Services

Dans l'onglet Services de l'interface de configuration du module Activer le support de WPAD doit être placé à oui.

 A screenshot of a configuration window titled "Wpad" with a sub-section "Configuration". It contains a field titled "Nom de domaine du service WPAD" with a blue error icon, a gear icon, a dropdown menu with "etb3.lan", and a small edit icon.

Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet Wpad au sein duquel le Nom de domaine du service WPAD doit être rempli avec la même valeur que le Nom de domaine privé du réseau local présent dans l'onglet Général.

⚠ Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au Nom de domaine privé du réseau local de l'onglet Général, il faut le déclarer dans le champ Nom domaine local supplémentaire ou rien de l'onglet Zones-dns.



Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande **reconfigure** sur le module.



WPAD supporte les VLAN et les alias, Nginx renvoie le bon fichier WPAD si des VLAN ou des alias sont déclarés.

En mode expert, Il est également possible de changer le port du proxy diffusé par défaut pour une interface, un VLAN ou un alias donné.

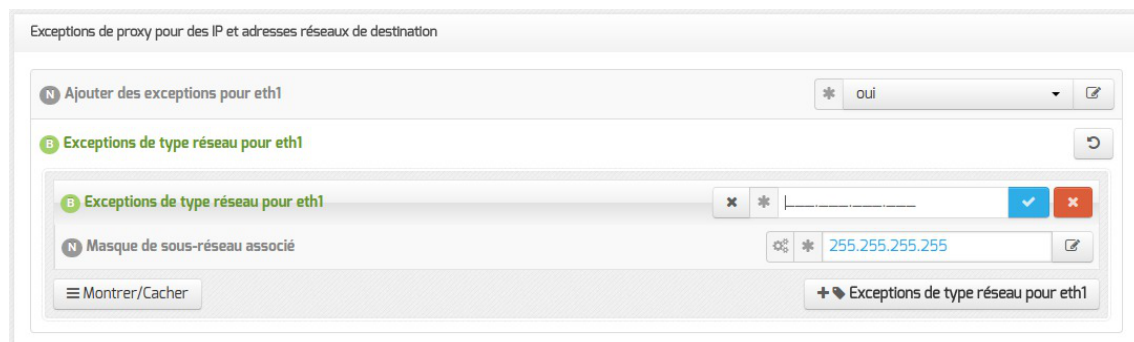
Ajouter des exclusions dans la configuration automatique du proxy

Dans l'onglet **Exceptions proxy** de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

Exception sur une adresse IP ou une plage d'adresses IP

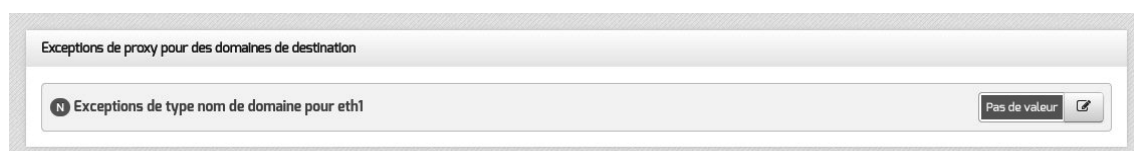
Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de destination pour laquelle on ne passe pas par le proxy.



Le bouton **Exceptions de type réseau pour eth1** permet d'ajouter plusieurs exceptions sur une même interface.

Exception sur un nom de domaine

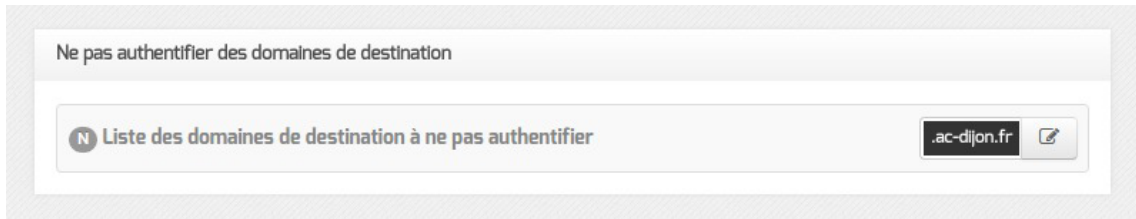
Cette exception commune à ERA et à WPAD permet de déclarer un domaine de destination pour laquelle on ne passe pas par le proxy.



Il est possible d'ajouter plusieurs exceptions sur une même interface.

Exception au niveau de l'authentification des domaines

Cette exception permet de déclarer des sites pour lesquels le proxy ne demandera pas l'authentification à l'utilisateur qui souhaite y accéder.

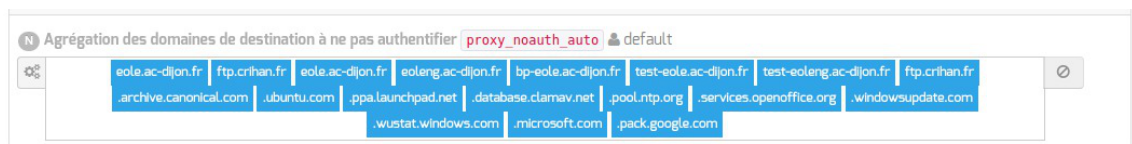


Si cNTLM et WPAD sont activés sur l'interface réseau, les utilisateurs utiliseront directement Squid (sans passer par cNTLM) pour accéder à ces sites.

Les domaines commençant par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

Si on spécifie la valeur `.ac-dijon.fr` alors `ac-dijon.fr` et `www.ac-dijon.fr` seront autorisés sans authentification.

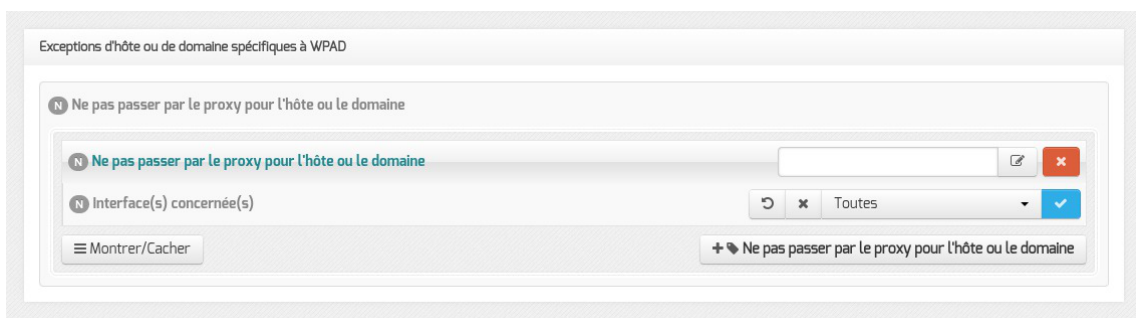
Une liste de sites à ne pas authentifier par défaut est stockée dans la variable cachée `proxy_noauth_auto`. Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



Cette variable reprend la liste des sites qui étaient dans le template `domaines_noauth` des versions EOLE antérieures à 2.5.2.

Exception sur un nom d'hôte (spécifique à WPAD)

L'exception sur un nom d'hôte s'effectue sur le nom d'hôte et sur le nom d'hôte complet.



Il faut choisir une interface ou toutes les interfaces sur lesquelles l'exception sera appliquée. Le bouton `+ Ne pas passer par le proxy pour l'hôte ou le domaine` permet d'ajouter plusieurs exceptions sur une même interface.

Ce type d'exception étant spécifique à WPAD, il n'est pas prise en compte par les autres services gérant des exceptions au niveau du proxy.

Si le champ `Ne pas passer par le proxy pour l'hôte ou le domaine` a comme valeur `www.ac-monacad.fr`, le fichier WPAD.dat généré contiendra la ligne `localHostOrDomainIs(host, "www.ac-monacad.fr")` qui permet d'exclure simplement des URLs.

Compléments sur `Ne pas passer par le proxy pour le domaine` (dnsDomains) :
<http://findproxyforurl.com/netscape-documentation/#dnsDomains>
Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomains) :
<http://findproxyforurl.com/netscape-documentation/#localHostOrDomains>

Configuration du serveur DHCP sur le module Scribe

Onglet Dhcp : Configuration du serveur DHCP

3. Proxy non configuré dans le navigateur : redirection ou page d'information

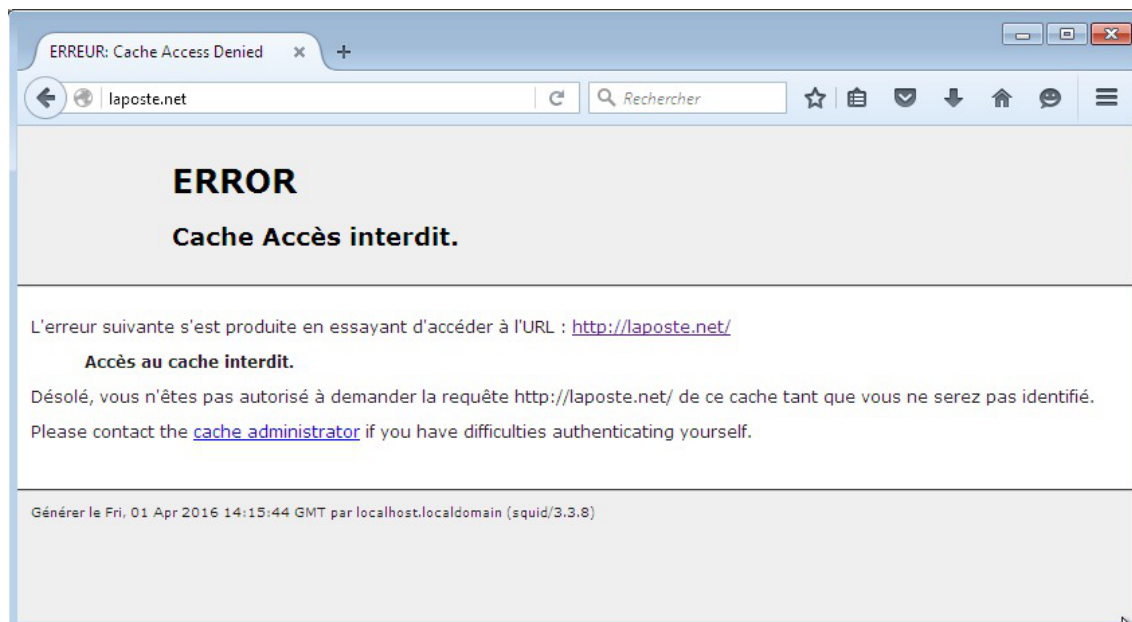
Redirection transparente HTTP sur Amon

Sur le module Amon, les flux HTTP provenant des réseaux internes sont redirigés vers le proxy.

La redirection transparente ne fonctionne pas avec le protocole HTTPS car il s'agit d'un mode connecté qui ne supporte pas ce genre de manipulation sur les paquets. La redirection est faite uniquement pour obliger les postes à utiliser le proxy.

La redirection transparente n'est pas mise en place sur le module AmonEcole et ses variantes.

Si l'authentification du proxy est activée sur l'interface, la redirection fonctionnera mais pas l'authentification et l'utilisateur obtiendra une page d'erreur explicite provenant du logiciel Squid.



Page d'erreur renvoyée par Squid en cas d'erreur d'authentification



Dans l'onglet **Exceptions proxy** de l'interface de configuration du module, il est possible de déclarer des adresses de destination qui seront exclues de la redirection vers le proxy.

Page d'information renvoyée par Nginx

Sur les modules Amon et AmonEcole, la configuration du logiciel Nginx a été adaptée afin de détecter le cas où le navigateur du client n'a pas été configuré correctement et lui renvoyer un message d'erreur suffisamment explicite.



Page d'erreur renvoyée par Nginx en cas de proxy non configuré



La page d'erreur affichée dans le navigateur peut être personnalisée.

Personnaliser la page renvoyée par Nginx à l'aide d'un patch

La page d'erreur affichée dans le navigateur est un template Creole :
`/usr/share/eole/creole/distrib/nginx.no_proxy.html`

Il est possible de le modifier de façon pérenne en utilisant un patch pour Creole.

Il faut copier le template d'origine dans le répertoire `/usr/share/eole/creole/modif/`

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
/usr/share/eole/creole/modif/nginx.no_proxy.html
```

Il faut éditer, modifier et enregistrer le fichier copié

```
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
```

Puis il faut générer le patch à l'aide de la commande `gen_patch`

```
root@amon:~# gen_patch
```

Le fichier contenant les différences est créé dans le répertoire `/usr/share/eole/creole/patch/`



Les changements prennent effet après la reconfiguration du serveur à l'aide de la commande `reconfigure`

```
root@amon:~# reconfigure
```

La page servie par Nginx contient les modifications :

```
root@amon:~# vim /var/www/index.html
```



```
1 root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
  /usr/share/eole/creole/modif/nginx.no_proxy.html
2 root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
3 [...]
4 root@amon:~# gen_patch
5
6 ** Génération des patches à partir de modif **
7
8 Génération du patch nginx.no_proxy.html.patch
9
10 ** Fin de la génération des patch **
11
12 root@amon:~# ls /usr/share/eole/creole/patch/
13 nginx.no_proxy.html.patch variante
14 root@amon:~# reconfigure
15 [...]
16 root@amon:~# vim /var/www/index.html
```

Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.

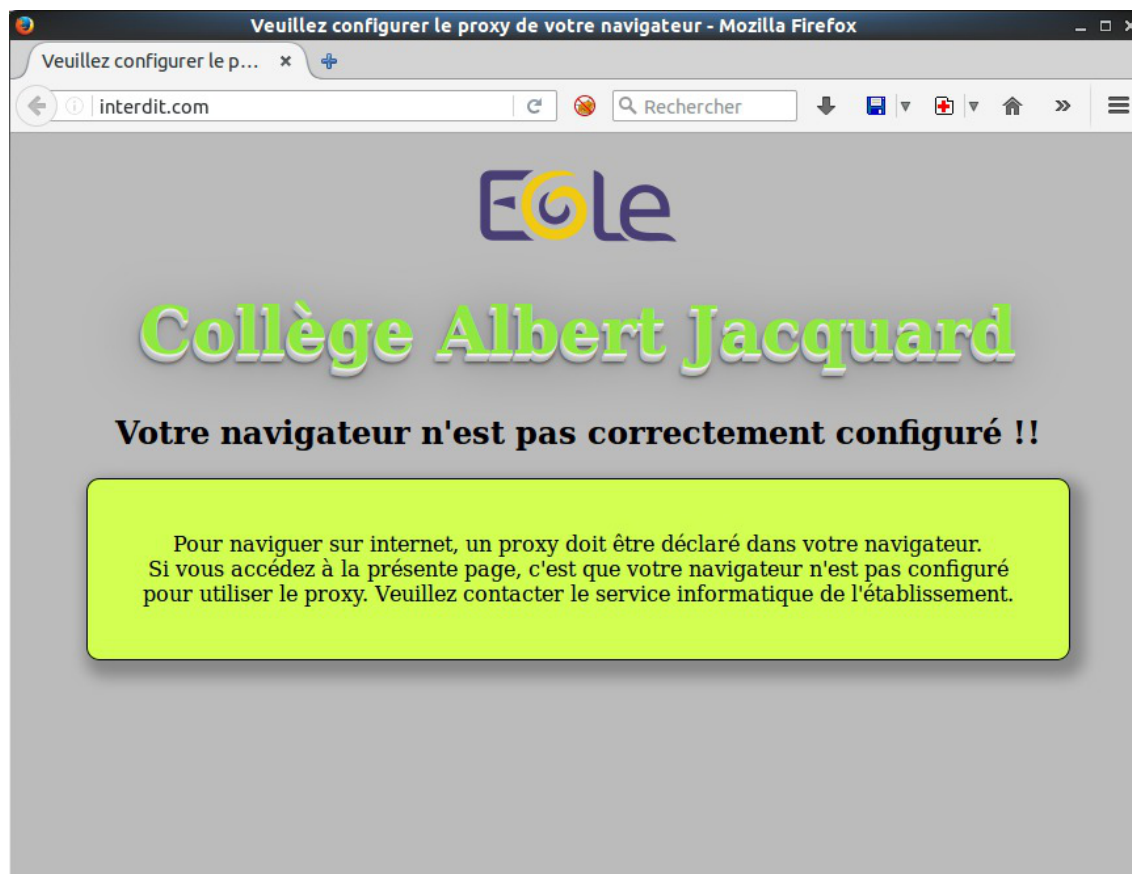


```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
2 <html>
3   <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
4   <head>
5 <title>Veuillez configurer le proxy de votre navigateur</title>
```

```

6 <style>
7 .main {
8     background:#bbbbbb;
9     text-align:center;
10 }
11 h1 {
12     /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
13     color: #91e842;
14     font-size: 50px;
15     text-align:center;
16     text-shadow: 0 1px 0 #eee,
17                 0 2px 0 #e5e5e5,
18                 -1px 3px 0 #C8C8C8,
19                 -1px 4px 0 #C1C1C1,
20                 -2px 5px 0 #B9B9B9,
21                 -2px 6px 0 #B2B2B2,
22                 -2px 7px 2px rgba(0,0,0, 0.6),
23                 -2px 7px 8px rgba(0,0,0, 0.2),
24                 -2px 7px 45px rgba(0,0,0, 0.4);
25 }
26 .message {
27     top:25%;
28     text-align:center;
29     margin-left: 50px;
30     margin-right: 50px;
31
32     padding: 40px;
33     background: #d2ff52;
34     border: 1px solid #000000;
35
36     border-radius: 10px;
37     -moz-border-radius: 10px;
38     -webkit-border-radius: 10px;
39
40     box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
41     -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
42     -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
43 }
44 </style>
45 </head>
46 <body class='main'>
47 
48 <h1>%%libelle_etab</h1>
49 <h2>Votre navigateur n'est pas correctement configuré !!</h2>
50 <div class="message">Pour naviguer sur internet, un proxy doit être
déclaré dans votre navigateur.<br />
51 Si vous accédez à la présente page, c'est que votre navigateur n'est pas
configuré pour utiliser le proxy. Veuillez contacter le service informatique
de l'établissement.</div>
52 </body>
53 </html>
54

```



Page d'erreur renvoyée par Nginx en cas de proxy non configuré

4. Synthèse des paramètres proxy à utiliser pour les postes client

Module Amon standard

Sur une installation standard du module Amon, l'adresse du proxy sera l'adresse du serveur Amon sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau administratif : `adresse_ip_eth1:3128`
- proxy sur le réseau pédagogique : `adresse_ip_eth2:3128`
- proxy sur la DMZ : `adresse_ip_eth3:3128`

Module AmonEcole et ses variantes

Sur une installation standard des modules AmonEcole/AmonHorus, l'adresse du proxy sera l'adresse IP réservée pour le proxy sur le réseau. Le port sera celui de e2guardian (3128 par défaut), ce qui donne par exemple :

- proxy sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3128`

On notera que, comme sur un module Amon standard, la passerelle est l'adresse du module Amon sur le réseau (`adresse_ip_eth1`). Mais par contre pour le DNS, il faut utiliser la même adresse IP que celle du proxy.

Double authentification

Si la double authentification est configurée, le port à utiliser pour le second proxy sera celui de la troisième configuration e2guardian (variable `dansguardian_port3` : 3129 par défaut), soit :

- proxy2 sur le réseau eth1 Amon : `adresse_ip_eth1:3129`
- proxy2 sur le réseau AmonEcole : `adresse_ip_eth1_proxy_link:3129`

Proxy NTLM

Si l'authentification NTLM pour des postes hors domaine est configurée :

- les postes intégrés au domaine doivent continuer à utiliser le port de e2guardian (3128 par défaut) ;
- les postes nomades (hors domaine) doivent utiliser le port défini par la variable `cntlm_port` (3127 par défaut) pour passer par Cntlm.

Filtrage web désactivé

Si le filtrage web est désactivé, le proxy Squid écoute sur le port 3128 en lieu et place du logiciel de filtrage e2guardian.

En cas de double authentification, le second proxy répondra sur le port 3129.

Chapitre 13

Compléments techniques

Cette partie de la documentation regroupe différentes informations complémentaires : des schémas, des informations sur les services, les ports utilisés sur chacun des modules...

1. Les services utilisés sur le module Amon

Les services disponibles sur les modules EOLE ont été répartis dans des paquets distincts, ce qui rend leur installation complètement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.



Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro.

<http://dev-eole.ac-dijon.fr/projects/eole-antivir>

<http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf>

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon [<http://www.clamav.net/>] et clamav-freshclam.

Historique

À la base, les services *clamav* et *freshclam* étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

Le serveur de mise à jour des bases antivirus (freshclam) s'installe sur le maître.

Le ou les services antivirus s'installent dans les conteneur qui en ont l'usage.

Sur les modules AmonEcole et AmonHorus, le service clamav-daemon est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.



C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.



Activation de clamav dans un conteneur

```
1 <container name='xxx'>
2   <package>eole-antivirus-pkg</package>
3   <service>clamav-daemon</service>
4   <file filelist='clamav' name='/etc/clamav/clamd.conf' />
5 </container>
```

1.2. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP.

Logiciels et services

Le paquet `eole-dhcrelay` s'appuie sur le service dhcp3-relay.

<http://www.isc.org>

Historique

Ce service est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le maître.

1.3. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9^[p.542].

Historique

À la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `dns (id=18)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.4. eole-exim

Le paquet `eole-exim` permet la mise en place d'un serveur SMTP Exim.

Logiciels et services

Le paquet `eole-exim` s'appuie principalement sur le service exim4.

<http://www.exim.org/>

Historique

Utilisé à la base sur les modules Scribe et Seshat, le paquet `eole-exim` est désormais utilisé sur tous les modules.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.

Sur le module AmonEcole et ses variantes, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

1.5. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.



La gestion des onduleurs fait l'objet d'une documentation dédiée : `GestionDesOnduleurs`.

Logiciels et services

Le paquet `eole-nut` s'appuie sur le service upsd.

<http://www.networkupstools.org/>

Historique

Ce paquet est pré-installé sur tous les modules depuis la version 2.3 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

 La gestion du proxy et du filtrage web fait l'objet d'une documentation dédiée : `Proxy`.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les services suivants :

- Squid : proxy cache ;
- e2guardian : filtrage web ;
- Lightsquid : analyseur de logs ;
- smb, nmbd, winbind, krb5 : authentification NTLM/KERBEROS.

<http://www.squid-cache.org/>

<http://e2guardian.org>

<http://lightsquid.sourceforge.net/>

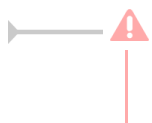
Historique

A la base, uniquement disponible sur les modules Amon et AmonEcole, ce paquet a été adapté pour être installé sur n'importe quel module EOLE, y compris en **mode une carte**.

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `proxy (id=20)`.

Sur les modules AmonEcole et AmonHorus, il est installé dans le groupe de conteneurs : `internet (id=53)`.

 En mode conteneur, l'accès à ces services nécessite la configuration d'une adresse spécifique sur le réseau cible (variable : `adresse_ip_proxy_link`).

Remarques

Afin d'assurer l'authentification en mode NTLM/KERBEROS, ce paquet fournit des configurations Samba incompatibles avec celles d'`eole-fichier`.

Si l'on souhaite installer `eole-proxy` et `eole-fichier` sur un même serveur, il est impératif qu'ils soient déclarés dans des conteneurs différents. Leur cohabitation est impossible en *mode non conteneur*.

1.7. eole-radius

Le paquet `eole-radius` permet la mise en place d'un serveur RADIUS^[p.559].

Logiciels et services

Le paquet `eole-radius` s'appuie sur le projet FreeRADIUS.

<http://freeradius.org/>

Historique

Ce paquet est pré-installé sur le module Amon.

Conteneurs

Le service s'installe sur le serveur maître.

1.8. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, Nginx^[p.555], peut aussi faire office de serveur web.

<http://nginx.org/>

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.9. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN^[p.559].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan^[p.562].

Historique

Ce paquet est pré-installé sur les modules Amon, AmonEcole et ses dérivés ainsi que sur le module Sphinx.

Conteneurs

Le service s'installe sur le serveur maître.

1.10. eole-wpad

Le paquet `eole-wpad` permet la mise en place du service de découverte automatique du proxy par les navigateurs (WPAD^[p.564]).

Le logiciel utilisé, Nginx^[p.555], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

<http://nginx.org/>

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

Historique

Ce service étaient auparavant inclus dans le paquet `eole-reverseproxy`. Il peut désormais être installé de façon indépendante.

Le paquet `eole-wpad` est pré-installé sur les modules Amon, AmonEcole et ses dérivés.

Conteneurs

Le service s'installe sur le système hôte (maître).

2. Ports utilisés sur le module Amon

Le module Amon propose de nombreux services.

Ce document donne la liste exhaustive des ports utilisés sur un module Amon standard.

Les ports utilisés sont, dans la mesure du possible, les ports standards préconisés pour les applications utilisées.

Il est possible de lister les ports ouverts sur le serveur par la commande :

```
netstat -ntulp
```



En mode conteneur, la commande `netstat` listera uniquement les services installés sur le maître.

Ports communs à tous les modules

- 22/tcp : ssh (sshd)
- 25/tcp : smtp (Exim4)
- 68/udp : dhclient
- 123/udp : ntpd
- 514/udp : rsyslogd (réception des journaux distants)
- 3493/tcp : nut (gestion des onduleurs)
- 4200/tcp : ead-web
- 4201/tcp : ead-server
- 4202/tcp : ead-server (transfert de fichiers)
- 5000/tcp : eoleflask/eolegenconfig (application admin)
- 7000/tcp : gen_config
- 8000/tcp : creoled
- 8090/tcp : z_stats (consultation des statistiques Zéphir locales), mise à jour automatique du client Zéphir
- 8443/tcp : EoleSSO
- 10514/tcp : rsyslogd (réception des journaux distants, protocole TCP)
- 12560/tcp : rsyslogd (réception des journaux distants, protocole RELP)

Ports spécifiques au module Amon

- 50/esp : IPsec
- 53/tcp+udp : bind (DNS)
- 67/udp : dhcrelay
- 500/udp : charon (VPN)
- 953/tcp : bind (RNDC)
- 1812/udp : radius
- 1813/tcp+udp : radius accounting
- 3127/tcp : Cntlm (proxy NTLM)
- 3128/tcp : e2guardian (filtrage web)
- 3129/tcp : e2guardian (filtrage web)
- 3401/udp : squid (agent SNMP)
- 4500/udp : charon (VPN)

- 8062/tcp : cgi lightsquid (consultation des statistiques de navigation)
- 8080/tcp : squid (proxy)
- 8081/tcp : squid (proxy)

Le proxy inverse Nginx est susceptible d'écouter sur de nombreux ports afin d'assurer ses missions de redirection :

- 80/tcp : nginx (redirection http)
- 81/tcp : nginx (erreur proxy http)
- 82/tcp : nginx (erreur proxy https)
- 443/tcp : nginx (redirection https)
- 4203/tcp : nginx (redirection vers un EAD)
- 7070/tcp : nginx (redirection vers un portail Envole)
- 8443/tcp : nginx (redirection vers un serveur EoleSSO)

Services et numéro de ports

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

Chapitre 14

Questions fréquentes

Certaines interrogations reviennent souvent et ont déjà trouvées une réponse ou des réponses.



1. Questions fréquentes communes aux modules

Accéder aux partitions du module depuis un Live Linux

Lorsqu'on a recours à un live CD ou USB, il n'est pas possible d'accéder directement aux partitions.

```
1 # mkdir /media/partition
2 # mount /dev/sda2 /media/partition
3 mount: type inconnu de système de fichiers 'LVM2_member'
```

💡 Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
1 # vgscan
2 Reading all physical volumes. This may take a while...
3 Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
1 # vgchange -a y eolebase-vg
2 4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
1 # ll /dev/mapper/
2 total 0
3 drwxr-xr-x 2 root root 160 févr. 8 11:53 ./
```



```

4 drwxr-xr-x 19 root root    4460 févr.  8 11:53 ../
5 crw-----  1 root root    10, 236 févr.  8 11:53 control
6 lrwxrwxrwx  1 root root         7 févr.  8 11:53 eolebase--vg-home ->
  ../dm-4
7 lrwxrwxrwx  1 root root         7 févr.  8 11:53 eolebase--vg-root ->
  ../dm-0
8 lrwxrwxrwx  1 root root         7 févr.  8 11:53 eolebase--vg-swap_1 ->
  ../dm-1
9 lrwxrwxrwx  1 root root         7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
10 lrwxrwxrwx  1 root root         7 févr.  8 11:53 eolebase--vg-var -> ../dm-3

```

OU

```

1 # lvsdisplay
2 --- Logical volume ---
3 LV Path                /dev/eolebase-vg/swap_1
4 LV Name                swap_1
5 VG Name                eolebase-vg
6 LV UUID                0047WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
7 LV Write Access        read/write
8 LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
9 LV Status              available
10 # open                 2
11 LV Size                1,09 GiB
12 Current LE            280
13 Segments               1
14 Allocation             inherit
15 Read ahead sectors    auto
16 - currently set to    256
17 Block device           252:1
18 [...]

```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

Ajouter de l'espace disque à un volume LVM

Sur le nouveau périphérique physique, créer une partition de type Linux LVM (8E), avec `cgdisk` par exemple.

La nouvelle partition s'appelle par exemple `/dev/sdb1` et peut être ajoutée au volume, par exemple pour agrandir `/var`.



Après avoir créé la nouvelle partition `/dev/sdb1` il peut être nécessaire de redémarrer le serveur pour la faire prendre en compte par le système.

Démonter la partition

Pour démonter la partition

```
# umount /var
```

Créer un volume physique

Créer un volume physique avec la nouvelle partition :

```
# pvcreate /dev/sdb1
```

Quel est le groupe de volumes

Rechercher dans quel groupe de volumes (VG Name) se trouve le volume logique `/var` :

```
1 root@scribe:/dev/mapper# lvs /dev/scribe-vg/var
2 --- Logical volume ---
3 LV Path                /dev/scribe-vg/var
4 LV Name                 var
5 VG Name                 scribe-vg
6 LV UUID                 N4dHMU-htpz-AhEI-x5Ld-EvpM-ZFJX-M3LbHD
7 LV Write Access        read/write
8 LV Creation host, time scribe, 2017-01-16 19:17:09 +0100
9 LV Status               available
10 # open                  1
11 LV Size                 8,35 GiB
12 Current LE             2138
13 Segments                1
14 Allocation              inherit
15 Read ahead sectors     auto
16 - currently set to     256
17 Block device           252:3
18
19 root@scribe:/dev/mapper#
```

Ajouter ce volume physique au groupe de volumes contenant le volume logique `/var`, ici `scribe-vg` :

```
# vgextend scribe-vg /dev/sdb1
```

Agrandir le volume logique

Agrandir le volume logique correspondant à `/var` avec le nouvel espace libre :

```
# lvextend -l +100%FREE /dev/scribe-vg/var
# e2fsck -f /dev/scribe-vg/var
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM

Sur un serveur où une partition est saturée.

```
1 root@scribe:~# df -h
2 Sys. de fichiers      Taille Utilisé Dispo Uti% Monté sur
3 udev                  1,5G      0 1,5G  0% /dev
4 tmpfs                 301M      52M 250M 18% /run
5 /dev/mapper/scribe--vg-root 9,1G    2,6G 6,0G 30% /
6 tmpfs                 1,5G      28K 1,5G  1% /dev/shm
7 tmpfs                 5,0M      0 5,0M  0% /run/lock
8 tmpfs                 1,5G      0 1,5G  0% /sys/fs/cgroup
9 /dev/sda1             687M    107M 531M 17% /boot
10 /dev/mapper/scribe--vg-tmp 1,8G    3,4M 1,7G  1% /tmp
11 /dev/mapper/scribe--vg-var 8,1G      8G 0,1G 99% /var
12 /dev/mapper/scribe--vg-home 18G    149M 18G  1% /home
13 tmpfs                 301M      0 301M  0% /run/user/0
14 root@scribe:~#
```

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.

Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

Pour démonter le périphérique :

```
root@scribe:~# umount /home
```

Si le périphérique est occupé, la commande `lsof` renvoie les programmes utilisant la partition :

```
# lsof | grep home
```

Il faut alors arrêter les services concernés puis démonter la partition.

Vérifier le support

Pour vérifier le support, lancer la commande :

```
# fsck -f /dev/mapper/scribe--vg-home
```

Diminuer la taille de la première partition

Réduire le système de fichiers :

```
# resize2fs -p /dev/scribe-vg/home 1G
```

Réduire la partition logique :

```
# lvresize -L-1G /dev/scribe-vg/home
```

Vérifier l'intégrité du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/home
```

Vérifier l'espace libéré

Pour vérifier que l'espace a bien été libéré il faut utiliser la commande `vgdisplay` :

```
# vgdisplay
1 root@scribe:~# vgdisplay
2 --- Volume group ---
3 VG Name          scribe-vg
4 System ID
5 Format           lvm2
6 Metadata Areas  1
7 Metadata Sequence No 6
8 VG Access       read/write
9 VG Status       resizable
10 MAX LV         0
11 Cur LV         5
12 Open LV        5
13 Max PV         0
14 Cur PV         1
15 Act PV         1
16 VG Size        39,30 GiB
17 PE Size        4,00 MiB
18 Total PE       10060
19 Alloc PE / Size 10060 / 39,30 GiB
20 Free PE / Size 0 / 0
21 VG UUID        hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3
22
23 root@scribe:~#
```

La ligne `Free PE / Size` affiche l'espace libre.

Agrandir la taille de la deuxième partition

Les agrandissements peuvent se faire à chaud, ce qui est recommandé si la partition contient les commandes.

Vérifier l'intégrité du système du système de fichiers :

```
# e2fsck -f /dev/scribe-vg/var
```

Agrandir la partition logique :

```
# lvresize -L+1G /dev/scribe-vg/var
```

Étendre le système de fichiers (sans option le système de fichiers prend toute la place possible) :

```
# resize2fs /dev/scribe-vg/var
```

Remonter le périphérique

Procéder au montage du périphérique avec la commande `mount` :

```
# mount /var/home
```



Pensez à redémarrer les services qui ont précédemment été arrêtés.

CAS Authentication failed !

Le message `CAS Authentication failed ! You were not authenticated.` (ou `Authentication CAS infructueuse ! Vous n'avez pas été authentifié(e).`) peut apparaître si des modifications ont été faites dans l'interface de configuration.



Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

```
# _____/usr/share/creole/gen_certif.py -f ou #  
/usr/share/creole/gen_certif.py -f nom du certificat
```

pour la régénération d'un certificat en particulier.

```
# reconfigure
```

💡 Vous avez ajouté un nom DNS alternatif ou une adresse IP alternative sur le serveur

Il faut ajouter le nom alternatif ou l'adresse IP alternative dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet **Certifs-ssl** en mode expert il faut remplir les champs `Nom DNS alternatif du serveur` et/ou l'adresse `IP alternative du serveur`.

Le bouton `+` permet d'ajouter autant d'alternatives que vous voulez. Il faut ensuite `Valider le groupe` et enregistrer la configuration.

L'opération doit être suivie de la reconfiguration du module, cela va régénérer le certificat `/etc/ssl/certs/eole.crt`

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc..) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

```
# reconfigure
```

```
# /usr/share/creole/gen_certif.py -f ou #  
/usr/share/creole/gen_certif.py -f nom du certificat
```

pour la régénération d'un certificat en particulier.

```
# reconfigure
```

Attention, les adresses suivantes ne sont pas définies comme sujet du certificat...

💡 Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc..) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient

à jour).

```
# reconfigure
# /usr/share/creole/gen_certif.py -f ou #
/usr/share/creole/gen_certif.py -f nom_du_certificat pour la régénération
d'un certificat en particulier.
# reconfigure
```

Une erreur se produit lors de l'instanciation ou d'un reconfigure : "starting firewall : [...] Erreur à la génération des règles eole-firewall !! non appliquées !"

Le message suivant apparaît à l'instance ou au reconfigure après changement de valeurs dans l'interface de configuration du module :

```
* starting firewall : bastion (modèle XXX) Erreur à la génération des
règles eole-firewall !!
non appliquées !
```

💡 Vérifier la configuration des autorisations d'accès à SSH et à l'EAD sur les interfaces réseau

Cette erreur provient certainement du masque des variables d'autorisation d'accès à SSH sur l'une des interfaces réseau.

Pour autoriser une seule IP, par exemple `192.168.1.10`, le masque doit être `255.255.255.255` pour autoriser une IP particulière et non `255.255.255.0`

Vérifier l'ensemble des autorisations pour l'accès SSH et pour l'accès à l'EAD.

Pour appliquer les changements il faut reconfigurer le module :

```
# reconfigure
```

La connexion SSH renvoie Permission denied (publickey)

Si les connexions par mots de passe sont interdites, une tentative de connexion sans clé valide entraînera l'affichage du message suivant : `permission denied (publickey).`

Gestion des mises à jour

Pour connaître la date et l'heure des mises à jour du système il est possible de passer par l'EAD ou par un terminal.

💡 Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système / Mise à jour` de l'EAD.

💡 Dans un terminal

```
python -c "from creole import maj; print maj.get_maj_day()"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un

terminal.

► **Via l'EAD**

Pour l'afficher il faut se rendre dans la section **Systeme** / **Mise à jour** de l'EAD.

► **Dans un terminal**

Activation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly add
```

ou :

```
python -c "from creole import maj; maj.enable_maj_auto(); print maj.maj_enabled()"
```

Désactivation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly del
```

ou :

```
python -c "from creole import maj; maj.disable_maj_auto(); print maj.maj_enabled()"
```

Le mot de passe par défaut ne fonctionne pas

Suite à une nouvelle installation le mot de passe par défaut ne fonctionne pas.



Le mot de passe à saisir comprend les dollars devant et derrière : `$eole&123456$`

Échec de la connexion sécurisée

Le navigateur affiche :

Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à IP:Port.

Vous avez reçu un certificat invalide. Veuillez contacter l'administrateur du serveur ou votre correspondant de messagerie et fournissez-lui les informations suivantes :

Votre certificat contient le même numéro de série qu'un autre certificat émis par l'autorité de certification. Veuillez vous procurer un nouveau certificat avec un numéro de série unique.

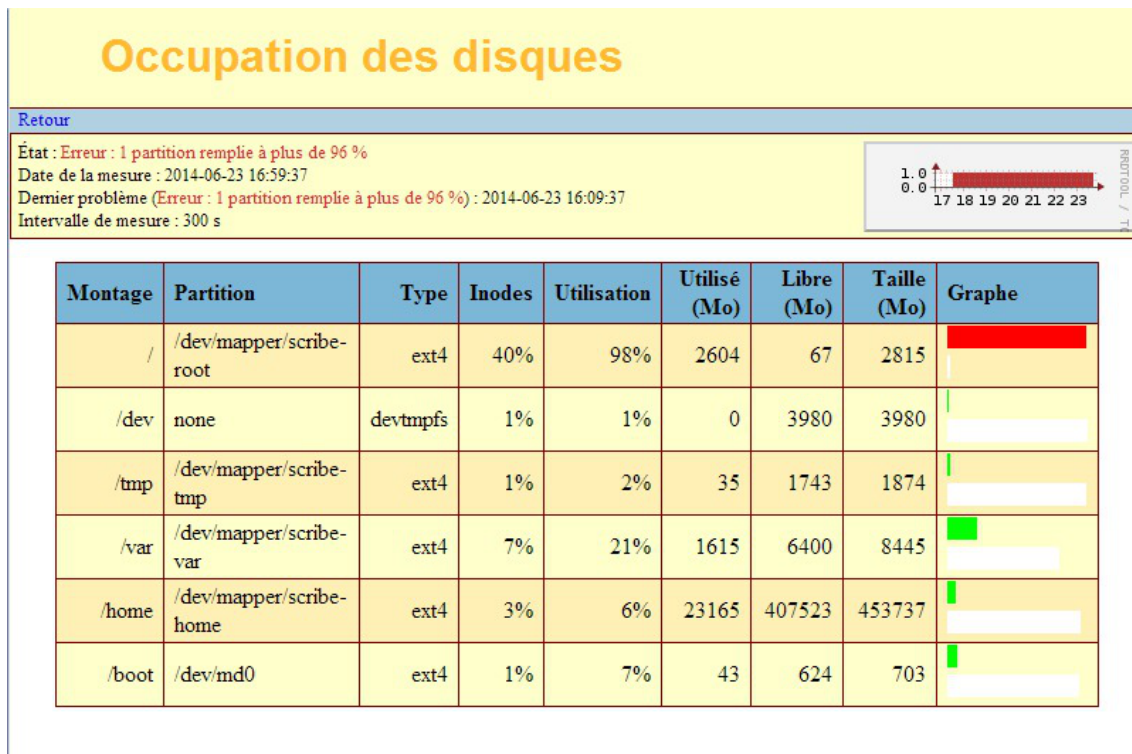
(Code d'erreur : sec error reused issuer and serial)

► **Les paramètres constituant un certificat ont été modifiés récemment**

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une régénération des certificats a eu lieu.

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

Partition saturée

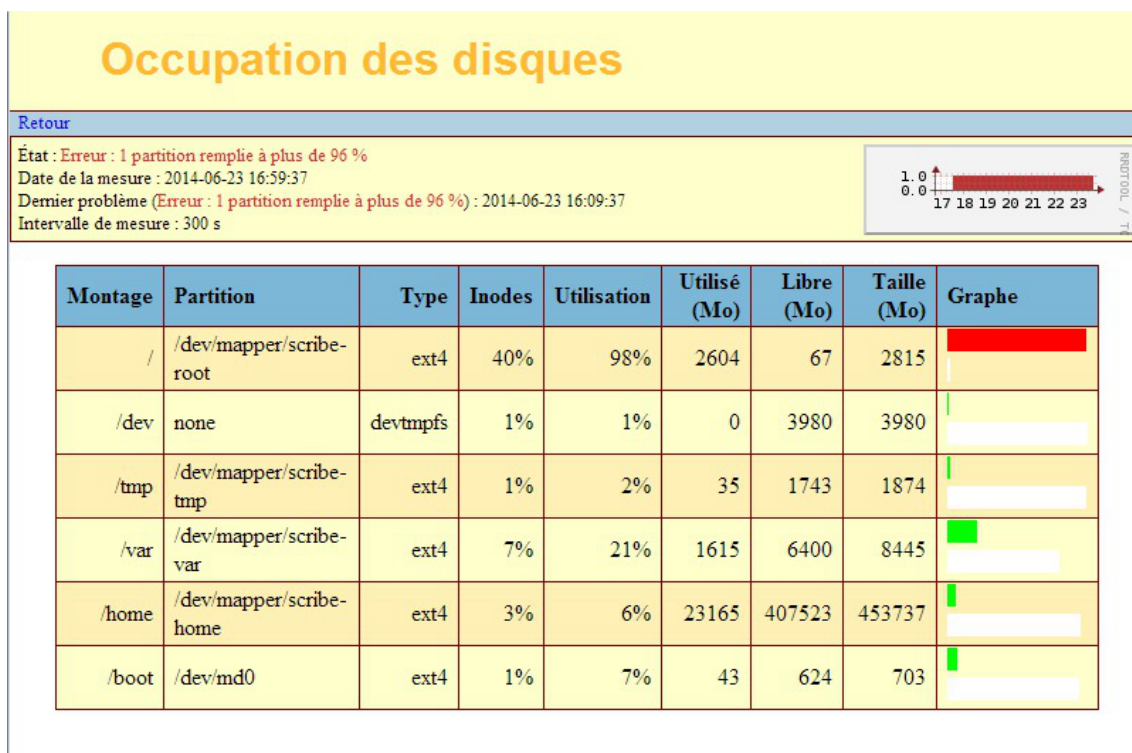


Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- le manque de place disponible ;
- le manque d'inodes disponibles.

La cause de la saturation apparaît dans la page Occupation des disques, soit les inodes soit l'utilisation sont à un pourcentage élevé. La résolution du problème est différente selon le cas.

Partition / saturée



Si la partition racine est saturée sans raison apparente et que le taux d'inodes est correct, le montage d'un répertoire avant copie a peut être échoué. La conséquence est que la copie c'est faite sur la partition racine et non sur le montage. Cela peut être le cas, par exemple, de la sauvegarde.



Il faut donc vérifier le contenu et la place occupée par les répertoires (points de montage) `/mnt`, `/mnt/sauvegardes` et `/media` :

Si le répertoire `/mnt/sauvegardes` n'est pas monté il doit être vide :

```
root@scribe:/mnt/sauvegardes# ls -la
total 8 drwxr-xr-x 2 root root 4096 mai 25 11:29 ./ drwxr-xr-x 26
root root 4096 sept. 9 21:07 ../
root@scribe:/mnt/sauvegardes#
```

Normalement le répertoire `/media` ne contient que des sous-dossiers pour le montage des partitions et ou des périphériques.

Pour vérifier l'espace occupé par ces différents répertoires :

```
root@scribe:/# du -h --max-depth=1 /media /mnt/
4,0K /media 4,0K /mnt/
```



Dans certains cas particuliers, la taille allouée à la partition `/` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM^[p. 552]).

Partition /var saturée

Cette partition contient entre autres les journaux systèmes du serveur.



La commande suivante affiche l'espace occupé par chaque répertoire et les classe par taille, le plus grand nombre en dernier (sans tenir compte de l'unité) :

```
# du -smh /var/* | sort -n
```



Un service mal configuré génère une quantité importante de journaux. Si le problème n'est pas résolu la partition va de-nouveau saturer.



Dans certains cas particuliers, la taille allouée à la partition `/var` peut être trop juste. Il est possible de revoir la taille des partitions avec l'outil de gestion des volumes logiques (LVM^[p. 552]).

Partition /var saturée en inode

Un nombre important de fichiers peut être du à un service mal configuré mais peut aussi être du à un fonctionnement normal. Il faut identifier le répertoire dans lequel il y a le plus de fichier.



La commande suivante affiche le nombre de fichiers par répertoire et les classe par taille, le plus grand nombre en dernier :

```
# for i in $(find /var -type d); do f=$(ls -A $i | wc -l); echo "$f : $i"; done | sort -n
```

Selon les circonstances il faudra soit supprimer des fichiers soit agrandir la partition.



La suppression de fichier ne doit pas être effectué sans connaissances solides du système d'exploitation.

Liste d'arguments trop longue

La commande `# rm -rf /var/<rep>/*` renvoie `Liste d'arguments trop longue`.



Préférez l'utilisation d'une autre commande :

```
# find /var/<rep>/* -type f -name "*" -print0 | xargs -0 rm
```

Le démarrage reste figé à l'étape de vérification des disques

Le serveur est virtualisé avec une solution basée sur l'émulateur qemu.



Seul l'affichage est figé, la machine démarre en fait normalement et est certainement accessible par SSH. Cela vient du support de la carte graphique. Il faut forcer la carte graphique à utiliser une autre carte graphique que celle par défaut (cirrus).

Sous Proxmox, indiquez carte `VGA standard` à la place de `par défaut`.

Accéder à l'interface de configuration du module depuis un navigateur web

Je n'arrive pas à accéder à l'interface de configuration du module depuis mon navigateur web.



Pour pouvoir accéder à l'interface de configuration du module depuis un navigateur web il faut que les deux pré-requis suivants soient respectés :

1. activer l'écoute de l'interface sur l'extérieur en passant la variable `En écoute depuis l'extérieur` à `oui` dans l'onglet Eoleflask.
2. autoriser votre adresse IP pour administrer le serveur dans l'onglet de l'interface réseau concernée.

Après instance ou reconfigure, l'interface de configuration du module est accessible depuis un navigateur web en HTTPS à l'adresse suivante :

```
https://<adresse_serveur>:7000/genconfig/
```

Revenir au dernier état fonctionnel du serveur

Un mauvais paramétrage du serveur ne permet plus d'aller au bout de la reconfiguration du module.



Un fichier `config.eole.bak` est généré dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur. Celui permet d'avoir une trace de la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eole.bak.1` est généré, celui-ci est une copie de la configuration fonctionnelle de l'état d'avant.

S'il existe une différence entre `config.eol` et `config.eole.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'est pas appliquée.

Impossible de trouver la base des matériels maintenue par EOLE

La base des matériels maintenue par EOLE a été supprimée, cette base n'était plus pertinente car elle pouvait contenir du matériel inutilisé comme étant compatible avec les modules EOLE.

Changer le disque dur du serveur

Il est possible entre autre de faire une image avec le logiciel Clonezilla.



L'UUID^[p.563] ayant naturellement changé il faut démarrer en utilisant un LiveCD et éditer l'UUID dans `/etc/fstab` du serveur.

Sources supplémentaires pour apt

Il est possible d'ajouter des sources supplémentaires pour le logiciel apt.



Pour que la solution soit pérenne il faut ajouter dans le répertoire `/etc/apt/sources.list.d/` la description de la nouvelle source dans un fichier portant l'extension `.list`



Par exemple pour avoir à disposition `SCENARIserveur` sur un module EOLE il faut ajouter le fichier `scenari.list` dans le répertoire `/etc/apt/sources.list.d/` avec le contenu suivante :

```
#scenari_ppa
deb https://download.scenari.org/deb precise main
```

Il faut ensuite mettre la liste des paquets disponibles à jour avec la commande `apt-get update` .

Dysfonctionnement des agents suite à un changement d'architecture

En allant sur la page des statistiques de surveillance d'un serveur (EAD ou Application Zéphir), j'obtiens

un message du type `rrdtool.error: This RRD was created on another architecture`

Ce problème peut survenir en cas de réinstallation des données d'un serveur 32 bits sur un serveur 64 bits (ou inversement).



Une solution consiste à supprimer les fichiers de statistiques :

- Statistiques propres au serveur Zéphir

Concerne les statistiques de Zéphir lui-même, pour les statistiques des serveurs clients, l'erreur doit être corrigée sur le client (voir cas suivant).

```
# service zephir stop
# rm -rf /var/lib/zephir/data/0/*
# service zephir start
```

- Sur un module EOLE autre que Zéphir

```
# service z_stats stop
# rm -rf /usr/share/zephir/monitor/data/*
# rm -rf /usr/share/zephir/monitor/stats/*
# service z_stats start
```



Si perdre les statistiques pose problème, il est possible de convertir les fichiers `.rrd` avec l'outil `rrdtool`.

Depuis l'ancien serveur, pour convertir les fichiers RRD vers des fichiers XML avec la commande `dump` :

```
# rrdtool dump stats.rrd > stats.xml
```

Après les avoir transférés sur le nouveau serveur il faut les convertir en RRD avec la commande `restore` :

```
# rrdtool restore -f stats.xml stats.rrd
```

Le serveur peut maintenant lire le fichier. Vous pouvez le tester avec la commande `info` :

```
# rrdtool info stats.rrd
```

Attention, il y a un (ou plusieurs) fichier par agent.

Exemple sur un serveur Zéphir :

```
root@zephir:~# ls -l /var/lib/zephir/data/0/*/*.rrd -rw-r--r-- 1
root root 11464 août 31 14:51
/var/lib/zephir/data/0/bastion/status.rrd -rw-r--r-- 1 root root
17032 août 31 15:27 /var/lib/zephir/data/0/bilan/status.rrd
-rw-r--r-- 1 root root 13576 août 31 15:26
/var/lib/zephir/data/0/debsums/status.rrd -rw-r--r-- 1 root root
1000 août 31 14:51 /var/lib/zephir/data/0/diag/status.rrd
-rw-r--r-- 1 root root 13576 août 31 15:26
/var/lib/zephir/data/0/diskspace /status.rrd
[...]
```

Si vous voulez convertir un répertoire entier en XML, utilisez ce petit script bash :

```
# for f in *.rrd; do rrdtool dump ${f} > ${f}.xml; done
```

S o u r c e :

<http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite>

Comment débloquent les messages en file d'attente ?

Un nombre de messages apparaissent comme étant *Frozen* dans le retour de la commande `diagnose`.

```
*** Messagerie
. Courrier SMTP => Ok
. File d'attente => 1 message(s)
. Messages "Frozen" => 1 message(s)
```



Une solution consiste à récupérer les identifiants des messages :

```
root@scribe:~# exim4 -bp
10h 2.5K 1abJaX-00036S-Bu <> *** frozen ***
touser@ac-test.fr
```

Il est ensuite possible de récupérer les journaux spécifiques message par message :

```
root@scribe:~# exim4 -Mvl 1abJaX-00036S-Bu
2016-03-03 04:06:05 Received from <> R=1abJaX-00036L-8j
U=Debian-exim P=local S=2525
2016-03-03 04:06:05 SMTP error from remote mail server after RCPT
TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr
[192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address
rejected: Access denied
2016-03-03 04:06:05 touser@ac-test.fr R=satellite_route
T=remote_smtp: SMTP error from remote mail server after RCPT
TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr
[192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address
rejected: Access denied
*** Frozen (delivery error message)
```

Dans cet exemple, le message d'erreur est `Recipient address rejected: Access denied`, l'expéditeur n'est pas autorisé à transiter par la passerelle configurée dans l'interface de configuration du module.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
1 root@eole:~# manage_schedule -l
2 Tâches planifiées EOLE :
3 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
4 - après sauvegarde
5 + Mise à jour du serveur (majauto)
6 root@eole:~#
```



Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
1 root@eole:~# rm /etc/eole/extra/schedule/config.eol
2 rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
3 root@eole:~# manage_schedule -l
4 Tâches planifiées EOLE :
5 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
6 - après sauvegarde
7 + Mise à jour du serveur (majauto)
8 root@eole:~#
```

Le proxy empêche les mises à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le blocage de certaines mises à jour aussi, la déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon.

```
1 root@scribe:~# Maj-Auto
2 Mise à jour le lundi 20 mars 2017 11:47:52
3 *** scribe 2.6.1 ***
4
5 Maj-Auto - (VERSION CANDIDATE) - Augmenter le niveau de mise à jour peut empêcher de
  revenir au niveau de mise à jour stable.
6 Voulez-vous continuer ? [oui/non]
7 [non] : oui
8 pyeole.pkg - Pas de configuration du miroir Ubuntu avec eole.ac-dijon.fr qui semble
  inaccessible : Impossible d'obtenir la version pour le dépôt :
  http://eole.ac-dijon.fr/ubuntu/dists/xenial/main/binary-amd64/Release
9 pyeole.pkg - Pas de configuration du miroir Ubuntu avec ftp.crihan.fr qui semble
  inaccessible : Impossible d'obtenir la version pour le dépôt :
  http://ftp.crihan.fr/ubuntu/dists/xenial/main/binary-amd64/Release
10 Maj-Auto - Impossible de configurer les sources APT pour Ubuntu
```



La déclaration du proxy s'effectue dans l'onglet **Général** de l'interface de configuration du module, passer **Utiliser un serveur mandataire (proxy) pour accéder à Internet** à **oui** et paramétrer l'adresse du proxy dans le champ **Nom ou adresse IP du serveur proxy**.



Pour effectuer les mises à jour d'un module qui n'est pas encore instancié, il faut configurer manuellement la variable d'environnement :

```
# export http_proxy=http://<adresseProxy>:<portProxy>
# Maj-Auto
```

Comment lister les services gérés par CreoleService

Il peut être utile de lister les services qui sont gérés par CreoleService.



Une astuce consiste à utiliser la commande `CreoleGet .containers.services|grep \.name=`


```

1 root@eolebase:~# CreoleGet .containers.services|grep \.name=
2 service0.name="networking"
3 service1.name="cron"
4 service10.name="exim4"
5 service11.name="eoleflask"
6 service12.name="nginx"
7 service13.name="ead3"
8 service14.name="genconfig"
9 service15.name="bastion"
10 service16.name="z_stats"
11 service2.name="rng-tools"
12 service3.name="ntp"
13 service4.name="nut-server"
14 service5.name="salt-api"
15 service6.name="salt-master"
16 service7.name="salt-minion"
17 service8.name="ead-server"
18 service9.name="ead-web"
19 root@eolebase:~#

```

Résoudre des dysfonctionnements liés à l'EAD

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation du fichier journal `/var/log/ead/ead-server.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```

1 service ead-server stop
2 cd /tmp
3 export PYTHONPATH=/usr/share
4 twistd -noy /usr/share/ead2/backend/eadserver.tac

```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

Si c'est le service `ead-web` qui est en erreur et que le fichier journal `/var/log/ead/ead-web.log` n'apporte pas d'informations pertinentes, le service peut être lancé manuellement à l'aide des commandes suivantes :

```

1 service ead-web stop
2 cd /tmp
3 export PYTHONPATH=/usr/share
4 twistd -noy /usr/share/ead2/frontend/frontend.tac

```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

2. Questions fréquentes propres au module Amon

Vider le cache du proxy

Vider le répertoire cache de Squid

Il faut arrêter le service Squid, supprimer les fichiers, re-générer l'arborescence du cache et redémarrer le service.

```

# service squid3 stop
# rm -rf $(CreoleGet cache_dir)/*

```



```
# squid3 -f /etc/squid3/squid.conf -z -N
# service squid3 start
```

💡 Vider le répertoire cache de la seconde instance de Squid

Il faut arrêter le second service Squid, supprimer les fichiers, re-générer l'arborescence du cache et redémarrer le service.

```
# service squid3-2 stop
# rm -rf $(CreoleGet cache_dir_2)/*
# squid3 -f /etc/squid3/squid2.conf -z -N
# service squid3-2 start
```

Problèmes avec le protocole HTTPS



La règle de pare-feu par défaut redirige le trafic Internet directement vers le proxy local.

C'est le mécanisme de proxy transparent.

Cette méthode ne permet toutefois pas de laisser passer le flux chiffré (HTTPS) par ce même mécanisme.

Pour accéder aux sites en HTTPS, il est nécessaire de configurer le proxy sur les postes clients (par exemple : avec ESU sur le module Scribe).



L'option Destinations non redirigées sur le proxy disponible en mode expert dans l'onglet Interface-1 permet, à l'inverse, de déclarer des exceptions.

Lenteur lors de la navigation web

Un filtrage web e2guardian est en place et la navigation web est très lente.

Dans les logs apparaissent des erreurs Squid à répétition (TCP_DENIED/407) :

```
Mar 01 10:36:01 amon (squid): 1363253761.503 51 192.168.10.10
TCP_DENIED/407 4006 GET http://linuxfr.org/ - NONE/- text/html
```



💡 Augmenter le nombre de processus e2guardian maximum dans le filtre

Avant d'augmenter le nombre de processus, on peut vérifier la valeur configurée dans l'interface de configuration du module. Celle-ci est fixée à 256 par défaut et se trouve dans l'onglet Filtrage web en mode expert.

Une commande rudimentaire permet de se rendre compte du nombre de processus effectivement exécutés sur le serveur mais elle ne permet pas de distinguer à quelle instance appartiennent les processus et renvoie aussi les processus qui servent à contrôler les autres processus :

```
# ps ax | grep -c guardian
```

La commande diagnose permet de connaître précisément le nombre de processus e2guardian exécutés par instance :

```
*** Filtre web
```

```
admin: test-eole.ac-dijon.fr => Ok
pedago: test-eole.ac-dijon.fr => Ok
dmz-priv: test-eole.ac-dijon.fr => Ok
. Nb instances 1 => 15/256
```

Si la commande renvoie un nombre trop proche voir supérieur à la valeur configurée dans l'interface de configuration du module, elle doit être augmentée. La valeur maximum est 8192.



Il est fortement recommandé de ne pas dépasser la valeur maximum de 8192 processus.

Glossaire

Agent Zéphir	<p>Les agents Zéphir sont des sondes qui génèrent divers statistiques et rapports sur les modules EOLE.</p> <p>Sur un module, elles sont consultables en HTTP sur le port 8090. Elles sont également accessibles via la page d'accueil de l'interface d'administration EAD.</p> <p>Si le module est enregistré sur un serveur Zéphir, ces données sont remontées à intervalles réguliers et sont susceptibles de générer des alertes centralisées dans l'interface web Zéphir.</p>
AGRIATES <i>= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires</i>	<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. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE.</p> <p>http://www.igc.education.fr/agriates/agriates.htm</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. 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>
AMD64	<p>AMD64 est le nom d'une architecture processeur développée par la société AMD.</p>

	Cette architecture est compatible avec le standard 32 bits x86 d'Intel.
ANSSI <i>= Agence nationale de la sécurité des systèmes d'information</i>	<p>Service à compétence nationale, l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale.</p> <p>Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.</p> <p>Source : https://www.cert.ssi.gouv.fr/a-propos/</p>
Anti-spoofing <i>= Anti-usurpation d'adresse IP</i>	<p>L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.</p> <p>L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.</p>
APT <i>= Advanced Packaging Tool</i>	<p>APT est un ensemble d'outils fondamentaux au cœur de Debian.</p> <p>Il permet :</p> <ul style="list-style-type: none"> • d'installer des applications ; • de supprimer des applications ; • de garder les applications à jour ; • et encore bien d'autres choses... <p>APT, qui essentiellement résout les problèmes de dépendances et récupère les paquets désirés, fonctionne avec <code>dpkg</code>, un autre outil qui réalise l'installation réelle ou la suppression des paquets (applications). APT est très puissant, et est essentiellement utilisé en ligne de commande.</p>
ARV <i>= Administration de Réseaux Virtuels</i>	<p>ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan.</p> <p>http://www.strongswan.org/</p>
Backbone.js	<p>Backbone est une bibliothèque JavaScript avec une interface RESTful JSON et est basée sur le modèle-vue-contrôleur (MVC). Cette bibliothèque est connu pour être légère, comme sa seule dépendance avec la bibliothèque JavaScript Underscore.js. Elle est conçu pour développer des applications web d'une seule page et permet de maintenir les différentes parties d'applications Web (par exemple, les clients multiples et le serveur) synchronisée. Backbone a été créé par Jeremy Ashkenas, qui est également connu pour CoffeeScript.</p> <p>http://backbonejs.org/</p>
Balise méta	Information sur la nature et le contenu d'une page web, ajoutée dans l'en-tête de la page HTML.
Bareos	

	<p>Bareos est un ensemble de programmes qui permet de gérer les sauvegardes, les restaurations ou la vérifications de données d'un ordinateur sur un réseau hétérogène.</p> <p>En termes techniques, il s'agit d'un programme de sauvegarde client/serveur. Il est relativement facile d'utilisation et efficace. Il offre de nombreuses fonctions avancées de gestion de stockage qui facilitent la recherche et la restauration de fichiers perdus ou endommagés.</p>
bastion	<p>bastion est un service qui récupère les règles par défaut des zones réseaux utilisées par le module ainsi que toutes les règles personnalisées :</p> <ul style="list-style-type: none"> • les règles optionnelles de l'EAD ; • les postes et les groupes de postes interdits ou restreints dans l'EAD ; • les règles sur les horaires de l'EAD ; • les règles ipsets (exceptions sur une directive) ; • les règles de la QOS ; • les règles tcpwrapper (host allow et hosts deny). <p>Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu.</p> <p>La liste des actions du service se trouve dans le script <code>/usr/share/era/bastion.sh</code>.</p> <p>Le service bastion met en cache les règles mais ne les régénère pas à chaque fois.</p> <p>À partir de la version 2.6.1, seules les commandes <code>reconfigure</code> et <code>bastion regen</code> régénèrent les règles.</p>
BIND = Berkeley Internet Name Domain	<p>BIND est un serveur DNS libre. C'est le plus utilisé sur Internet.</p> <p>http://www.isc.org/downloads/bind/</p>
broadcast	<p>le broadcast désigne une méthode de transmission de données à l'ensemble des machines d'un réseau.</p> <p>Les protocoles de communications réseau prévoient une méthode simple pour diffuser des données à plusieurs machines en même temps (multicast). Au contraire d'une communication « Point à Point » (unicast), il est possible d'adresser des paquets de données à un ensemble de machines d'un même réseau uniquement par des adresses spécifiques qui seront interceptées par toutes les machines du réseau ou sous-réseau.</p> <p>Source : http://fr.wikipedia.org/wiki/Broadcast_(informatique)</p>
CETIAD	<p>DSI de l'académie de Dijon en charge l'informatisation des services académiques et des établissements des 1er et 2nd degré nommée ainsi jusqu'au déménagement du service de la rue Berbisey à la rue</p>

<p>= <i>Centre d'Études et de Traitements Informatiques de l'Académie de Dijon</i></p>	<p>du Général Delaborde dans les nouveaux locaux du rectorat de l'académie de Dijon.</p>
<p>CIDR = <i>Classless Inter-Domain Routing</i></p>	<p>La notation CIDR permet de diminuer la taille de la table de routage contenue dans les routeurs.</p> <p>Elle donne le numéro du réseau suivi par une barre oblique (/) et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0).</p> <p>Source : http://fr.wikipedia.org/wiki/Sous-réseau</p>
<p>Cntlm</p>	<p>Cntlm proxy d'authentification NTLM rapide écrit en C.</p> <p>Il s'intercale entre le poste client et le proxy. Il oblige l'utilisateur à renseigner son identifiant/mot de passe dans une fenêtre surgissante (popup).</p> <p>Il ouvre une socket en écoute et gère la transmission de chaque requête au proxy parent. Si une connexion au proxy parent est créée à nouveau et authentifiée, la connexion précédente est mise en cache et est réutilisée pour une plus grande efficacité. Cntlm intègre également la redirection transparente de port TCP/IP. Il existe de nombreuses fonctions avancées telles que le support de NTLMv2, la protection de mot de passe, le hachage de mot de passe, etc. Il est peu gourmand en terme de ressources.</p> <p>http://cntlm.sourceforge.net/</p>
<p>Conteneur = <i>LXC</i></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.</p> <p>Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.</p>
<p>Corosync Cluster Engine = <i>Corosync</i></p>	<p>Corosync Cluster Engine est un moteur libre de cluster. C'est un système de communication avec des fonctionnalités supplémentaires pour la mise en œuvre de la haute disponibilité dans les applications.</p> <p>Le projet fournit quatre fonctionnalités principales :</p> <ul style="list-style-type: none"> • un groupe restreint de processus avec une garantie de synchronisation virtuelle afin de créer des machines à états répliquées ; • un simple gestionnaire de disponibilité qui redémarre les processus d'application lorsqu'ils ont échoués ; • une configuration et des statistiques stockées en base de données dans la mémoire vive permet de définir, de récupérer et de recevoir des notifications concernant les changements d'état ;

	<ul style="list-style-type: none"> • un système de notification qui se déclenche lorsque un quorum est atteint ou perdu. <p>Sources : https://fr.wikipedia.org/wiki/Corosync_Cluster_Engine et http://clusterlabs.org/</p>
CPU <i>= Central Processing Unit</i>	Le CPU , ou en français UCT pour Unité Centrale de Traitement, désigne le ou les microprocesseurs d'un ordinateur. C'est lui qui exécute les programmes informatiques.
Creole <i>= Création EOLE</i>	Creole gère la personnalisation des options de configuration des modules, le redémarrage des services, l'installation de paquets additionnels, la mise à jour du système. Il a été conçu pour être facilement personnalisable pour l'utilisateur final. Un ensemble d'outils est proposé pour modifier ou étendre les fonctionnalités offerte par EOLE.
CRL	Acronyme : Certificate Revocation List Une CRL ou Liste de Certificats Révoqués (LCR) est une liste, datée et signée par une Autorité de Certification, des numéros de série des certificats révoqués (mis en opposition) et non expirés, mise à jour périodiquement.
cron	cron est un programme qui permet aux utilisateurs des systèmes Unix d'exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiées à l'avance, ou selon un cycle défini à l'avance.
CSV <i>= Comma-separated values</i>	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.
DHCP <i>= Dynamic Host Configuration Protocol</i>	Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut et des serveurs de noms DNS.
Dictionnaire Creole	Fichier, au format XML, décrivant l'ensemble de variables, de fichiers, de services et de paquets personnalisés en vue de configurer un serveur.
Directive optionnelle	Directive paramétrée dans ERA et qui peut être activée ou désactivée depuis une autre interface. Les directives optionnelles le sont depuis l'EAD et les directives optionnelles cachées le sont par l'intermédiaire du template Creole <code>active_tags</code> des modules Amon et AmonEcole.
Distribution	Une distribution GNU/Linux est un ensemble cohérent de logiciels rassemblant un système d'exploitation composé d'un noyau Linux et d'applications, la plupart étant des logiciels libres.

DKMS = <i>Dynamic Kernel Module Support</i>	DKMS est un framework utilisé pour créer des modules noyau dont les sources ne résident pas dans celles du noyau Linux.
DMZ = <i>Demilitarized Zone</i>	<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 : http://fr.wikipedia.org/wiki/Zone_démilitarisée_(informatique)</p>
DNS = <i>Domain Name System</i>	<p>Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types.</p> <p>L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP.</p> <p>Source : http://fr.wikipedia.org/wiki/Dns</p>
DTD = <i>Document Type Definition</i>	<p>La Définition de Type de Document, est un document permettant de décrire un modèle de document SGML ou XML. Le modèle est décrit comme une grammaire de classe de documents : grammaire parce qu'il décrit la position des termes les uns par rapport aux autres, classe parce qu'il forme une généralisation d'un domaine particulier, et document parce qu'on peut former avec un texte complet.</p> <p>Une DTD décrit les documents à deux niveaux :</p> <ul style="list-style-type: none"> • la structure logique, que l'on peut assimiler à la syntaxe abstraite ; • la structure physique, que l'on peut assimiler à la syntaxe concrète. <p>Source : http://fr.wikipedia.org/wiki/Document_Type_Definition</p>
e2guardian	<p>e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie.</p> <p>Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian.</p> <p>http://e2guardian.org</p>
EAD	<p>L'EAD est l'interface d'administration des modules EOOLE. Il s'agit</p>

<p>= <i>EOLE ADmin</i></p>	<p>d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse <a href="https://<adresse_module>:4200">https://<adresse_module>:4200. L'authentification peut être locale et/ou au travers d'EoleSSO (authentification unique). L'EAD est composé de deux parties :</p> <ul style="list-style-type: none"> • un serveur de commandes (service ead-server), présent et actif sur tous les modules ; • une interface web (service ead-web), présent et actif sur tous les modules. <p>Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, ...) ne disposent que de la version de base qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...). Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.</p>
<p>ELF = <i>Executable and Linkable Format</i></p>	<p>ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé</p>
<p>Envole</p>	<p>Envole est un Espace Numérique Personnel pour l'Éducation. Il propose une interface de type portail Web 2.0 qui permet l'interaction entre un utilisateur et son environnement numérique résultant de l'utilisation de services hétérogènes. Il centralise dans une seule interface l'ensemble des applications de l'utilisateur : mail, agenda, dossier personnel, B2I, blog, gestion de notes, gestion des absences, etc ... Envole est adapté pour mettre en œuvre un Portail Internet Académique (PIA), un Portail Internet Établissement (PIE) ou un Espace Numérique de Travail (ENT). http://envole.ac-dijon.fr/</p>
<p>ERA = <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>Erlang</p>	<p>Erlang est un langage de programmation, supportant plusieurs paradigmes : concurrent, temps réel, distribué. Son cœur séquentiel est un langage fonctionnel à évaluation stricte, affectation unique, au typage dynamique fort. Sa couche concurrente est fondée sur le modèle d'acteur. Il possède des fonctionnalités de tolérance aux pannes et de mise à jour du code à chaud, permettant le développement d'applications à très haute disponibilité. Erlang est</p>

	<p>conçu pour s'exécuter sur une machine virtuelle spécifique appelée BEAM.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Erlang_%28langage%29</p>
<p>ESU = <i>Environnements</i> <i>Sécurisés des Utilisateurs</i></p>	<p>Environnement Sécurisé des Utilisateurs (ESU) est un projet initialement développé par Olivier Adams du CRDP de Bretagne qui est maintenant publié par EOLE et distribué sous licence CeCILL. Cet outil permet aux administrateurs de réseaux en établissement scolaire de définir (très simplement) les fonctions laissées disponibles aux utilisateurs des postes informatiques.</p> <p>ESU propose de nombreuses fonctions :</p> <ul style="list-style-type: none"> • limitation des accès aux paramètres de Windows (panneau de configuration...) ; • définition par salle ou par poste des lecteurs réseaux, icônes du bureau, menu démarrer et limitation des fonctions ; • configuration des imprimantes partagées sur les postes ; • configuration des navigateurs (Internet Explorer et Mozilla Firefox) ; • éditeur de règles permettant de rajouter autant de règles que vous le souhaitez.
Extrémité	<p>Une extrémité est un sous ensemble d'une zone. Elle est définie par une ou plusieurs adresses IP ou bien un sous-réseau. Elle hérite du niveau de sécurité de la zone à laquelle elle appartient.</p>
Filtrage syntaxique	<p>Système de pondération détectant des mots interdits dans une page et lui assignant un score en fonction de la gravité et du nombre de mots détectés. Le proxy bloquera les pages dont le score dépasse un certain seuil.</p>
Flask	<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. http://flask.pocoo.org/</p>
Flux	<p>Lien entre deux zones.</p>

Flux descendant	Interactions d'un niveau de sécurité plus fort vers un niveau de sécurité plus faible avec une politique par défaut "autorisé".
Flux montant	Interactions d'un niveau de sécurité plus faible vers un niveau de sécurité plus fort avec une politique par défaut "interdit".
FTP = <i>File Transfert Protocol</i>	<p>File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.</p> <p>La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS.</p> <p>FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).</p> <p>FTP, qui appartient à la couche application du modèle OSI et du modèle ARPA, utilise une connexion TCP.</p> <p>Par convention, deux ports sont attribués (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990.</p> <p>Ce protocole peut fonctionner avec IPv4 et IPv6.</p> <p>(Source : http://fr.wikipedia.org/wiki/File_Transfer_Protocol)</p>
Gaspacho	Gaspacho est une application qui permet de configurer automatiquement le poste de travail de l'utilisateur selon son profil. Pour le moment il n'existe que la version GNU/Linux du client Gaspacho.
GNU = <i>GNU is Not Unix</i>	<p>GNU est l'acronyme récursif de GNU is Not Unix. Projet fondé en 1984, il vise à produire un OS complet de type Unix.</p> <p>Le noyau propre au projet n'étant pas fini, GNU est le plus souvent utilisé avec Linux. On parle alors de système GNU/Linux.</p>
GNU GRUB = <i>GRand Unified Bootloader</i>	GNU GRUB est un programme d'amorçage de micro-ordinateur. Il s'exécute à la mise sous tension de l'ordinateur, après les séquences de contrôle interne et avant le système d'exploitation proprement dit, puisque son rôle est justement d'en organiser le chargement. Lorsque le micro-ordinateur héberge plusieurs systèmes (on parle alors de multi-amorçage), il permet à l'utilisateur de choisir quel système démarrer.

	Source : http://fr.wikipedia.org/wiki/GRand_Unified_Bootloader
GPG = <i>GnuPG</i>	GPG est l'implémentation GNU du standard OpenPGP. OpenPGP est un format pour l'échange sécurisé de données. http://fr.wikipedia.org/wiki/GNU_Privacy_Guard
Gunicorn = <i>Green Unicorn (Licorne Verte)</i>	Gunicorn est un serveur Web HTTP WSGI écrit en Python et disponible pour Unix. Son modèle d'exécution est basé sur des sous-processus créés à l'avance, adapté du projet Ruby Unicorn. Le serveur Gunicorn est compatible avec un large nombre de frameworks Web, repose sur une implémentation simple, légère en ressources et relativement rapide. Source Wikipédia : http://fr.wikipedia.org/wiki/Gunicorn_(HTTP_server)
Haute Disponibilité = <i>High Availability ou HA</i>	La haute disponibilité c'est garantir la disponibilité et le bon fonctionnement d'un service ou d'une architecture informatique. Deux moyens complémentaires sont utilisés pour améliorer la haute disponibilité : <ul style="list-style-type: none"> • la mise en place d'une infrastructure matérielle spécialisée, généralement en se basant sur de la redondance matérielle. Est alors créé un cluster de haute-disponibilité (par opposition à un cluster de calcul) : une grappe d'ordinateurs dont le but est d'assurer un service en évitant au maximum les indisponibilités ; • la mise en place de processus adaptés permettant de réduire les erreurs, et d'accélérer la reprise en cas d'erreur. ITIL contient de nombreux processus de ce type. Source Wikipédia : http://fr.wikipedia.org/wiki/Haute_disponibilité
HTTP = <i>HyperText Transfer Protocol - protocole de transfert hypertexte</i>	HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (le S signifiant sécurisé) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS. HTTP est un protocole de la couche application. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).
ICMP = <i>Internet Control Message Protocol</i>	Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
Image ISO = <i>Image disque</i>	Une image ISO est une archive proposant la copie conforme d'un disque optique ou magnétique. L'opération de gravure de l'image ISO consiste à recopier cette structure sur un disque optique.
INI	Un fichier INI est un fichier de configuration dans un format de données introduit par les systèmes d'exploitation Windows en 1985.

	<p>Par convention les noms de ces fichiers portent l'extension « <code>.ini</code> ».</p> <p>Les fichiers INI sont des fichiers texte qui peuvent être manipulés avec un logiciel courant de type éditeur de texte.</p> <p>La valeur de chaque paramètre de configuration est indiquée par une formule : paramètre = valeur.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Fichier_INI</p>
<p>instance = <i>instanciation, instancier</i></p>	<p>Instancier un serveur correspond à la troisième étape de mise en œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande <code>instance</code>.</p>
<p>InterBase</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 : http://fr.wikipedia.org/wiki/InterBase</p>
<p>iptables</p>	<p>iptables est un logiciel libre grâce auquel l'administrateur système peut configurer les chaînes et règles dans le pare-feu dans l'espace noyau composé par des modules Netfilter.</p> <p>Netfilter est un framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches (hooks) dans le noyau pour l'interception et la manipulation des paquets réseau lors des appels des routines de réception ou d'émission des paquets des interfaces réseau.</p>
<p>IPv6 = <i>Internet Protocol version 6</i></p>	<p>L'IPv6 est un protocole réseau sans connexion de la couche 3 du modèle OSI. IPv6 est le successeur d'IPv4.</p> <p>Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire.</p> <p>IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. Les mécanismes de sécurité comme IPsec font partie des spécifications de base du protocole. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés.</p>
<p>JSON = <i>JavaScript Object Notation</i></p>	<p>JSON est un format de données textuelles dérivé de la notation des objets du langage JavaScript. Il permet de représenter de l'information structurée comme le permet XML par exemple.</p>

	<p>Un document JSON a pour fonction de représenter de l'information accompagnée d'étiquettes permettant d'en interpréter les divers éléments, sans aucune restriction sur le nombre de celles-ci.</p> <p>Un document JSON ne comprend que deux types d'éléments structurels :</p> <ul style="list-style-type: none"> • des ensembles de paires nom / valeur ; • des listes ordonnées de valeurs. <p>Ces mêmes éléments représentent trois types de données :</p> <ul style="list-style-type: none"> • des objets ; • des tableaux ; • des valeurs génériques de type tableau, objet, booléen, nombre, chaîne ou null. <p>Source Wikipédia : http://fr.wikipedia.org/wiki/JavaScript_Object_Notation</p>
L'expérience à tâtons	Ne pouvant établir avec certitude qui de l'équipe a introduit ce type d'expérience dans la documentation du module Amon en version 2.2, l'équipe dans son intégralité revendique la paternité du concept.
LDAP = <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.
Licence CeCILL	Acronyme pour CEa Cnrs Inria Logiciel Libre. C'est une licence libre de droit français compatible avec la licence GNU GPL.
Linux = <i>Kernel Linux</i>	Le noyau Linux est un noyau de système d'exploitation de type Unix. Le noyau Linux est un logiciel libre développé initialement par Linus Torvalds. Il a officiellement vu le jour en 1991. Formellement, « Linux » est le nom du seul noyau, mais dans les faits, on appelle souvent « Linux » l'ensemble du système d'exploitation, aussi appelé « GNU/Linux », voire l'ensemble d'une distribution Linux.
Liste blanche	Une liste blanche est une liste d'adresse web autorisées par le proxy.
Liste noire	Une liste noire est un document rassemblant les noms d'entités concrètes ou virtuelles jugés indésirables. Dans le contexte informatique une liste noire est une liste d'adresses web indésirables qui seront bloquées par le proxy.
LTS = <i>Long Term Support</i>	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 : <ul style="list-style-type: none"> • la récupération des paquets de Debian se fait de manière plus conservatrice, synchronisée depuis Debian testing plutôt que

	<p>Debian unstable ;</p> <ul style="list-style-type: none"> • 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. <p>Une version LTS est :</p> <ul style="list-style-type: none"> • 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. <p>Clairement, une version LTS n'est pas :</p> <ul style="list-style-type: none"> • 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.
<p>LVM = <i>Logical Volume Management</i></p>	<p>La gestion par volumes logiques est à la fois une méthode et un logiciel. Elle permet le découpage, la concaténation, le redimensionnement et l'utilisation des espaces de stockage. Le logiciel permet de gérer, de sécuriser et d'optimiser de manière souple les espaces de stockage sur les systèmes d'exploitation de type UNIX.</p>

<p>LXC = <i>Linux Containers</i></p>	<p>LXC, contraction de l'anglais Linux Containers, est un système de virtualisation au niveau système d'exploitation utilisé pour faire fonctionner de multiples environnements Linux isolés les uns des autres sur un seul et même système hôte. Le conteneur LXC n'est pas une machine virtuelle mais uniquement un environnement virtualisé qui dispose de ses propres processus et de son propre réseau (isolés du système physique hôte).</p>
<p>Marionette</p>	<p>Marionette simplifie le code applicatif Backbone grâce à des vues robustes et des solutions d'architecture. http://marionettejs.com/</p>
<p>MD5 = <i>Message Digest 5</i></p>	<p>L'algorithme MD5 est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier. Il a été inventé par Ronald Rivest en 1991. Source : https://fr.wikipedia.org/wiki/MD5</p>
<p>MEEM = <i>Ministère de l'Environnement, de l'Énergie et de la Mer</i></p>	<p>Le ministère de l'Environnement, de l'Énergie et de la Mer est l'administration française chargée de préparer et mettre en œuvre la politique du Gouvernement dans les domaines du développement durable, de l'environnement et des technologies vertes, de la transition énergétique et de l'énergie, du climat, de la prévention des risques naturels et technologiques, de la sécurité industrielle, des transports et de leurs infrastructures, de l'équipement et de la mer. Il est dirigé par le ministre de l'Environnement, de l'Énergie et de la Mer, membre du gouvernement français.</p> <p>Né de la fusion, en 2007, du Ministère de l'Environnement et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer il a depuis changé plusieurs fois de nom et de compétences :</p> <ul style="list-style-type: none"> • Ministère de l'Écologie, du Développement et de l'Aménagement durables (2007-2010) Le ministère de l'Écologie, du Développement et de l'Aménagement durables (MEDAD) naît ainsi de la fusion du Ministère de l'Écologie et du Développement durable et du Ministère des Transports, de l'Équipement, du Tourisme et de la Mer. Il intègre également l'énergie, qui relevait alors du ministère de l'économie. • Ministère de l'Écologie, du Développement durable, des Transports et du Logement (2010-2012) Le ministère devient le Ministère de l'Écologie, du Développement durable, des Transports et du Logement (MEDDTL) et perd au passage ses compétences sur l'énergie, exception faite des énergies renouvelables. • Ministère de l'Écologie, du Développement durable et de l'énergie (2012-2016) Le Ministère de l'Écologie, du Développement durable et de

	<p>l'énergie (MEDDE) assemble des fonctions historiquement séparées dans différents ministères : l'écologie (ministère de l'écologie et du Développement durable) et l'énergie (auparavant rattachée au ministère de l'industrie).</p> <ul style="list-style-type: none"> Ministère de l'Environnement, de l'Énergie et de la Mer (depuis 2016) <p>Le ministère devient Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM) et est chargée des relations internationales sur le climat.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Minist%C3%A8re_de_l'Environnement_de_la_Mer http://fr.wikipedia.org/wiki/Liste_des_ministres_fran%C3%A7ais_des_Affaires_Ext%C3%A9rieures</p>
Modèle	<p>ERA enregistre la description d'un pare-feu dans un fichier XML situé par défaut dans un répertoire nommé <code>/usr/share/era/modeles/</code>.</p> <p>Ce fichier est souvent dérivé d'un modèle livré de base, fichiers de référence présent dans le dossier <code>/usr/share/era/modeles</code> sur lequel se base l'utilisateur. Par extension, un modèle est n'importe quel fichier de description de pare-feu dans ERA.</p>
MTU = <i>Maximum Transmission Unit</i>	<p>Le MTU définit la taille maximum d'un paquet (en octets) pouvant être transmis sur le réseau sans fragmentation.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit</p>
NAS = <i>Network Access Server</i>	<p>Un Network Access Server (NAS), ici un switch, fonctionne comme un client RADIUS.</p> <p>Au sein d'un réseau, le premier équipement qui prend en charge un client (machine ou utilisateur) est un équipement d'accès (switch, point d'accès Wifi). Ces équipements jouent un rôle crucial car ce sont eux qui détectent la présence d'un équipement qui essaye de rejoindre le réseau. Ils interviennent donc dans le processus d'authentification. Dans la terminologie RADIUS, ces équipements d'accès sont appelés NAS (Network Access Server), ou clients Radius : ce sont ces équipements qui interagissent avec le serveur RADIUS en utilisant le protocole du même nom. Ils devront d'ailleurs être configurés pour cela (ils doivent connaître l'adresse IP du serveur Radius).</p> <p>Source : http://juboite.hd.free.fr/doku.php?id=tuto:radius:freeradius</p>
NAT = <i>Network Address Translation</i>	<p>Le NAT est un mécanisme informatique permettant de faire communiquer un réseau local avec l'Internet.</p> <p>En réseau informatique, on dit qu'un routeur fait de la traduction d'adresse réseau lorsqu'il fait correspondre les adresses IP internes non-uniqes et souvent non routables d'un intranet à un ensemble d'adresses externes unques et routables.</p> <p>Ce mécanisme permet notamment de faire correspondre une seule</p>

	<p>adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Network_address_translation</p>
Netfilter	<p>Netfilter est un outil de filtrage de paquets sous linux. Le logiciel qui lui est associé est iptables.</p>
Nginx = <i>Engine-x</i>	<p>Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions.</p> <p>Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.</p>
Niveau de sécurité	<p>Nombre entier (entre 0 et 100) permettant d'ordonner les zones par ordre croissant.</p>
Nom de domaine	<p>Dans le système de noms de domaine, un nom de domaine (NDD en notation abrégée française ou DN pour Domain Name en anglais) est un identifiant de domaine internet.</p> <p>Un domaine est un ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune.</p> <p>Voici des exemples de domaine :</p> <p>le domaine .fr est l'ensemble des ordinateurs hébergeant des activités pour des personnes ou des organisations qui se sont enregistrées auprès de l'AFNIC qui est le registre responsable du domaine de premier niveau .fr ; en général, ces personnes ou ces entreprises ont une certaine relation (qui peut être tenue dans certains cas) avec la France ;</p> <p>le domaine paris.fr est l'ensemble des ordinateurs hébergeant des activités pour la ville de Paris.</p> <p>Un nom de domaine est un « masque » sur une adresse IP. Le but d'un nom de domaine est de retenir et communiquer facilement l'adresse d'un ensemble de serveurs (site web, courrier électronique, FTP...). Par exemple, wikipedia.org est plus simple à mémoriser que 91.198.174.2.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Nom_de_domaine</p>
NTLM	<p>NTLM est un protocole d'identification utilisé dans diverses</p>

<p>= <i>NT Lan Manager</i></p>	<p>implémentations des protocoles réseau Microsoft. Il est aussi utilisé partout dans les systèmes de Microsoft comme un mécanisme d'authentification unique SSO.</p>
<p>NTP = <i>Network Time Protocol</i></p>	<p>NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.</p>
<p>NUT = <i>Network UPS Tools</i></p>	<p>NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments :</p> <ul style="list-style-type: none"> • le démon <code>nut</code> lancé au démarrage du système ; • le démon <code>upsd</code> qui permet d'interroger l'onduleur, il est lancé sur le PC relié à l'onduleur ; • le démon <code>upsmmon</code> qui permet de monitorer et lancer les commandes nécessaires sur le réseau ondulé (arrêt de machines ...) ; • différents programmes pour envoyer des commandes manuellement à l'onduleur. <p><code>upsd</code> peut communiquer avec plusieurs onduleurs si nécessaire. <code>upsmmon</code> interroge à intervalle régulier la machine du réseau sur laquelle est lancée <code>upsd</code>.</p>
<p>OpenNebula</p>	<p>OpenNebula est un projet libre et européen qui fournit un ensemble de fonctionnalités permettant de gérer un nuage informatique. OpenNebula organise le fonctionnement d'un ensemble de serveurs physiques, fournissant des ressources à des machines virtuelles. Il orchestre et gère le cycle de vie de toutes ces machines virtuelles. http://opennebula.org/</p>
<p>OpenVZ</p>	<p>OpenVZ est une technique de virtualisation de niveau système d'exploitation basée sur le noyau Linux. Cette technique de virtualisation de niveau système d'exploitation est souvent appelée conteneurisation et les instances sont appelées conteneur. OpenVZ permet à un serveur physique d'exécuter de multiples instances de systèmes d'exploitation isolés, qualifiés de serveurs privés virtuels (VPS) ou environnements virtuels (VE). Source Wikipédia : https://fr.wikipedia.org/wiki/OpenVZ</p>
<p>OSPF = <i>Open Shortest Path First</i></p>	<p>Open Shortest Path First (OSPF) est un protocole de routage interne IP de type « à état de liens ».</p> <p>Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise</p>

	<p>ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB.</p> <p>Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire.</p> <p>En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Open_Shortest_Path_First</p>
<p>OTP = <i>One-time password</i></p>	<p>Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisés par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir.</p> <p>Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique</p>
<p>Pare-feu = <i>firewall</i></p>	<p>Un pare-feu est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique. Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent.</p> <p>Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).</p> <p>Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège.</p> <p>Le filtrage se fait selon divers critères.</p> <p>Les plus courants sont :</p> <ul style="list-style-type: none"> • 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 à un motif, etc.) ; • les utilisateurs pour les plus récents.

	Source Wikipédia : http://fr.wikipedia.org/wiki/Pare-feu_(informatique)
Patch	<p>Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à l'instance ou à chaque reconfigure.</p> <p>Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch.</p> <p>La procédure pour réaliser des patches est expliquée dans la rubrique Personnalisation du serveur à l'aide de Creole dans les documentations complètes ou dans la documentation partielle dédiée nommée PersonnalisationEOLEAvecCreole.</p>
PID <i>= Process Identifier</i>	<p>L'identifiant de processus ou PID est un code unique attribué sur les systèmes Unix ou Windows à tout processus lors de son démarrage. Il permet ainsi d'identifier le processus dans la plupart des commandes s'appliquant sur un processus donné (comme kill).</p> <p>Wikipédia : https://fr.wikipedia.org/wiki/Identifiant_de_processus</p>
Politique de filtrage	<p>Une politique de filtrage permet de définir une suite d'autorisation et d'interdiction dans les accès web.</p>
PPPoE <i>= Point-to-Point Protocol over Ethernet</i>	<p>PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP et du contrôle de la connexion (débit, etc.), sur un réseau 802.3.</p> <p>Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers, bien qu'une connexion utilisant un pont Ethernet-Ethernet soit souvent plus stable et plus performante. Il pose également des problèmes de MTU.</p>
Préfixe binaire	<p>Les préfixes binaires (kibi-, mébi-, gibi-, tébi-, pébi- et exbi-) sont souvent utilisés lorsqu'on a affaire à de grandes quantités d'octets. Ils sont dérivés, tout en étant différents, des préfixes du système international (kilo-, méga-, giga- et ainsi de suite). La raison d'être de ces préfixes binaires est d'éviter la confusion de valeur avec les préfixes du système international.</p> <p>http://fr.wikipedia.org/wiki/Préfixe_binaire</p>
Pronote	<p>Pronote est un logiciel privé de gestion de vie scolaire créé en 1999. C'est au départ un client lourd, mais il existe, depuis 2003, une extension permettant d'utiliser une version Web.</p>
Proxy sibling <i>= proxy frère</i>	<p>Hiérarchiquement, un cache interrogé peut être un de niveau supérieur (parent) ou de niveau égal (frère ou sibling).</p> <p>Les serveurs parents sont d'ordinaire plus proches du serveur hébergeant l'objet recherché que les serveurs fils. Si un serveur fils ne peut trouver l'objet, la requête est en général relayée vers un serveur de cache parent qui va rapporter, mémoriser (mettre en cache) et finalement transmettre la requête au demandeur.</p> <p>Les serveurs frères (siblings) sont des serveurs de cache d'un niveau</p>

	hiérarchique égal, dont le but est de répartir la charge. http://fr.wikipedia.org/wiki/Internet_Cache_Protocol
PUA <i>= Potentially Unwanted Applications</i>	Applications potentiellement indésirables.
PXE <i>= Pre-boot eXecution Environment</i>	L'amorçage PXE permet à une station de travail de démarrer depuis le réseau en récupérant une image de système d'exploitation qui se trouve sur un serveur. L'amorce par PXE s'effectue en plusieurs étapes : <ul style="list-style-type: none"> • recherche d'une adresse IP sur un serveur DHCP/BOOTP et recherche du fichier à amorcer ; • téléchargement du fichier à amorcer depuis un serveur Trivial FTP ; • exécution du fichier à amorcer.
Qualité de service <i>= QoS</i>	Régulation des flux du trafic sur un réseau, définition de Wikipedia ^[http://fr.wikipedia.org/wiki/QoS]
RADIUS <i>= Remote Authentication Dial-In User Service</i>	RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification. Source : http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
Ramsese <i>= Répertoire académique et ministériel sur les établissements du système éducatif</i>	Une base Ramsese est le fichier de gestion des établissements secondaires d'une académie : EPLE (établissements publics locaux d'enseignements) et EREA (établissements régionaux d'enseignements adaptés) publics et privés. Il contient toutes les informations concernant chaque établissement, notamment sa localisation, son code. Caractéristiques techniques : <ul style="list-style-type: none"> • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
RELP <i>= Reliable Event Logging Protocol</i>	Reliable Event Logging Protocol ou RELP est un protocole définissant un service de journaux d'événements d'un système informatique. Il est supporté entre autres par Rsyslog.
Réseau virtuel Privé <i>= RVP ou VPN (Virtual Private Network) en anglais</i>	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.
RIP <i>= Routing Information Protocol</i>	RIP, protocole d'information de routage, est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé. Il permet à chaque routeur de communiquer aux routeurs voisins la métrique,

	<p>c'est-à-dire la distance qui les sépare d'un réseau IP déterminé quant au nombre de sauts ou « hops » en anglais. Pour chaque réseau IP connu, chaque routeur conserve l'adresse du routeur voisin dont la métrique est la plus petite. Ces meilleures routes sont diffusées toutes les 30 secondes.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Routing_Information_Protocol</p>
<p>Round-robin = <i>tourniquet</i></p>	<p>Round-robin (RR) est un algorithme d'ordonnement courant dans les systèmes d'exploitation. Ce dernier attribue des tranches de temps à chaque processus en proportion égale, sans accorder de priorité aux processus.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Round-robin_(informatique)</p>
<p>SAML = <i>Security assertion markup language</i></p>	<p>SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.</p>
<p>Scannedonly</p>	<p>Scannedonly est composé d'un module VFS (Virtual File System) Samba et d'un service d'exploration qui garantissent que seuls les fichiers qui ont été scannés pour les virus sont visibles et accessibles à l'utilisateur final.</p> <p>http://olivier.sessink.nl/scannedonly/</p>
<p>SecurID</p>	<p>SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information.</p> <p>Source : http://fr.wikipedia.org/wiki/SecurID</p>
<p>Service</p>	<p>Couple protocole et/ou port (ou plage de ports).</p>
<p>SID = <i>Security Identifier</i></p>	<p>Le SID est un identifiant de sécurité utilisé pour identifier les ressources et les personnes sur un réseau Microsoft.</p> <p>Le SID d'un domaine se présente sous la forme <u>S-1-5-21-nnnnnnnnnnnn-nnnnnnnnnnnn-nnnnnnnnnnnn</u> .</p> <p>Chaque serveur de fichiers possède son propre SID et celui-ci est utilisé lors de la création des comptes (utilisateurs, groupes, machines rattachées au domaine).</p> <p>Lors de l'installation de module Scribe, Samba génère aléatoirement son propre SID.</p> <p>http://fr.wikipedia.org/wiki/Security_Identifier</p>
<p>SMTP = <i>Simple Mail Transfer Protocol</i></p>	<p>SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.</p>
	<p>Le secrétariat général pour la modernisation de l'action publique</p>

<p>Socle Interministériel de Logiciel Libre = <i>SILL</i></p>	<p>(SGMAP) relève du Premier ministre.</p> <p>L'un des services du SGMAP, la Direction Interministérielle des Systèmes d'Information et de Communication (DISIC), coordonne les administrations d'État en matière de systèmes d'information.</p> <p>L'instance DISIC en charge des logiciels libres préconise une sélection de logiciels, sous la forme d'un socle interministériel de logiciels libres (SILL).</p> <p>Le SILL propose des logiciels libres répondant aux besoins des administrations françaises. Il est mis à disposition sans garantie de l'État. Il peut être utilisé librement et gratuitement par tous, à titre public, professionnel ou privé. Il peut être copié et diffusé sans restriction.</p> <p>http://references.modernisation.gouv.fr/socle-logiciels-libres</p>
<p>Squid</p>	<p>Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.</p>
<p>SSH = <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>SSO = <i>Single Sign On, Authentification unique</i></p>	<p>SSO est une méthode permettant de centraliser l'authentification afin de permettre à l'utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques.</p> <p>Les objectifs sont :</p> <ul style="list-style-type: none"> • simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent ; • simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ; • simplifier la définition et la mise en œuvre de politiques de sécurité.
<p>StartTLS</p>	<p>Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas,</p>

	par exemple des protocoles de mails IMAP et SMTP ou LDAP.
strongSwan	strongSwan est une implémentation libre et complète de VPN IPsec pour le système d'exploitation Linux (noyaux Linux 2.6 et 3.x). L'objectif de ce projet est de proposer des mécanismes d'authentification forts. http://www.strongswan.org/
Swap = <i>Verbe échanger</i>	En informatique le swap sert à étendre la mémoire utilisable par un système d'exploitation, par un fichier d'échange ou une partition dédiée ; c'est aussi une instruction de certains processeurs et une fonction de certains langages de programmation qui permet l'échange de deux variables.
Tableaux de flux	Ensemble de lien entre les zones permettant de définir une politique par défaut et de classer un ensemble de règles (directives).
TCP = <i>Transmission Control Protocol</i>	TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport qui travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.
TCP Wrapper = <i>tcpd</i>	TCP Wrapper est une technique, propre à Unix, permettant de contrôler les accès à un service (ou démon) suivant la source. Il se configure grâce au deux fichiers <code>/etc/hosts.allow</code> et <code>/etc/hosts.deny</code> . Tous les démons ne supportent pas la technique TCP Wrapper.
Telnet = <i>TERminal NETwork ou TELecommunication NETwork</i>	Telnet est une commande permettant de créer une session Telnet sur une machine distante. Cette commande a d'abord été disponible sur les systèmes Unix, puis elle est apparue sur la plupart des systèmes d'exploitation. Telnet est un protocole réseau utilisé sur tout réseau prenant en charge le protocole TCP/IP. Le but du protocole Telnet est de fournir un moyen de communication très généraliste, bi-directionnel et orienté octet.
Template = <i>Modèle Creole</i>	Un template est un fichier contenant des variables Creole, qui sera instancié pour générer un fichier cible (typiquement un fichier de configuration serveur).
timeout	Le timeout est la durée de validité d'une donnée avant son expiration.
Tiramisu = <i>Outil de gestion de configuration</i>	À cause de l'afflux de plus en plus grand des options de configuration des serveurs EOLE (plus de 1600 au dernier recensement), il était devenu de plus en plus difficile de correctement récupérer les options et de les utiliser là où elles devaient effectivement être employées. Pour remédier à ces difficultés, l'outil Tiramisu a été développé, il est utilisé comme moteur du générateur de configuration de la version

	<p>EOLE 2.4.</p> <p>La documentation technique du projet : http://tiramisu.labs.libre-entreprise.org</p> <p>Les sources du projet Tiramisu : http://labs.libre-entreprise.org/projects/tiramisu/</p>
<p>TLS = <i>Transport Layer Security</i></p>	<p>Le TLS et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le TLS est la poursuite des développements de SSL. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.</p>
<p>Type MIME</p>	<p>Un type MIME est une information permettant de connaître le format d'un document sans se baser sur l'extension.</p>
<p>UEFI = <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.</p> <p>Source Wikipédia : https://fr.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface</p>
<p>Unicode</p>	<p>Unicode est un standard informatique qui permet des échanges de textes dans différentes langues, à un niveau mondial. Il est développé par le Consortium Unicode, qui vise à permettre le codage de texte écrit en donnant à tout caractère de n'importe quel système d'écriture un nom et un identifiant numérique, et ce de manière unifiée, quelle que soit la plate-forme informatique ou le logiciel.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Unicode</p>
<p>URI = <i>Uniform Resource Identifier</i></p>	<p>L'URI est une courte chaîne de caractères identifiant une ressource sur un réseau.</p>
<p>UUID = <i>Universally Unique Identifier</i></p>	<p>Le but des UUID est de permettre à des systèmes distribués d'identifier de façon unique une information sans coordination centrale importante. Dans ce contexte, le mot « unique » doit être pris au sens de « unicité très probable » plutôt que « garantie d'unicité ».</p> <p>Source : http://fr.wikipedia.org/wiki/Universal_Unique_Identifier</p>
<p>Version admissible ou pre-release</p>	<p>Une version admissible, bien que le terme anglais release candidate (souvent abrégé en RC) soit beaucoup plus utilisé, est une version du logiciel qui correspond, du côté pratique, à la version « finale » ou « stable » du dit logiciel. Elle est mise à disposition à des fins de « tests de dernière minute » visant à déceler les toutes dernières erreurs subsistant au sein du programme.</p> <p>Source Wikipédia : http://fr.wikipedia.org/wiki/Version_d%27un_logiciel#Version_admissible</p>
<p>VLAN</p>	

<p>= Réseau local virtuel</p>	<p>Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.</p>
<p>WPAD = Web Proxy Autodiscovery Protocol</p>	<p>WPAD définit la façon selon laquelle un navigateur web se connecte à Internet. Ce protocole permet au navigateur d'utiliser automatiquement le proxy approprié à l'URL demandée. WPAD laisse le navigateur découvrir l'emplacement du fichier PAC grâce aux services DHCP et DNS.</p> <p>Un fichier PAC est un fichier texte en JavaScript, qui contient entre autres la fonction FindProxyForURL(url, host).</p> <p>Cette fonction possède deux arguments associés :</p> <ul style="list-style-type: none"> • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL
<p>x86</p>	<p>La famille x86 regroupe les microprocesseurs compatibles avec le jeu d'instructions de l'Intel 8086.</p> <p>Cette série est nommée IA-32 (pour Intel architecture 32 bits) par Intel pour ses processeurs à partir du Pentium.</p> <p>Source : https://fr.wikipedia.org/wiki/X86</p>
<p>Xen</p>	<p>Xen est un logiciel libre de virtualisation, plus précisément un hyperviseur de machine virtuelle.</p>
<p>XML = Extensible Markup Language</p>	<p>L'Extensible Markup Language (« langage de balisage extensible » en français) est un langage informatique de balisage générique qui dérive du SGML. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG... Elle est reconnaissable par son usage des chevrons (< >) encadrant les balises. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche...) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés une application XML respecte généralement certains principes :</p> <ul style="list-style-type: none"> • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. <p>Source : http://fr.wikipedia.org/wiki/XML</p>
<p>XML-RPC = XML Remote procedure call</p>	<p>XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau.</p> <p>XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et avec n'importe quel langage de programmation. Le serveur est lui</p>

	<p>même sur n'importe quel système et est programmé dans n'importe quel langage.</p> <p>Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage.</p> <p>Source : http://fr.wikipedia.org/wiki/XML-RPC</p>
ZéphirLog	<p>ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.</p>
Zone	<p>Découpage d'un réseau en restant centré sur le pare-feu, le pare-feu lui-même étant une zone nommée par convention bastion, c'est la zone la plus sécurisée (niveau 100). Chaque zone est définie par un nom, une adresse réseau, et un niveau de sécurité.</p>