Installation et mise en œuvre du module Amon

EOLE 2.9



création : Mars 2022 Version : révision : Avril 2022 Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

EOLE 2.9

Version : révision : Avril 2022

Date : création : Mars 2022

Editeur : Pôle national de compétences Logiciels Libres

Auteur(s) : Équipe EOLE

Copyright : Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

Vous êtes libres :

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

Selon les conditions suivantes :

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

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

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

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

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

EOLE est un projet libre (Licence GPL).

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

Pour toute information concernant ce projet vous pouvez nous joindre :

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

Table des matières

Chapitre 1 - Présentation et historique du projet EOLE 10
1. Les objectifs d'EOLE 10
2. Historique du projet EOLE 10
3. Versions des modules EOLE 14
4. Logiciel Libre 17
5. Méta-distribution EOLE 18
6. EOLE 2.9 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 ? 26
3. Les services Amon 26
4. Les différences entre les versions 2.8 et 2.9 27
5. Errata 2.9.n 28

Chapitre 3 - Fonctionnement du module Amon 30
Chapitre 4 - Mise en œuvre du module 34
Chapitre 5 - Installation du module 36
1. Pré-requis 36
2. Médias d'installation 38
3. Déroulement de l'installation 43
4. Partitionnement automatique 47

Chapitre 6 - Configuration du module Amon 55
1. Configuration généralités 55
1.1. Configuration en mode autonome 56
1.1.1. Accès distant 58
1.1.2. La zone Menu 60
1.1.3. La zone Onglet 63
1.1.4. La zone Formulaire 64
1.1.5. La zone Validation 67
1.1.6. Enregistrer la configuration 67
1.1.7. Le mode Debug 68
1.1.8. Édition synchronisée avec l'application Zéphir 70
1.1.9. FAQ 72
1.2. Configuration en mode Zéphir 74
2. Configuration en mode basique 83
2.1. Onglet Général 84
2.2. Onglet Firewall 90
2.3. Onglet Interface-0 91
2.4. Onglet Interface-1 93
2.5. Onglet Interface-n 95
2.6. Onglet Messagerie 97
2.7. Onglet Proxy authentifié : 5 méthodes d'authentification 98
2.8. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (Mode Basique) 102

3. Configuration en mode normal 104
3.1. Onglet Général 105
3.2. Onglet Services 112
3.3. Onglet Firewall 112
3.4. Onglet Interface-0 115
3.5. Onglet Interface-1 119
3.6. Onglet Interface-n 123
3.7. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité 128
3.8. Onglet Clamav : Configuration de l'anti-virus 132
3.9. Onglet Relai DHCP 133
3.10. Onglet Onduleur 134
3.11. Onglet Rvp : Mettre en place le réseau virtuel privé 140
3.12. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 142
3.13. Onglet Mode Restreint : Configuration des restrictions de navigation 148
3.14. Onglet Messagerie 149
3.15. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS 152
3.16. Onglets Squid et Squid2 : activation du déchiffrement HTTPS 154
3.17. Onglet Proxy authentifié : 4 méthodes d'authentification 157
3.18. Onglets Proxy authentifié 2 : Double authentification 161
3.19. Onglet Exceptions proxy 162
3.20. Onglet Wpad : découverte automatique du proxy 165
3.21. Onglet Nginx 166
3.22. Onglet Reverse proxy : Configuration du proxy inverse 167
3.23. Onglet Freeradius : Configuration de l'authentification Radius 171
3.24. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (Mode Normal) 177
4. Configuration en mode expert 184
4.1. Onglet Général 186
4.2. Onglet Services 193
4.3. Onglet Firewall 195
4.4. Onglet Système 197
4.5. Onglet Sshd : Gestion SSH avancée 204
4.6. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système 205
4.7. Onglet Logs : Gestion des logs 205
4.8. Onglet Interface-0 208
4.9. Onglet Interface-1 214
4.10. Onglet Interface-n 221
4.11. Onglet Réseau avancé 228
4.12. Onglet Certificats ssl : gestion des certificats SSL 233
4.13. Onglet Dépôt tiers 240
4.14. Onglet Schedule 242
4.15. Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité 243
4.16. Onglet Clamav : Configuration de l'anti-virus 247
4.17. Onglet Relai DHCP 251
4.18. Onglet Onduleur 252
4.19. Onglet Ead3 258
4.20. Onglet Rvp : Mettre en place le réseau virtuel privé 259
4.21. Onglet Eole sso : Configuration du service SSO pour l'authentification unique 263
4.22. Onglet Zones-dns : Configuration du DNS 273
4.23. Onglet Ead-web : EAD et proxy inverse 275
4.24. Onglet Mode Restreint : Configuration des restrictions de navigation 275
4.25. Onglet Messagerie 276
4.26. Onglet Authentification : Configuration du proxy authentifié et de FreeRADIUS 283
4.27. Onglet Filtrage web : Configuration du filtrage web 285
4.28. Onglets Squid et Squid2 : activation du déchiffrement HTTPS 292

4.29. Onglet Squid : Configuration du proxy 295
4.30. Onglet Proxy authentifié : 4 méthodes d'authentification 300
4.31. Onglets Squid2 et Proxy authentifié 2 : Double authentification 304
4.32. Onglet Exceptions proxy 306
4.33. Onglet Proxy parent : Chaînage du proxy 310
4.34. Onglet Wpad : découverte automatique du proxy 312
4.35. Onglet Nginx 313
4.36. Onglet Applications web nginx 314
4.37. Onglet Reverse proxy : Configuration du proxy inverse 315
4.38. Onglet Freeradius : Configuration de l'authentification Radius 319
4.39. Onglet Eoleflask 325
4.40. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (mode Expert) 326
5. Configuration du module Amon avec le module Scribe en DMZ 337
6. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur 339
7. Configurer le module Amon pour Envole 341
8. Configuration DNS pour chaque interface 346
9. Configurer la découverte automatique du proxy avec WPAD 348
10. Paramétrage de l'authentification Squid pour le module Seth 354
11. Paramétrage de l'authentification Squid avec un serveur Windows 355
12. Mise en place de l'agrégation de liens Ethernet (bonding) 358
Chapitre 7 - Instanciation du module 360
1. Principes de l'instanciation 360
2. Lancement de l'instanciation 361
2.1. Les mots de passe 361
2.2. Création d'un deuxième administrateur 362
2.3. Jonction au domaine 363
2.4. Mise à jour 363
2.5. Le redémarrage 364
Chapitre 8 - Administration du module Amon 365
1. Administration généralités 365
1.1. Principes de l'administration 365
1.2. Découverte de GNU/Linux 366
1.2.1. Les Bases 366
1.2.2. Quelques Commandes 372
1.2.3. Les conteneurs 373
1.2.4. La gestion des onduleurs 373
1.2.5. Les manuels 374
1.2.6. L'éditeur de texte Vim 375
1.2.7. Les commandes à distance avec SSH 380
1.2.8. Quelques références 385
1.3. Reconfiguration 386
1.4. L'interface d'administration EAD 387
1.4.1. Principe général 388
1.4.2. Premier pas dans l'administration d'un serveur 391
1.4.3. Accéder directement à l'EAD d'un serveur Scribe depuis l'extérieur 393
1.4.4. Ajout/suppression de serveurs 394
1.4.5. Surveillance de l'état du serveur 398
1.4.6. Authentification locale et SSO 400
1.4.7. Redémarrer, arrêter et reconfigurer 402
1.4.8. Mise à jour depuis l'EAD 402
1.4.9. Arrêt et redémarrage de services 403

1.4.10. Rôles et association de rôles 405
1.4.11. La console 426
1.4.12. Listing matériel 428
1.4.13. Bande passante 429
1.4.14. Résoudre des dysfonctionnements liés à l'EAD 429
1.5. L'interface d'administration EAD 3 433
1.5.1. Présentation 433
1.5.2. Installation et configuration 434
1.5.3. L'application web 435
1.5.4. Généralités sur les actions 439
1.5.5. Créer une nouvelle action 441
1.5.6. Type d'actions 443
1.5.7. Compléments techniques 446
1.6. L'interface d'administration semi-graphique 446
1.7. Les mises à jour 447
1.7.1. Les différents types de mises à jour 449
1.7.2. Les procédures de mise à jour 452
1.7.3. Ajout de dépôts supplémentaires 457
1.7.4. Désactivation temporaire des mises à jour 457
1.8. Installation manuelle de paquets 458
1.9. Les administrateurs locaux à droits restreints 459
1.10. Passage d'une version d'EOLE à une autre 460
1.11. Passage d'une version RC à une version stable 460
2. Fonctionnalités de l'EAD3 sur le module Amon 461
2.1. Fonctionnalités de l'EAD3 communes à tous les modules 461
2.1.1. Action de stockage de fichiers pour les actions EAD3 461
2.1.2. Action de mise à jour 462
2.1.3. Action système 464
2.1.4. Action de tâches planifiées 470
2.2. Fonctionnalités de l'EAD3 propres au module Amon 473
2.2.1. Actions liées au fonctionnement du pare-feu 473
3. Fonctionnalités de l'EAD propres au module Amon 481
3.1. Rôles et association de rôles 481
3.1.1. Gestion des rôles 481
3.1.2. Association des rôles 485
3.1.3. Les rôles sur le module Amon 487
3.2. Directives optionnelles ERA depuis l'EAD 488
3.3. Exceptions sur la source ou la destination 488
3.4. Filtrage web 491
3.4.1. Groupe de machine : Filtrage par machine ou par groupe de machine 492
3.4.2. Sources et destinations : Interdire l'accès à un sous-réseau depuis une interface 498
3.4.3. Sources et destinations : Interdire ou restreindre l'activité d'un sous-réseau 500
3.4.4. Visites des sites : Observatoire des navigations 503
3.4.5. Sites : Bases de filtres optionnels 504
3.4.6. Sites : Filtrage syntaxique 506
3.4.7. Sites : Interdire et autoriser des domaines 507
3.4.8. Sites : Interdire des extensions et des types MIME 510
3.4.9. Sites : Politique liste blanche 511
3.4.10. Utilisateurs : Filtrage par utilisateur 512
3.5. Outil d'analyse de logs LightSquid 513
4. ERA, éditeur de règles pour le module Amon 517

4.1. Introduction 517
4.1.1. Présentation 517
4.1.2. Les fichiers XML de modèles 518
4.1.3. Utilisation de variables Creole 520
4.2. Utilisation 521
4.2.1. Les zones de sécurité 521
4.2.2. Les flux 527
4.2.3. Les directives 529
4.2.4. La qualité de service 541
4.2.5. Les options du modèle 542
4.2.6. L'inclusion statique 543
4.2.7. Imbriquer des modèles : l'héritage 543
4.2.8. Communication avec Zéphir 544
4.3. Directives optionnelles ERA depuis l'EAD 545
4.4. Compléments techniques 546
4.4.1. Le format XML interne 546
4.4.2. Comportement du Backend 547
4.4.3. Le compilateur 548
4.5. Quelques références 549
5. Gestion des tunnels : RVP 549
6. Résoudre des dysfonctionnements liés au MTU 550
Chapitre 9 - Paramétrage des postes client 553
1. Authentification NTLM/SMB hors domaine 553
2. Configurer la découverte automatique du proxy avec WPAD 553
3. Proxy non configuré dans le navigateur : redirection ou page d'information 559
4. Synthèse des paramètres proxy à utiliser pour les postes client 562
Chapitre 10 - Personnalisation du module 564
1. Panorama des services 564
1.1. Services liés aux bases de données 564
1.1.1. eole-annuaire 564
1.1.2. eole-client-annuaire 565
1.1.3. eole-db 565
1.1.4. eole-interbase 566
1.1.5. eole-mysql 566
1.1.6. eole-postgresql 566
1.2. Services liés aux serveurs de fichiers 567
1.2.1. eole-ad-dc 567
1.2.2. eole-fichier-primaire 567
1.2.3. eole-cups 568
1.2.4. eole-proftpd 569
1.2.5. eole-dhcp 569
1.2.6. Partages avec NFS 570
1.3. Services liés au web 572
1.3.1. eole-web 572
1.3.2. eole-reverseproxy 573
1.3.3. eole-wpad 573
1.4. Services liés à la messagerie 574
1.4.1. eole-exim 574
1.4.2. eole-spamassassin 574
1.4.3. eole-courier 575

1.4.4. eole-sympa 575
1.5. Services liés au proxy et à l'authentification 576
1.5.1. eole-proxy 576
1.5.2. eole-radius 577
1.6. Services liés à la virtualisation 577
1.6.1. eole-libvirt 577
1.6.2. eole-one-frontend 578
1.6.3. eole-one-node 578
1.6.4. eole-one-singlenode 579
1.7. Autres services réseau 579
1.7.1. eole-antivirus 579
1.7.2. eole-apt-cacher-ng 580
1.7.3. eole-bareos 580
1.7.4. eole-dns 581
1.7.5. eole-dhcrelay 582
1.7.6. eole-ltsp-server 582
1.7.7. eole-nut 582
1.7.8. eole-open-iscsi 583
1.7.9. eole-pacemaker 583
1.7.10. eole-snmpd 584
1.7.11. eole-vpn 584
2. Personnalisation du serveur à l'aide de Creole 585
2.1. Répertoires utilisés par EOLE 585
2.2. Création de patch Creole 586
2.3. Les dictionnaires Creole 588
2.3.1. Ajouter un en-tête XML 588
2.3.2. Utiliser des fichiers templates, paquets, services et règles de pare-feu 589
2.3.3. Utiliser des familles, variables et des séparateurs 597
2.3.4. Comportement des variables 601
2.3.5. Mettre en place des contraintes 602
2.3.6. Afficher de l'aide 611
2.4. Le langage de template Creole 611
2.4.1. Déclarations du langage Creole 612
2.4.2. Fonctions prédéfinies 616
2.4.3. Utilisation avancée 620
2.4.4. Exemple 621
2.5. Le fichier de configuration Creole 622
2.6. Les scripts Creole 623
2.6.1. CreoleLint et CreoleCat 623
2.6.2. CreoleGet et CreoleSet 625
2.6.3. CreoleRun et CreoleService 628
2.6.4. CreoleLock 628
2.6.5. Indications pour la programmation 630
2.7. Ajout de script exécuté à l'instance ou au reconfigure 633
2.8. Ajout d'un test diagnose 634
2.9. Gestion des noyaux Linux 635
2.10. Gestion des tâches planifiées eole-schedule 636
2.11. Gestion du pare-feu eole-firewall 640
2.12. Gestion de drapeaux eole-flag 642
Chapitre 11 - Résolution de problèmes 646
1. Problèmes à la mise en œuvre 646

2. Problèmes à l'exploitation 646
3. Trouver de l'information 651
4. Demander de l'aide / Signaler un problème 654
5. Contribuer au projet EOLE 659

Chapitre 12 - Documentations techniques 661
1. Les dépôts EOLE 661
2. Gestion des journaux systèmes sur EOLE 663
3. Préconisations de l'ANSSI pour la mise en œuvre d'un système de journalisation 664
3.1. Contexte juridique 664
3.2. Recommandations de sécurité pour la mise en œuvre d'un système de journalisation 665

Chapitre 13 - Compléments techniques 669
1. Les services utilisés sur le module Amon 669
1.1. eole-antivirus 669
1.2. eole-dhcrelay 670
1.3. eole-dns 670
1.4. eole-exim 671
1.5. eole-nut 671
1.6. eole-proxy 672
1.7. eole-radius 673
1.8. eole-reverseproxy 673
1.9. eole-vpn 673
1.10. eole-wpad 674

2. Ports utilisés sur le module Amon 675

Chapitre 14 - Questions fréquentes 678
1. Questions fréquentes communes aux modules 678
2. Questions fréquentes propres au module Amon 698

Glossaire 702

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 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.705] :
- 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 diagnostique 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.735].

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.724] ;
  - **Seshat** le relais de messagerie pour le domaine intra-académique ;
- la console de visualisation de l'IDS Prélude (fonctionnant avec ZéphirLog) ;
- nouveau module 2.2 eSSL par le MEDDE[p.720] ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- intégration d'Envole[p.711] 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.719] 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.720].

2012

- portage d'Eclair en 2.3 (juillet), repose sur ltsp-cluster, le serveur embarque le logiciel Gaspacho[p.713] ;
- 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.731] 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.731] 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.724].
- 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 (MENSR) et le Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM[p.720]).

  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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- EOLE 2.7.1 LTS (juin)
  - portage du module Eclair ;
  - portage des modules Scribe et Horus en Scribe AD et Horus AD, le mode NT est définitivement abandonné ;
  - abandon du module eSBL au profit du module Seth en mode membre.

2020

- EOLE 2.7.2 LTS (juillet)
- EOLE 2.8.0 LTS (décembre)
  - migration du code de la distribution de python2 vers python3 ;
  - possibilité d'utiliser LemonLDAP::NG[p.717] en tant qu'alternative à EoleSSO.

2021

- EOLE 2.8.1 LTS (juillet)
  - nouvelle version du module AmonEcole (non disponible sur EOLE 2.7) ;
  - possibilité de filtrer les flux HTTPS à l'aide d'une configuration type Man in the middle[p.720] (SSL interception) ;
  - mise à disposition des paquets `eole-fog` et `eole-lts-server` permettant respectivement la mise en œuvre de FOG[p.712] et d'un seveur LTSP[p.727] sur un module EOLE.

2023

- EOLE 2.9.0 LTS (février)
  - intégration du moteur de conteneur[p.707] Podman[p.726] avec une première implémentation pour le service EoleSSO et une seconde pour l'IHM ERA.

2025

- EOLE 2.10.0 LTS (mars)

3. Versions des modules EOLE

Versions supportées des modules EOLE

Version	**2.7.0**	**2.7.1**	**2.7.2**	**2.8.0**	**2.8.1**	**2.9.0**	**2.10.0**
Date de sortie	2018	2019	2020	2020	2021	2022	2025
Fin du support	Juin 2023	Juin 2023	Juin 2023	Juin 2025	Juin 2025	Juin 2027	Juin 2029
eCDL							
eSBL							
Amon							

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Eclair							
Hâpy							
Hâpy Node							
Horus (NT)							
Horus (AD)							
Scribe (NT)							
Scribe (AD)							
Seshat							
Seth							
Sphynx							
Thot							
AmonEcole							
AmonEcoleEclair							
Zéphir							
Envole							

Tableau des modules par versions d'EOLE

Versions non supportées 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**	**2.**
Date de sortie	2007	2008	2009	2011	2014	2015	2015	2015	2015	2016	2016	2(

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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												

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

AmonEcole+ AmonEcoleEclair												
AmonHorus												
Zéphir												
ZéphirLog												
Envole												

Tableau des modules par versions d'EOLE

4. Logiciel Libre

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

Le logiciel libre garantit quatre niveaux de libertés :

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

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

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

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

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.718].

Contributions au libre

Contribuer au libre peut prendre plusieurs formes : promotion, amélioration, documentation, traduction,

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 : https://dev.opennebula.org/users/1416.html ;
- 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/ContributionsExterieures

5. 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.

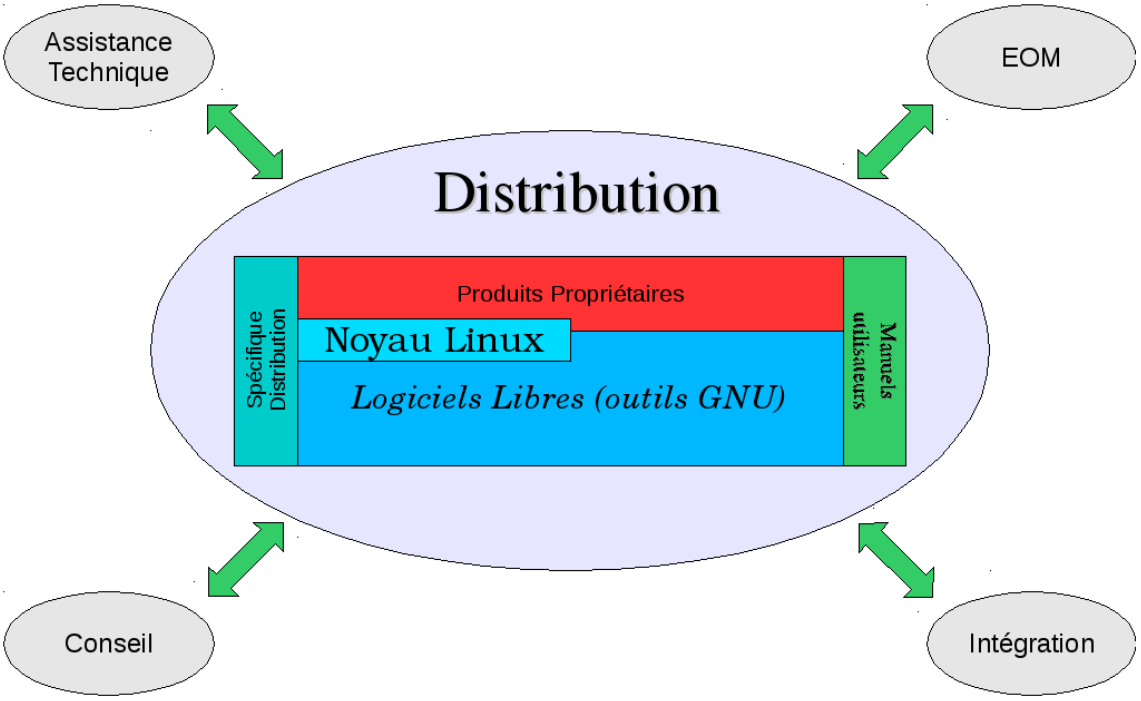
Une distribution GNU/Linux

Une distribution[p.709] GNU/Linux[p.718] 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

6. EOLE 2.9

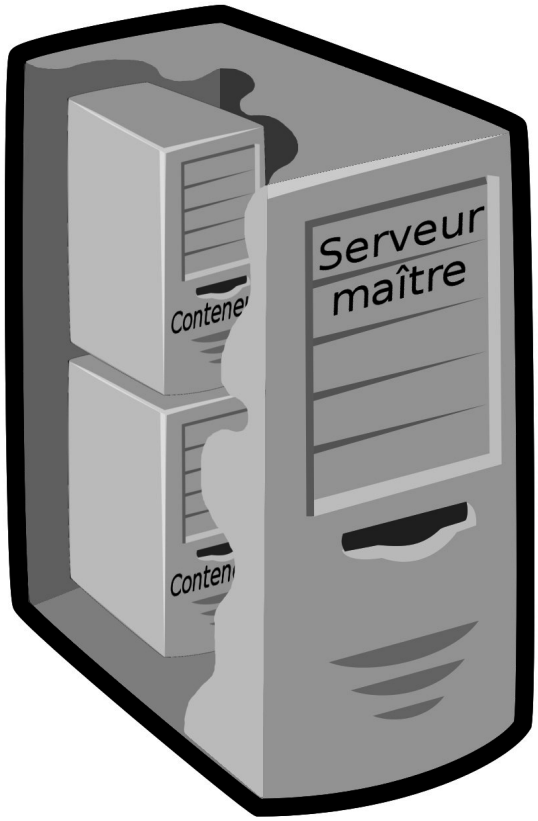


Logo officiel d'Ubuntu par Canonical Ltd

Les modules de la version EOLE 2.9 s'appuient sur la distribution GNU/Linux Ubuntu 22.04 LTS nommée également Jammy Jellyfish.

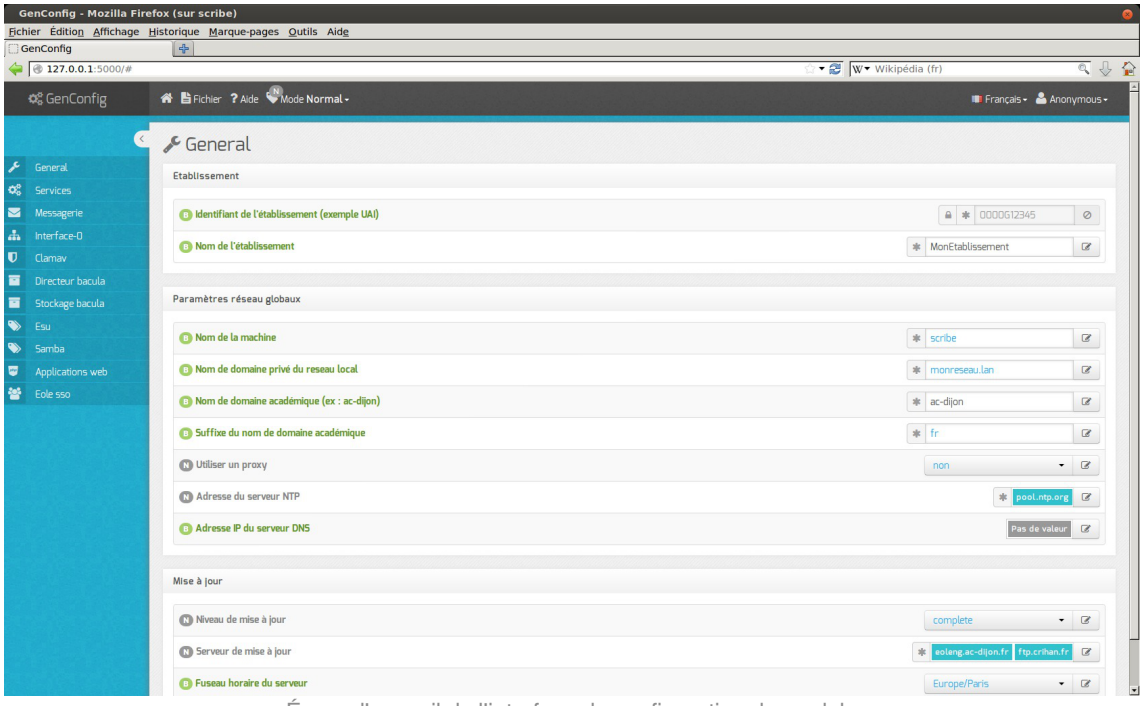
Ubuntu 22.04 LTS est disponible depuis le mois d'avril 2022. Portant le label LTS[p.718], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2027. Le Pôle de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2027.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



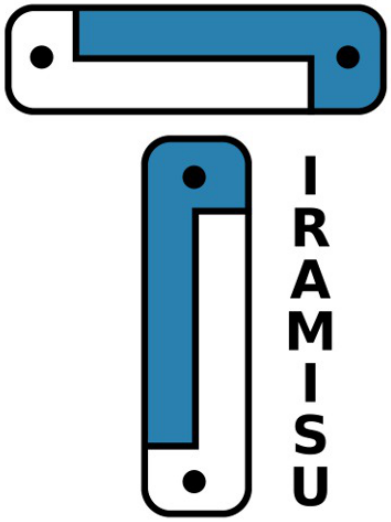
La version 2.9 des modules utilise toujours la technique de virtualisation par conteneur. Les conteneurs isolent certains services les uns des autres à l'intérieur même du système, ce qui lui confère un haut degré de sécurité. Contrairement à d'autres techniques de virtualisation, il n'y a qu'une seule 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.733].



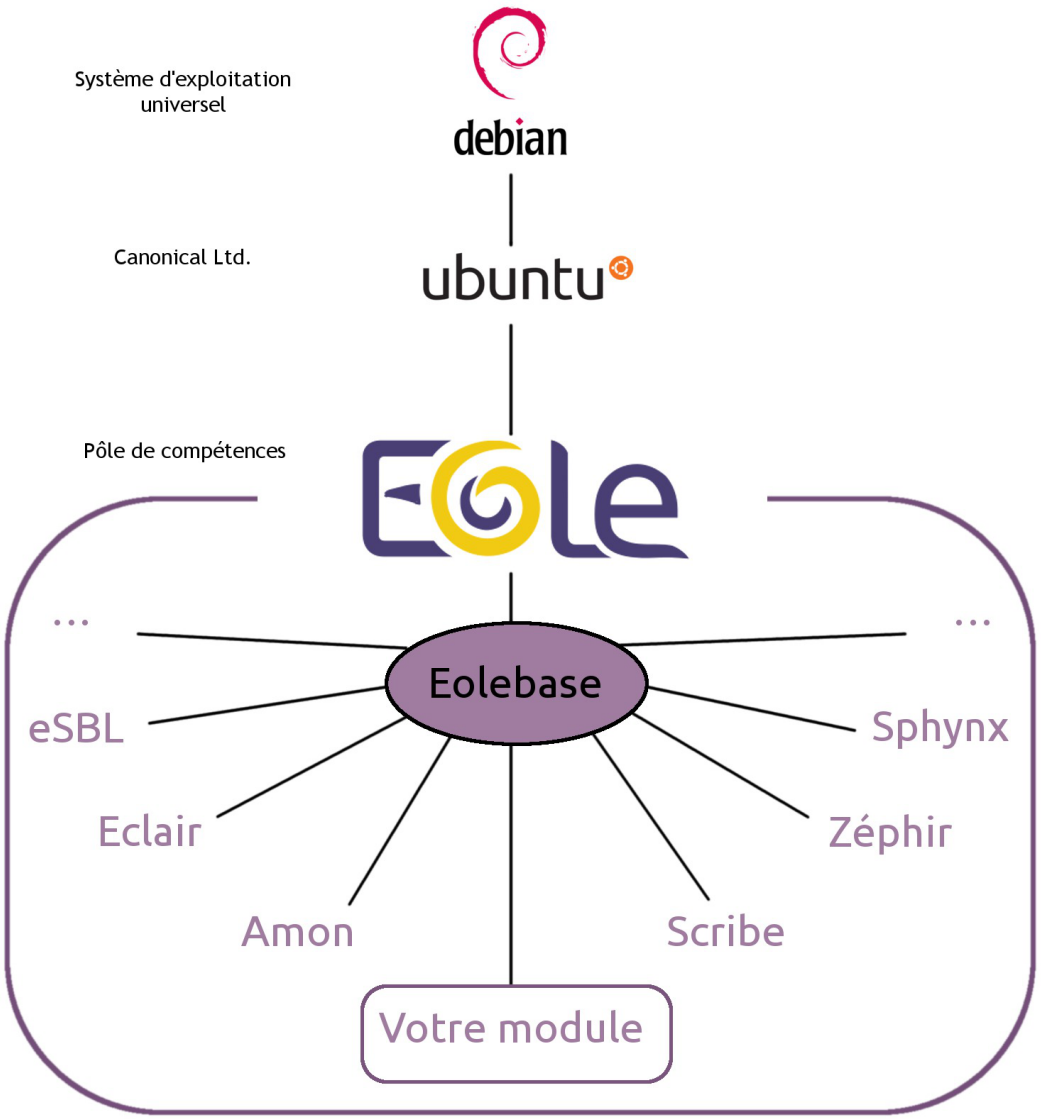
Logo du logiciel Tiramisu

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 a disposition :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- le **patch** : permettant de modifier les modèles (templates) fournit 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 : https://cecill.info
  - Wikipédia : http://fr.wikipedia.org/wiki/Licence_CeCILL

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 2

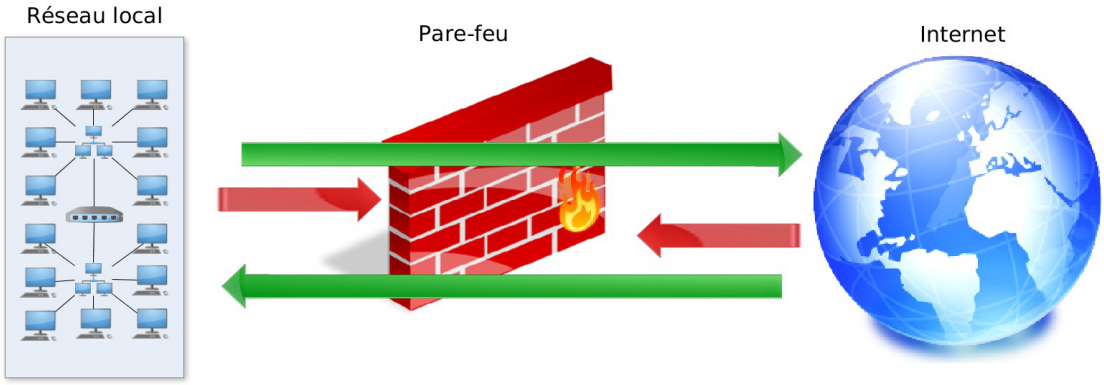
Introduction au module Amon

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.711], est à votre disposition pour effectuer ce travail.

Il est également possible de créer un réseau virtuel privé (RVP[p.728], 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.702] .

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Dans le cadre de la mise en œuvre d'un réseau virtuel privé[p.728] entre le serveur Amon et et un concentrateur académique (par exemple le module Sphynx), il faut au préalable s'assurer de la compatibilité des logiciels.

Pour les connexions VPN, la compatibilité est assurée par strongSwan

Actuellement toutes les versions maintenues du module Sphynx peuvent établir des tunnels VPN 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.732] 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/.

Quant-au serveur Sphynx utilisé pour la gestion des VPN dans l'application ARV, il est impératif d'utiliser une version EOLE supérieure ou égale à la version des serveurs Amon/Amonecole/Sphynx importés dans l'application via Zéphir.

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 le module 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.

Spécificités matérielles

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.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.709].

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.

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 5.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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- *Exim4* : serveur de messagerie ;
- *NUT* : gestion des onduleurs ;
- *NTP* : synchronisation avec les serveurs de temps ;
- *Nginx* : proxy inverse et serveur web.

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 ;
- *FreeRADIUS* : service d'authentification réseau ;
- *ERA* : outil de génération de règles iptables.

4. Les différences entre les versions 2.8 et 2.9

Les modules de la version EOLE 2.9 s'appuient sur la distribution GNU/Linux Ubuntu 22.04 LTS nommée également Jammy Jellyfish.

Ubuntu 22.04 LTS est disponible depuis le mois d'avril 2022. Portant le label LTS[p.718], cette version est soutenue et mise à jour pendant une durée de cinq ans, son support s'arrête donc en avril 2027. Le Pôle de Compétences Logiciels Libres prend en charge son support jusqu'à fin juin 2027.

Noyau Linux

Cette nouvelle version d'Ubuntu implique également un changement de version du noyau avec de nouvelles prises en charge matériel.

Les modules EOLE 2.9 utilisent par défaut le noyau le plus récent de la distribution Ubuntu, soit, à ce jour une version `linux-image-generic 5.15.0`.

OpenSSH

Le passage à la version 8.9 supprime notamment la prise en charge des mots de passe hachés en MD5 [p.720].

Les algorithmes de signature `Ed25519` et `ssh-rsa/SHA-2` sont à privilégier.

Modules disponibles sur EOLE 2.9

Les modules suivants sont proposés sur EOLE 2.9.0 :

- Eolebase
- Amon
- Scribe
- Seth

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- AmonEcole
- Sphynx
- Seshat
- Thot
- Zéphir

Hâpy

Au moment de la sortie d'EOLE 2.9.0, il n'existait pas de paquets OpenNebula[p.724] disponibles pour Ubuntu 22.04.

De ce fait, les modules Hâpy et HâpyNode sont disponibles uniquement à partir de l'image d'installation EOLE 2.9.0.1.

Modules supportés par Zéphir 2.9

En version 2.9, un module Zéphir gère les modules EOLE de la version 2.6.0 jusqu'à sa propre version d'EOLE 2.9.

2.9.0

Moteur de conteneur Podman

En 2.9.0, EOLE intègre le moteur de conteneur[p.707] Podman[p.726] avec une première implémentation pour le service EoleSSO et une seconde pour l'IHM ERA.

Mode promiscuité sur les interfaces

De nouvelles variables permettent d'activer le mode promiscuous[p.721] interface par interface.

Dans le cas de l'installation d'un module Scribe ou AmonEcole dans Virtualbox, leur activation est nécessaire.

FOG 1.5.10

Le paquet additionnel `eole-fog` permet désormais de déployer la version 1.5.10 du serveur de copie et de déploiement d'images FOG[p.712].

Proxy NTLM

Sur EOLE 2.9, le proxy NTLM Cntlm[p.706] anciennement proposé sur le port 3127 est totalement supprimé.

Depuis EOLE 2.8.1, les postes hors domaine peuvent utiliser directement le proxy authentifié.

5. Errata 2.9.n

Il y a un seul niveau de mise à jour qui comporte 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 2.9.Y. Les dysfonctionnement connus sont corrigés d'une version à une autre d'EOLE.

https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/Errata29

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 3

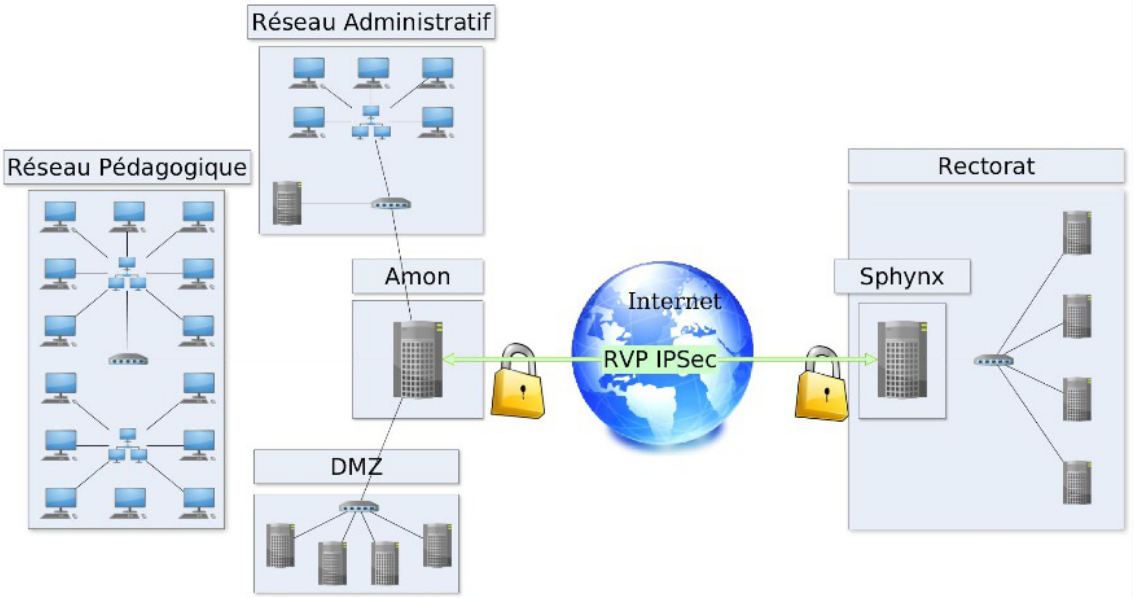
Fonctionnement du module Amon

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 :

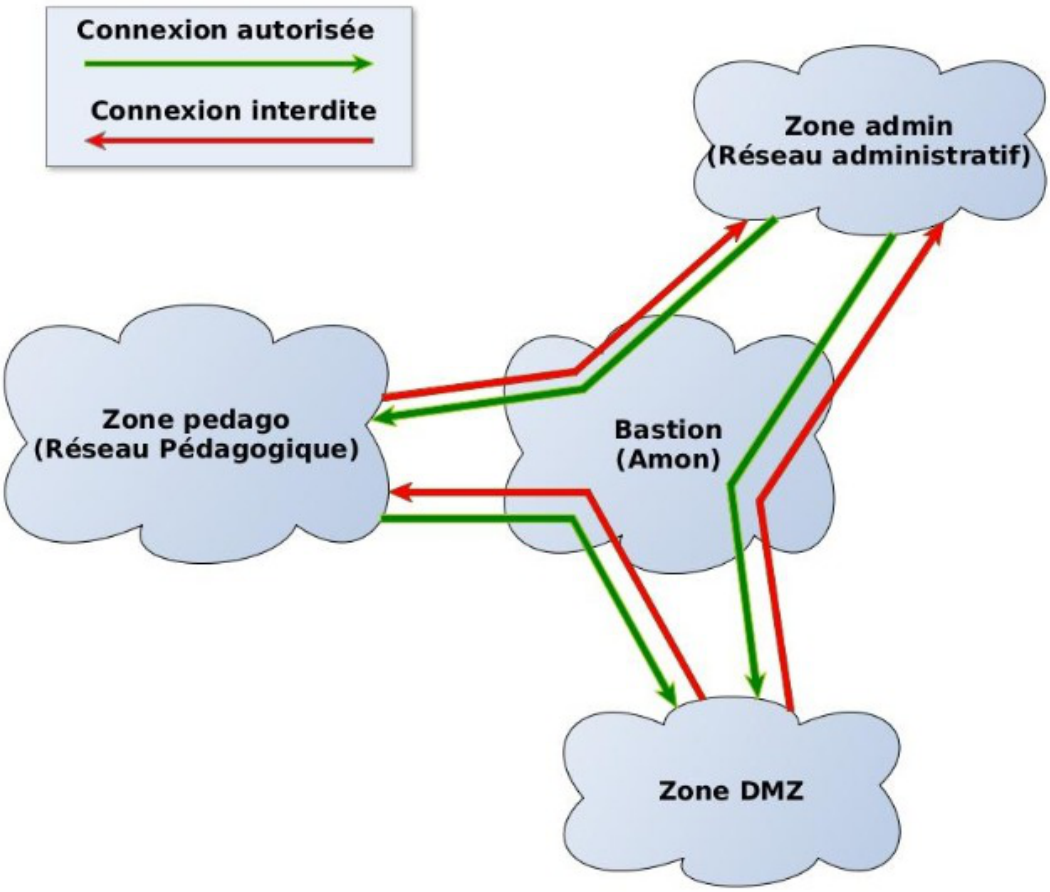
- la mutualisation de l'accès Internet pour les réseaux locaux ;
- la gestion des Réseaux Virtuels Privés (RVP/VPN).



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.725] repose sur le logiciel iptables[p.716] et l'éditeur de règles ERA[p.711] 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.735] 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 l'interface 1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur l'interface 1) ;
- **3zones** : gestion d'une zone admin sur l'interface 1 et d'une zone pedago sur l'interface 2 ;
- **3zones-dmz** : gestion d'une zone pedago sur l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.



Chaque modèle de zone proposé 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/`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

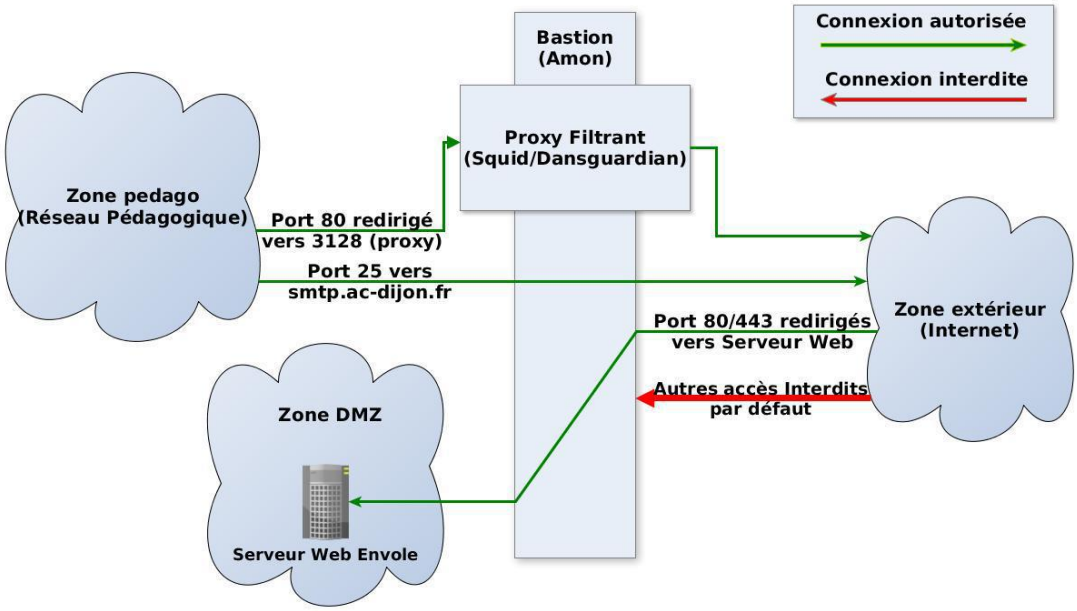
Le service bastion met en cache les règles mais ne les régénère pas à chaque fois.

À partir de la version 2.6.1, seules les commandes `reconfigure` et `bastion regen` régénèrent les règles.

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

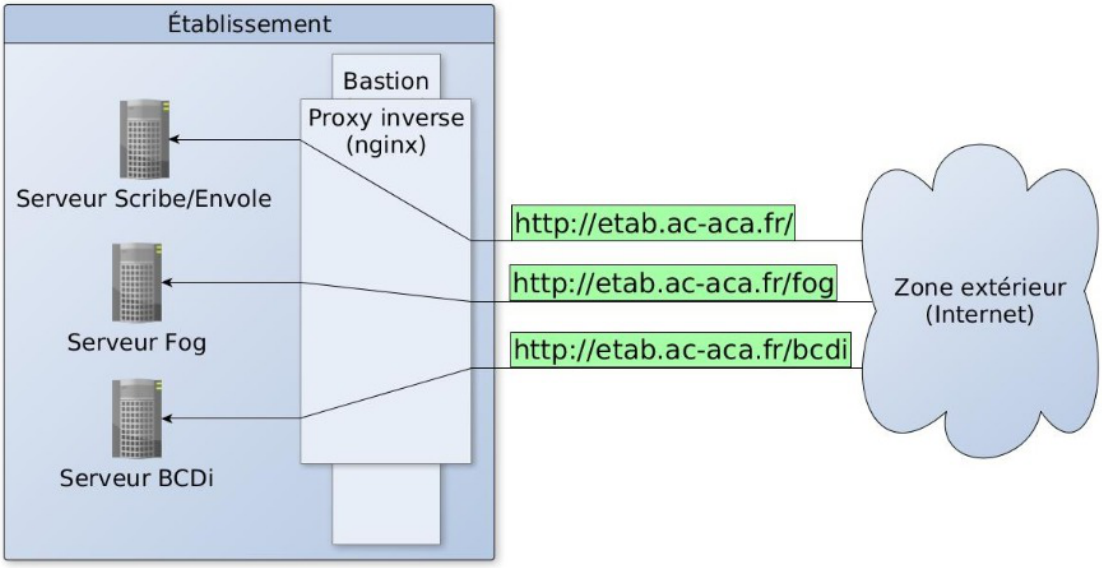
- de gérer une liste de sites et d'URL interdits ;
- le filtrage syntaxique ;
- l'interdiction par extension et type MIME ;
- de gérer une liste blanche (« tout interdit sauf ») ;
- d'interdire une plage d'IP et plage horaire ;
- l'économie de bande passante par la mise en cache.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Le module Amon utilise Nginx pour mettre en place un proxy inverse qui permet :

- d'ouvrir des services Web sur Internet ;
- de rediriger par URL ;
- de forcer l'utilisation de HTTPS ;
- la ré-écriture d'URL (expressions régulières).



D'autres services sont également proposés.

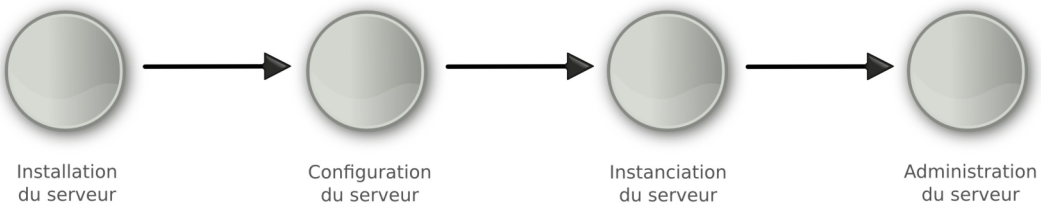
Parmi les plus couramment utilisés :

- l'établissement de réseaux virtuels privés ;
- la délégation de zone DNS et le DNS local reposent sur bind ;
- l'authentification Wifi repose sur le logiciel libre FreeRADIUS.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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'amorce au moyen d'un support de type CD-ROM ou clé USB. L'image ISO [p.715] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (https://pcll.ac-dijon.fr/eole/). Tous les modules sont installables depuis cette unique image ISO.

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

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

  Les versions précédentes s'appuyaient sur isolinux pour la construction de l'image ISO.

  À partir de la version 2.9.0, EOLE construit ses images ISO en utilisant les outils préconisés par Ubuntu : le live CD[p.718] et subiquity[p.732].

  Ce changement s'accompagne de l'utilisation du menu de boot GRUB[p.713] et d'interactions pour la configuration du réseau et du proxy (si nécessaire).

- 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 première interface réseau 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.731], e2guardian[p.710], etc.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

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

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

  Chaque module possède des fonctionnalités propres, souvent complémentaires.

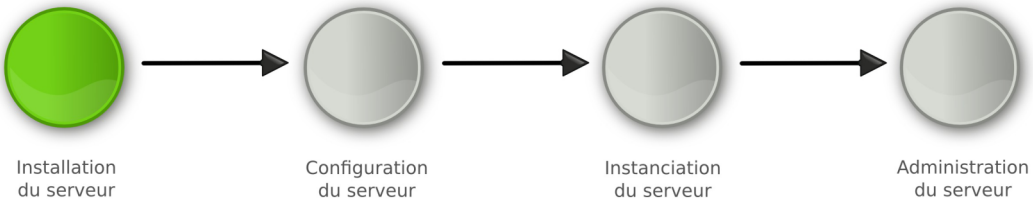
  Diverses interfaces permettent la mise en œuvre de ces fonctionnalités et en facilitent l'usage.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 5

Installation du module

La première des quatre phases



Installation

- La **phase d'installation** s'amorce au moyen d'un support de type CD-ROM ou clé USB. L'image ISO [p.715] pour réaliser le support est téléchargeable sur le site internet du projet EOLE (https://pcll.ac-dijon.fr/eole/). Tous les modules sont installables depuis cette unique image ISO.

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

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

Les versions précédentes s'appuyaient sur isolinux pour la construction de l'image ISO.

À partir de la version 2.9.0, EOLE construit ses images ISO en utilisant les outils préconisés par Ubuntu : le live CD[p.718] et subiquity[p.732].

Ce changement s'accompagne de l'utilisation du menu de boot GRUB[p.713] et d'interactions pour la configuration du réseau et du proxy (si nécessaire).

1. Pré-requis

Matériel

Il est recommandé de vérifier la compatibilité matérielle en s'assurant que le serveur est compatible avec Ubuntu 22.04 LTS (Jammy Jellyfish).

Les images ISO générées par EOLE nécessitent désormais le support de l'UEFI[p.733] et seule l'architecture 64 bits (AMD64[p.703]) est supportée.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pré-requis par module

Les pré-requis des différents modules en termes de RAM, disque et processeur sont désormais regroupés dans la page wiki suivante :

https://dev-eole.ac-dijon.fr/projects/modules-eole/wiki/PreRequis

Serveurs certifiés par Ubuntu

Ubuntu propose une liste de serveurs certifiés : https://certification.ubuntu.com/server

Le support des BIOS (legacy) n'est plus assuré avec les nouvelles images ISO générées par EOLE.

Environnement virtualisé

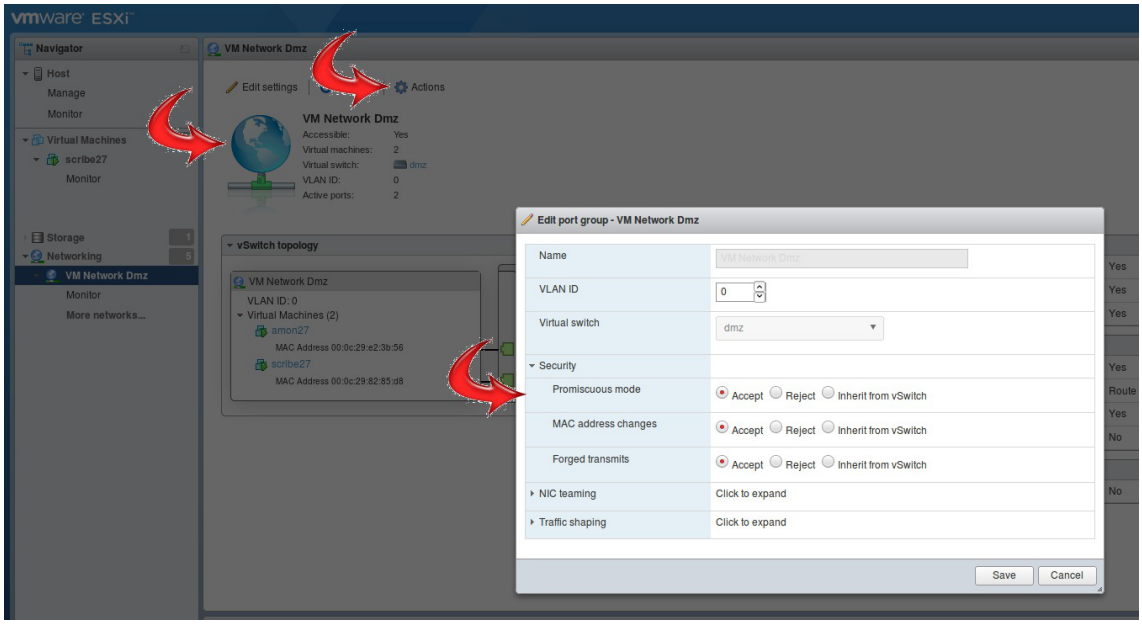
Les modules AmonEcole et Scribe 2.9 utilisent un conteneur LXC[p.719] pour héberger les services Active Directory.

Ce conteneur utilise la technologie Macvlan en mode bridge.

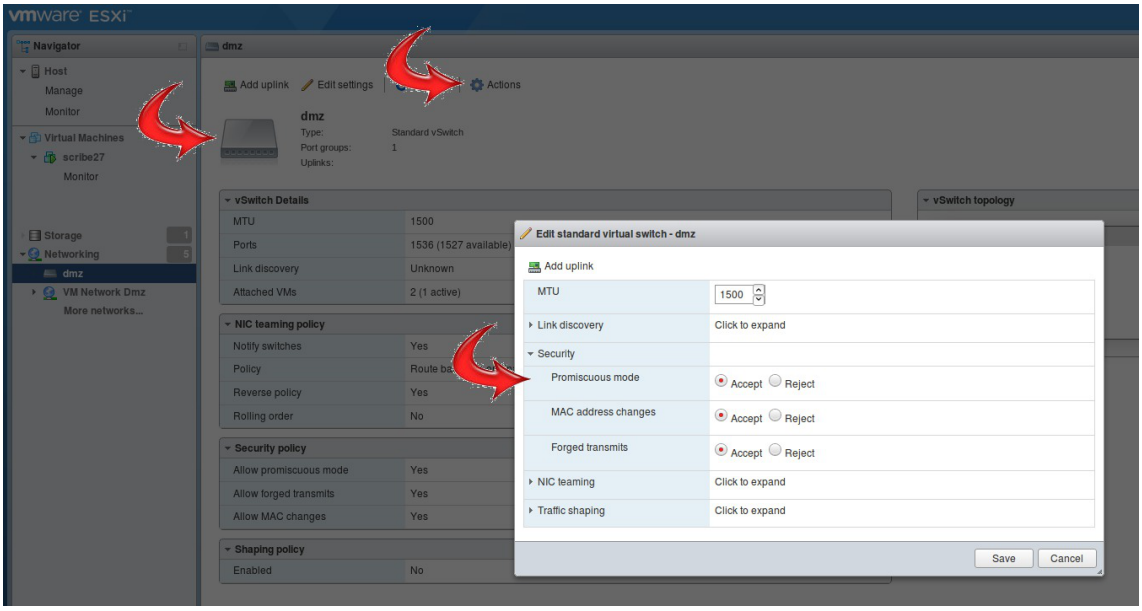
Dans le cas d'une installation dans une infrastructure virtualisée (ESXI, Virtualbox, ...) le bon fonctionnement du réseau nécessite l'activation du mode promiscuous[p.721].

L'activation du mode promiscuous des interfaces réseaux du module s'effectue au moment de la configuration dans les onglets de chaque interface.

Activation de la carte virtuelle et du switch ESXI en mode promiscuous



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



2. Médias d'installation

Les images d'installation des modules EOLE sont disponibles sur le site du projet EOLE en HTTP[p.714] :

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

Le fichier SHA256SUMS sert à vérifier l'intégrité de l'image ISO téléchargée, avec la commande `sha256sum` (l'image et le fichier SHA256[p.730] sont dans le même répertoire) :

```
$ sha256sum -c SHA256SUMS
eole-2.9.x-amd64.iso: Réussi
```

Différents types de média sont utilisables pour installer les modules.

À partir de la version 2.9.0, les images d'installation ne contiennent pas tous les paquets nécessaires à la mise en route des modules (live CD[p.718]).

Une connexion internet est nécessaire pour récupérer ces paquets lors de la phase d'installation.

Les versions précédentes s'appuyaient sur isolinux pour la construction de l'image ISO.

À partir de la version 2.9.0, EOLE construit ses images ISO en utilisant les outils préconisés par Ubuntu : le live CD[p.718] et subiquity[p.732].

Ce changement s'accompagne de l'utilisation du menu de boot GRUB[p.713] et d'interactions pour la configuration du réseau et du proxy (si nécessaire).

Clé USB

Créer une clé USB bootable depuis une distribution GNU/Linux

Pour créer une clé EOLE 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 (

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

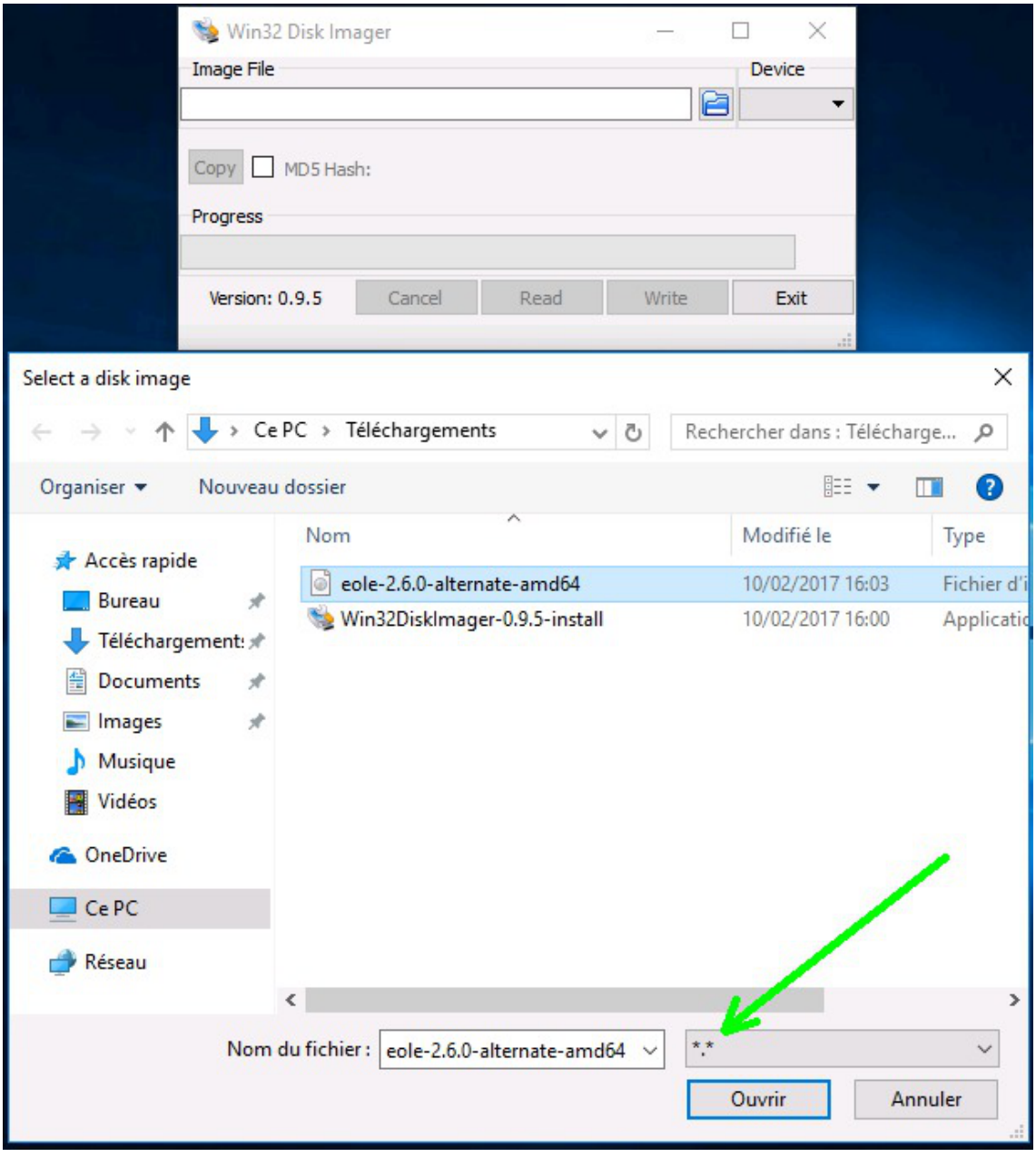
`umount /dev/sdxy`) ;

3. se placer dans le répertoire contenant l'image ISO préalablement téléchargée ;
4. `# dd if=eole-2.9.x-amd64.iso of=/dev/sdx` (les données seront perdues !) ;
5. démarrer le serveur cible sur la clé USB.

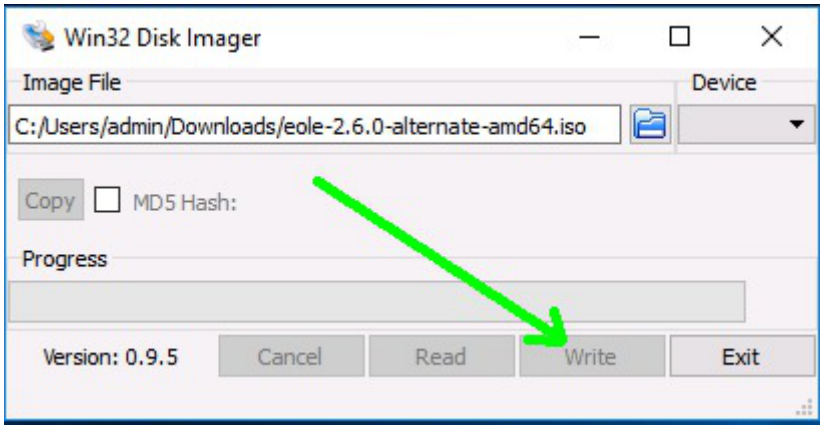
La commande `dd` écrase intégralement le contenu de la clé.

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/



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



DVD-ROM

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

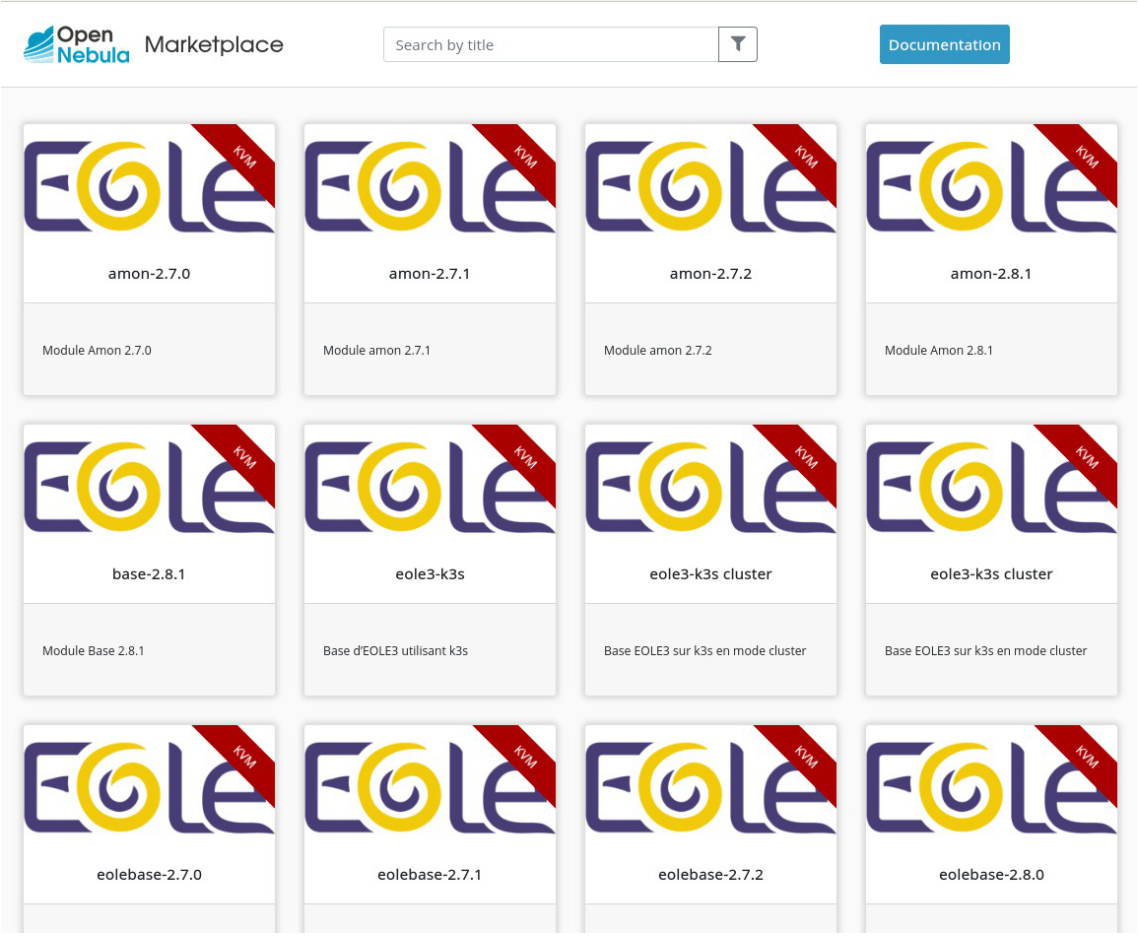
Image KVM pré-installée

Dans le cadre de l'automatisation du déploiement de serveurs sur le module Hâpy des images KVM[p.717] des principaux modules EOLE sont régulièrement générées et mises à disposition.

Ces images peuvent tout-à-fait être utilisées directement dans un hyperviseur[p.714].

Les images sont distribuées via le magasin d'applications EOLE disponible à l'adresse suivante : https://magasin.eole.education/appliance

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Le magasin d'applications EOLE

Les images KVM[p.717] hébergées sur la plate-forme sont régulièrement actualisées afin de minimiser la durée de l'étape de mise à jour lors du déploiement des serveurs.

PXE

Le document suivant décrit la mise en place d'une configuration PXE[p.728] 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 2.9 sur une version installée de Ubuntu LTS 22.04 édition serveur [http://releases.ubuntu.com/22.04/] .



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.719] proposé par l'installateur de l'image ISO EOLE.

La version d'Ubuntu pré-installée chez certains hébergeurs peut être en anglais par défaut.

Il faut passer les locales à la valeur `fr_FR.UTF-8` :

```
# apt install locales
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
# dpkg-reconfigure locales
```

Il faut également passer le clavier en français :

```
# dpkg-reconfigure keyboard-configuration
```

Utiliser les dépôts EOLE

- ajouter les dépôts EOLE et Envole

```
# cat > /etc/apt/sources.list.d/eole.list <<EOF
deb http://eole.ac-dijon.fr/eole eole-2.9.0 main cloud
deb http://eole.ac-dijon.fr/eole eole-2.9.0-security main cloud
deb http://eole.ac-dijon.fr/eole eole-2.9.0-updates main cloud
deb http://eole.ac-dijon.fr/envole envole-9 main
EOF
```

- ajouter les clés GPG publiques d'EOLE (clés qui signent les paquets EOLE et Envole pour en vérifier l'intégrité)

```
# wget -qO- "http://eole.ac-dijon.fr/eole/project/eole-2.9-repository.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/eole-archive-keyring.gpg add -
# wget -qO- "http://eole.ac-dijon.fr/envole/project/envole-9-repository.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/eole-archive-keyring.gpg add -
```

- désactiver l'architecture étrangère *i386*

```
# dpkg --remove-architecture i386
```

- mettre à jour les dépôts

```
# apt update
```

- faire en sorte que les paquets s'installent sans interaction

```
# export DEBIAN_FRONTEND=noninteractive DEBIAN_PRIORITY=critical
```

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Installer le paquet méta-paquet du module souhaité :

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

Exemples

```
# apt-get -y --force-yes install eole-server eole-amon-all
# apt-get -y --force-yes install eole-server eole-seth-all
# apt-get -y --force-yes install eole-server 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 ssmtp
```

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 ssmtp
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

3. Déroulement de l'installation

Pour installer un module, il suffit de :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

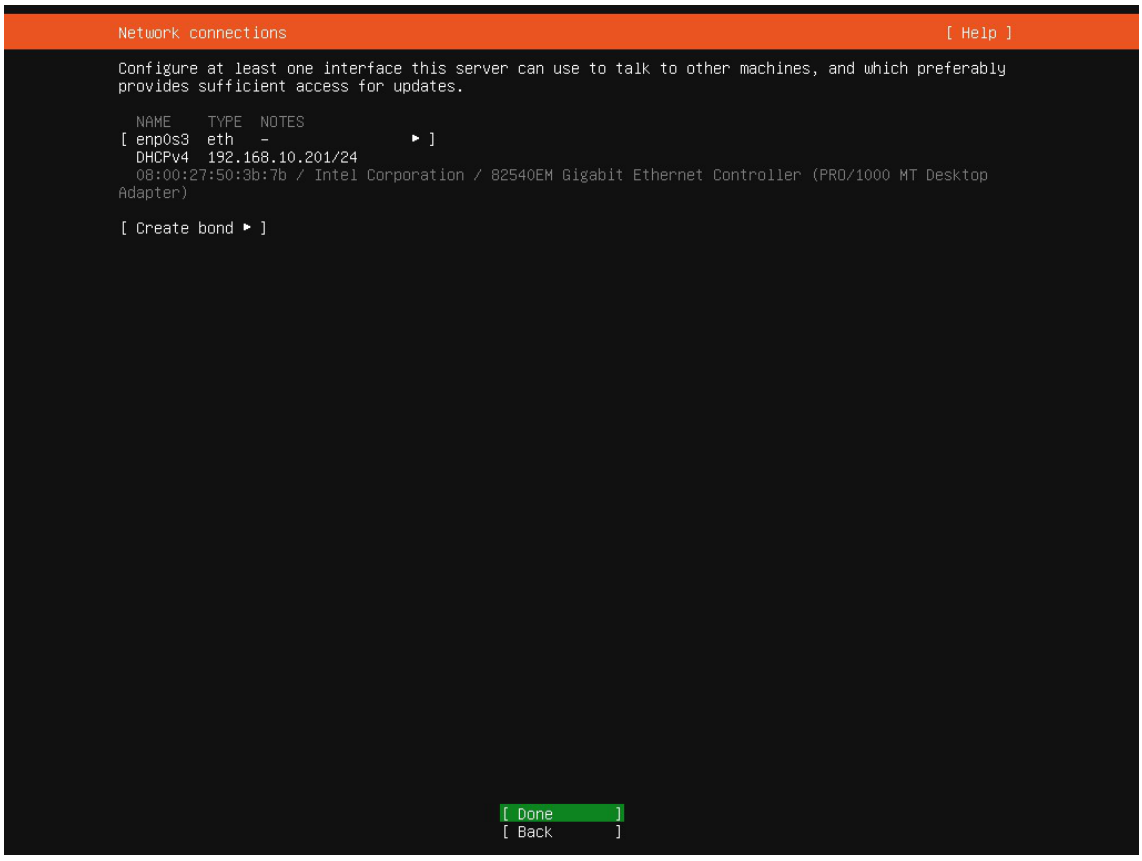
- démarrer le serveur cible avec le média d'installation choisi ;
- sélectionner le module à installer parmi ceux proposés ;
- valider en appuyant sur la touche Entrée.



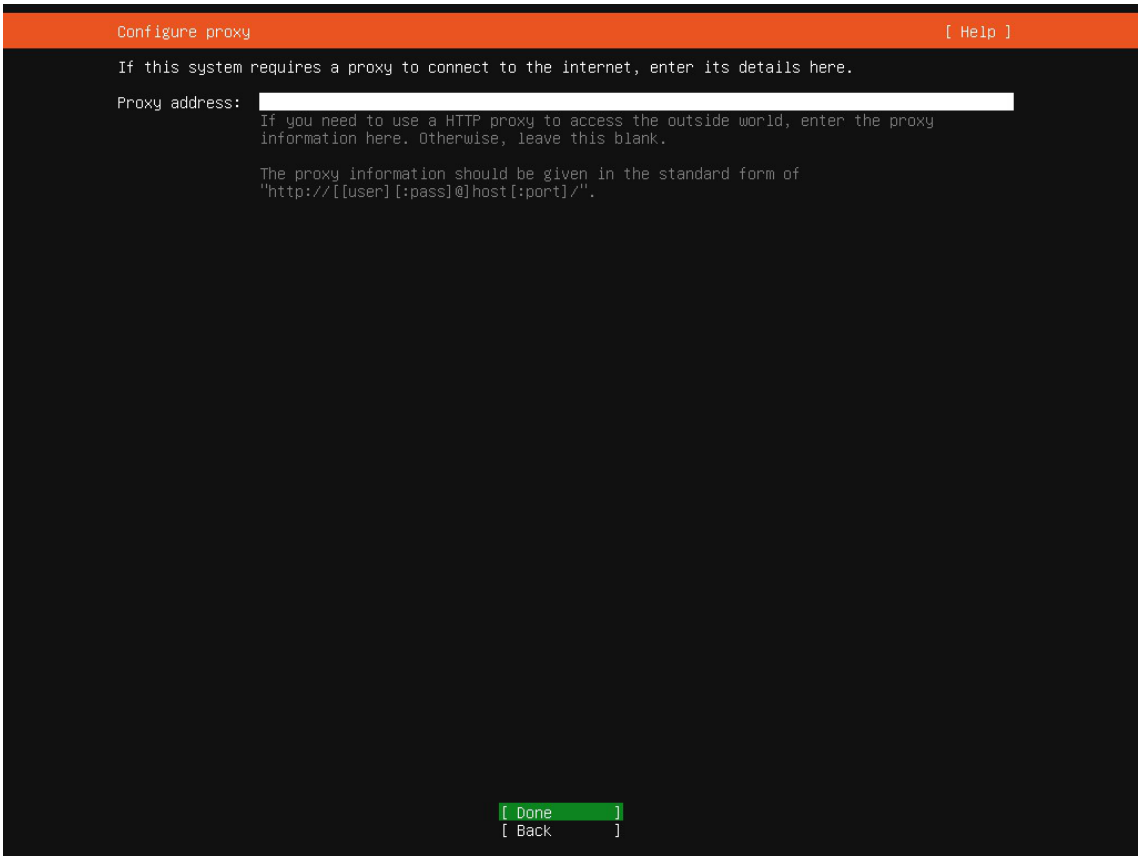
L'installation se déroule en deux phases principales : le démarrage du système contenu sur le live CD[p. 718] jusqu'à la cible Cloud-init puis les traitements délégués à Cloud-init, qui constituent l'installation proprement dite des composants du module.

Les différentes phases de traitement de Cloud-init sont :

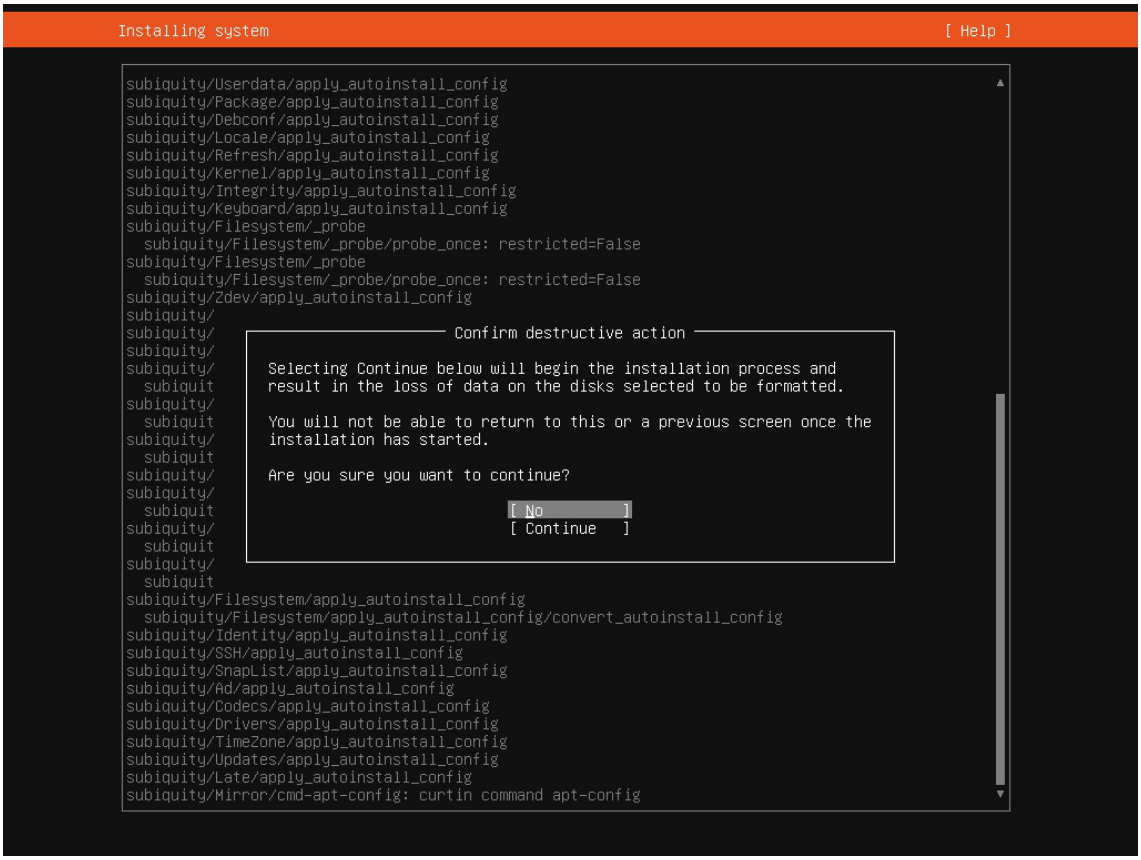
1. la configuration du réseau ;



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



2. la configuration du gestionnaire de paquets ;
3. le partitionnement automatique utilisant LVM[p.719] ;

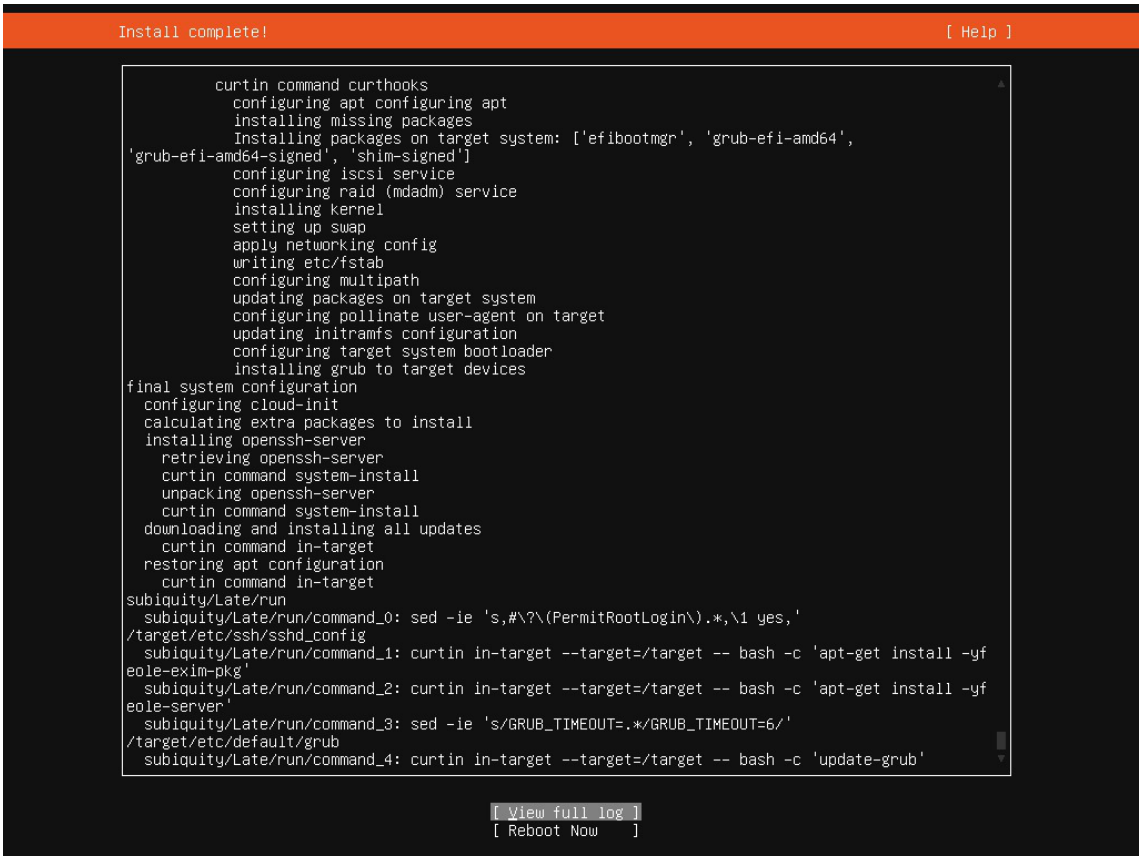


4. la configuration du boot UEFI[p.733] ;
5. la création des images de démarrage ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

6. installation du programme de démarrage GNU GRUB[p.713] ;
7. installation des paquets définissant le module ;
8. fin de l'installation.

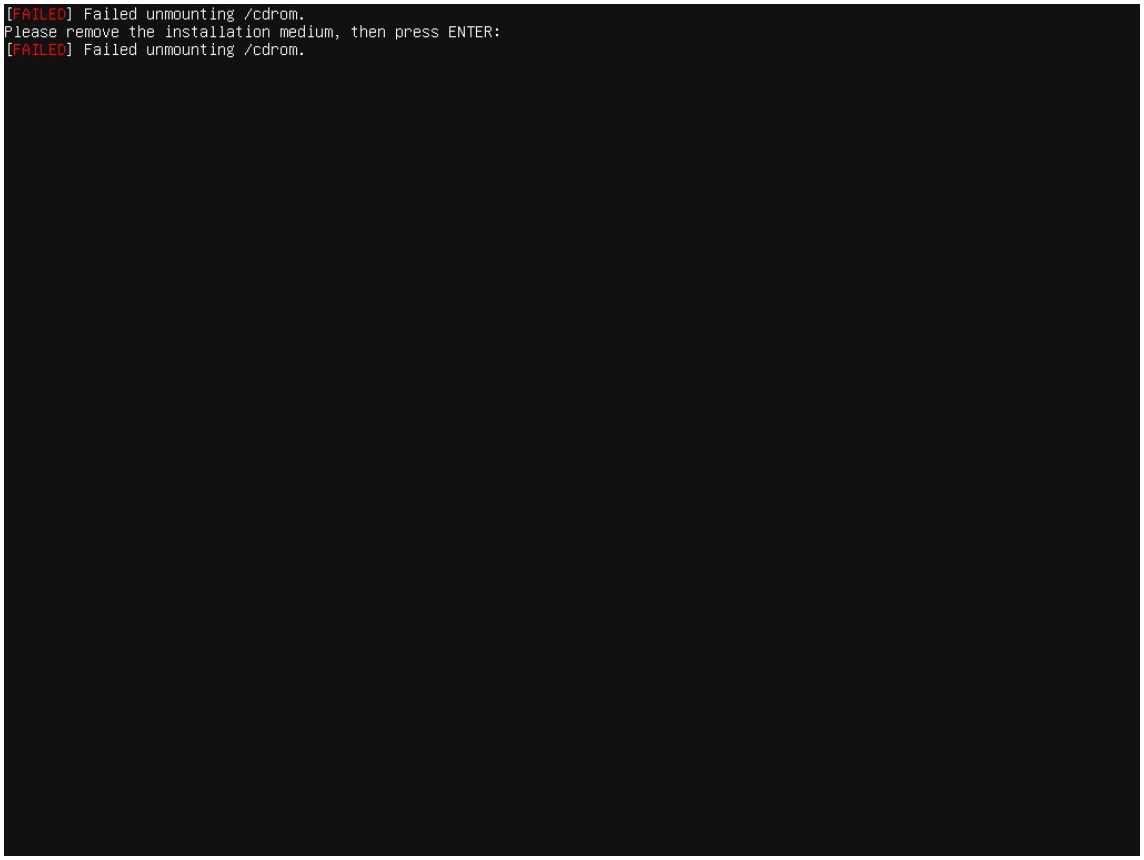
À la fin de l'installation, le système propose de redémarrer.



En validant `Reboot now`, le système redémarrera quand l'installation sera terminée (cela peut prendre plusieurs minutes).

Il peut arriver l'erreur suivante :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Comme indiqué à l'écran, il suffit d'enlever le support d'installation et d'appuyer sur Entrée.

La bonne répartition de l'espace disque résultant d'un partitionnement automatique n'est pas garantie 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.

Voir aussi...

Les mots de passe [p.361]

4. Partitionnement automatique

Le partitionnement automatique utilise le logiciel LVM[p.719].

À partir de la version 2.9.0, l'outil d'installation ne permet plus de configurer le partitionnement lors de la phase d'installation.

Le partitionnement s'appuyant sur LVM[p.719] peut toutefois être effectué lors de la phase de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

configuration, pour une mise en œuvre lors de la phase d'instanciation.
Se rapporter à la suite de la section pour plus de détails sur les possibilités offertes.

Ajustement du partitionnement au travers de l'interface de configuration



L'ajustement du partitionnement est disponible dans l'interface de configuration du module en mode expert et ce uniquement :

- avant l'instance
- si le partitionnement à l'installation depuis l'ISO n'a pas été modifié

Pour maîtriser correctement ce qui va être fait il faut consulter l'état du partitionnement avant de saisir les paramètres souhaités à l'aide de la commande `df -h /` et des commandes `vgdisplay` et `lvdisplay`.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     2,1G  6,5G  25% /
tmpfs                          1000M      28K 1000M   1% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     2,9M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
root@eolebase:~#
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  8
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       5550 / 21,68 GiB
  Free  PE / Size       4510 / 17,62 GiB
  VG UUID               ctPVcP-76Se-EpMp-FLO3-13aR-Ghg9-PdIdUW

root@scribe:~#
```

```
root@scribe:~# lvdisplay

  --- Logical volume ---
  LV Path                /dev/scribe-vg/root
  LV Name                root
  VG Name                scribe-vg
  LV UUID                uN8emF-hD9j-eNwv-zdaC-mEeK-9XGe-uBu2OU
```

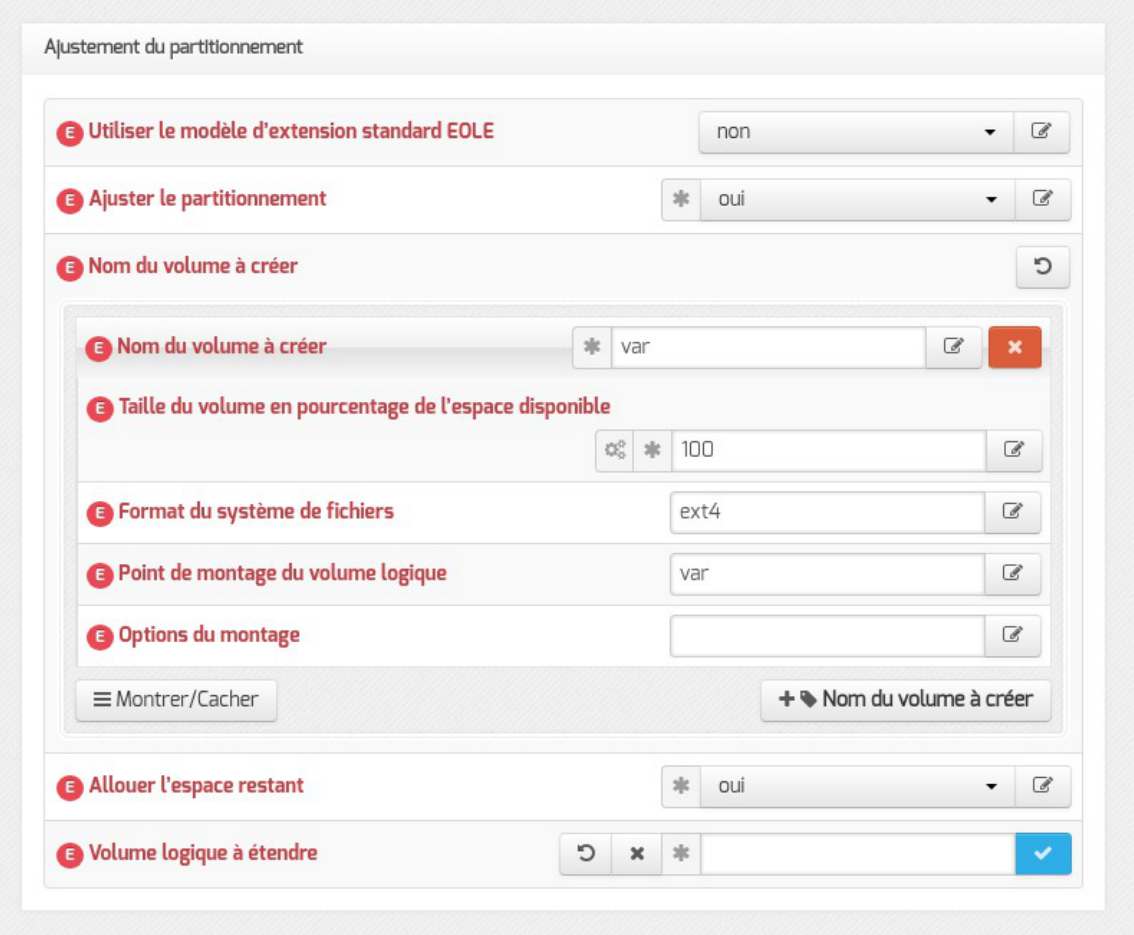

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-10-05 18:37:11 +0200
  LV Status              available
  # open                 1
  LV Size                8,94 GiB
  Current LE             2288
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:0

[...]
```

Ajuster le partitionnement

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques et d'ajouter de l'espace à des partitions existantes.

Pour ajuster le partitionnement à partir de la version 2.6.2 d'EOLE, ouvrir l'interface de configuration du module, passer en mode Expert et se rendre dans l'onglet `Système`. Puis il faut passer `Utiliser le modèle d'extension standard EOLE` à `non` pour ajuster le partitionnement.



Ajustement du partitionnement à partir d'EOLE 2.6.2

Après avoir passer `Ajuster le partitionnement` à `oui`, les partitions existantes sont affichées et un certain nombre de paramètres s'affichent.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;
- point de montage ;
- les options du montage (indispensable pour la gestion des quotas par exemple).

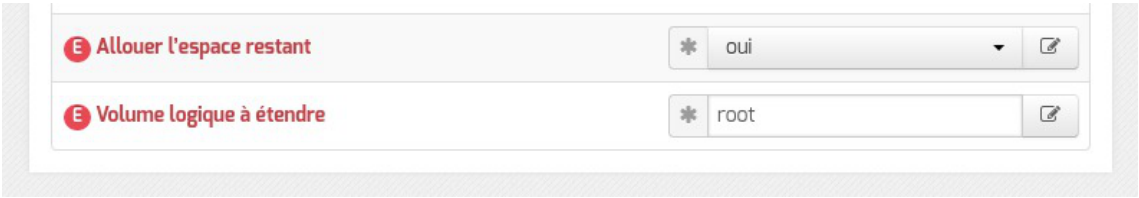
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

Allouer l'espace restant

Positionner la variable `Allouer l'espace restant` à `oui` permet de choisir un volume existant auquel ajouter la totalité de l'espace libre restant.



La valeur à saisir est la partie du nom du volume qui permet d'identifier le point de montage, par exemple pour le volume `/dev/mapper/eolebase--vg-root` il faut saisir `root` dans le nom du `Volume logique à étendre`. S'il ne reste pas d'espace, ce jeu de paramètres est sans effet.

Résultat après instance

Le paramétrage est effectif après l'instanciation du module.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     1,9G  6,7G  22% /
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
tmpfs                          1000M        0 1000M   0% /dev/shm
tmpfs                           5,0M        0  5,0M   0% /run/lock
tmpfs                          1000M        0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M    107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G    3,6M  1,7G   1% /tmp
tmpfs                           200M        0  200M   0% /run/user/0
/dev/mapper/eolebase--vg-var     27G    311M   25G   2% /var
root@eolebase:~#
```

Le nouveau volume logique est présent et la partition `/root` s'est vu augmentée du reste de l'espace libre.

Ajustement du partitionnement avec les outils dédiés LVM

Ajouter de l'espace disque à un volume LVM

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

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



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

Démonter la partition

Pour démonter la partition

```
# umount /var
```

Créer un volume physique

Créer un volume physique avec la nouvelle partition :

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

Quel est le groupe de volumes

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

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

```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
root@scribe:/dev/mapper#
```

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

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

Agrandir le volume logique

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

```
# lvextend -l +100%FREE /dev/scribe-vg/var
# e2fsck -f /dev/scribe-vg/var
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM



Sur un serveur où une partition est saturée.

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

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.
Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

Vérifier l'intégrité du système du système de fichiers :

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

Vérifier l'espace libéré

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

```
# vgdisplay
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  6
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       10060 / 39,30 GiB
  Free  PE / Size       0 / 0
  VG UUID               hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3

root@scribe:~#
```

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

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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

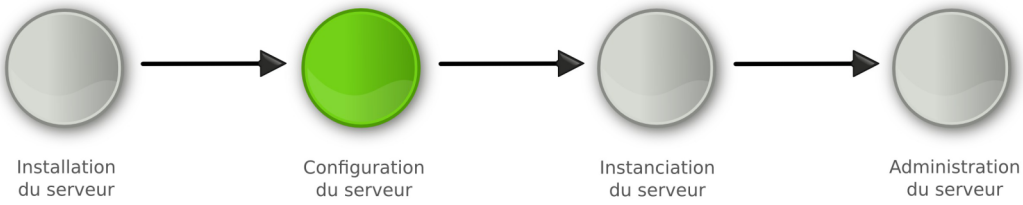


Pensez à redémarrer les services qui ont précédemment été arrêtés.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 6

Configuration du module Amon



Configuration

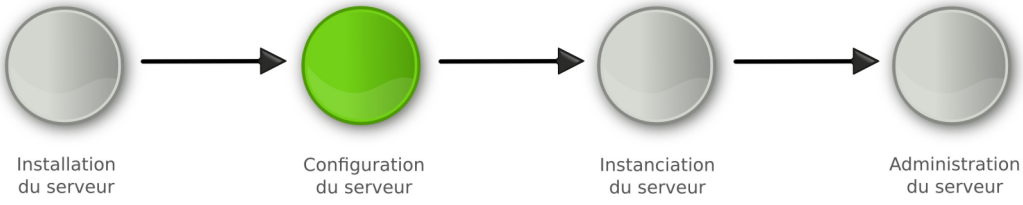
- La **phase de configuration** s'effectue au moyen de l'interface de configuration du module, celle-ci se lance avec la commande `gen_config` .

  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 première interface réseau 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.731], e2guardian[p.710], etc.

1. Configuration généralités



Configuration

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.709], l'adresse du serveur de temps NTP[p.723], ...). 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 bénéficier 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`.

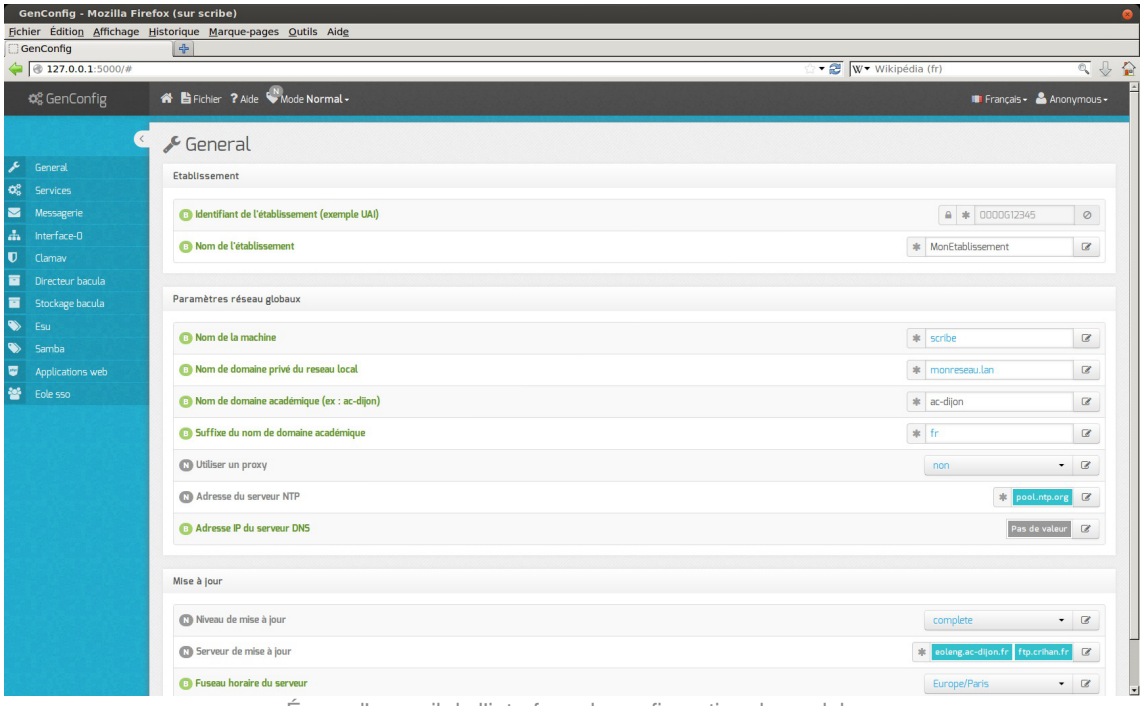
Il est donc possible d'utiliser le fichier `config.eol` d'un serveur en production pour en *instancier* un nouveau.



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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

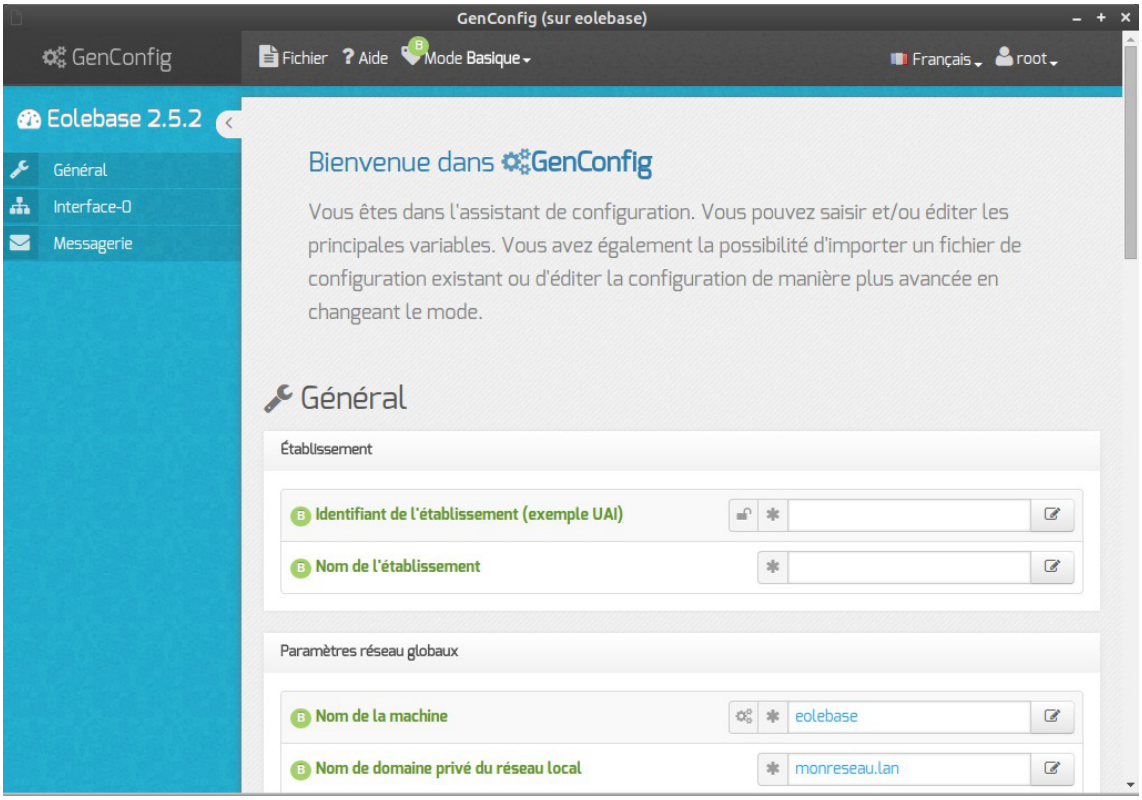
Une fois la commande `gen_config` lancée, comme indiqué dans la mire, vous devez ouvrir une session avec l'utilisateur **root** et le **mot de passe aléatoire** généré à l'installation.



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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

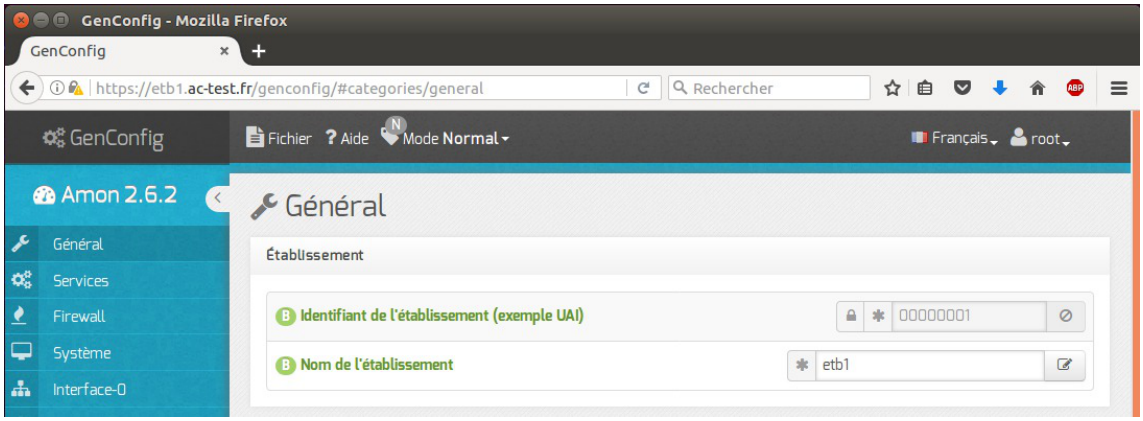
1.1.1. Accès distant

Accès distant via le port 443

Après instance ou reconfigure, l'interface de configuration du module est accessible pour les adresses IP autorisées à administrer le serveur via SSH, depuis un navigateur web en HTTPS à l'adresse suivante :

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Vue de l'interface de configuration au travers d'un navigateur web (port 443)

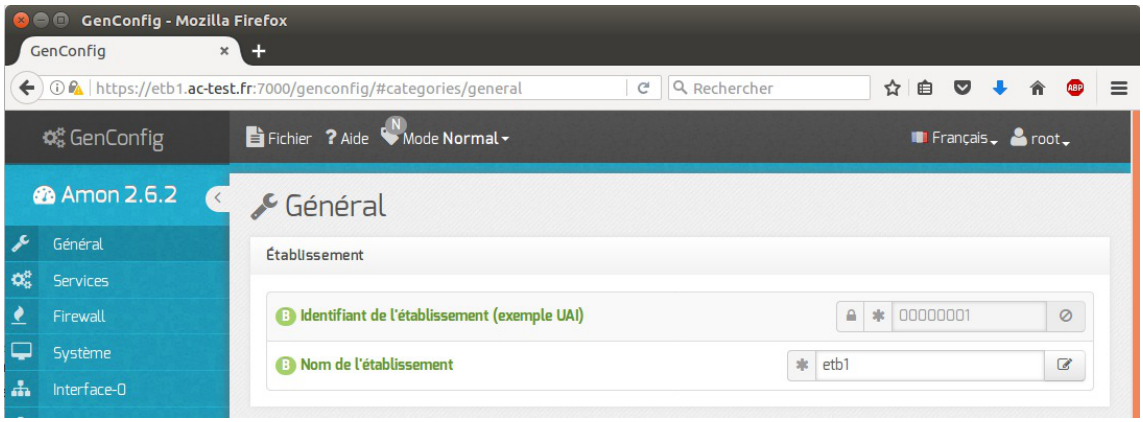
En fonction des certificats mis en place sur le module, il peut s'avérer nécessaire de les accepter pour accéder à l'interface.

La variable experte `Activer l'interface de configuration du module (GenConfig)` de l'onglet `Services` permet de désactiver la publication de l'interface sur le port `443`.

> Pour autoriser l'accès distant depuis 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`.

Accès distant via le port historique

Après instance ou reconfigure, l'interface de configuration du module est accessible pour les adresses IP autorisées à administrer le serveur via SSH, 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`.



Vue de l'interface de configuration au travers d'un navigateur web (port 7000)

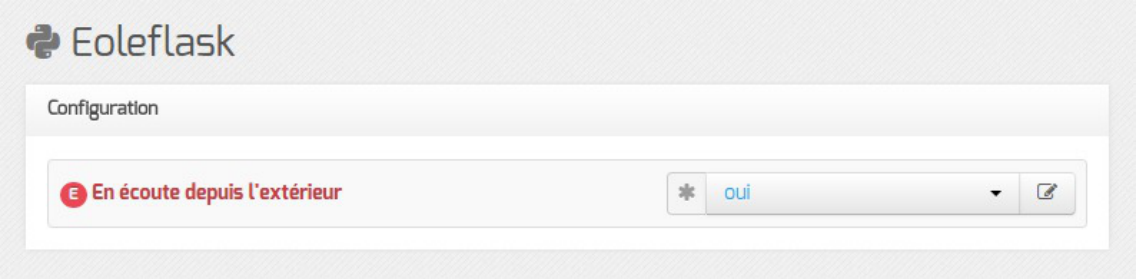
En fonction des certificats mis en place sur le module, il peut s'avérer nécessaire de les accepter pour accéder à l'interface.

> Pour autoriser l'accès distant depuis une ou plusieurs adresses IP, il faut le déclarer explicitement dans l'onglet `Interface-n` de l'interface de configuration du module en passant

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

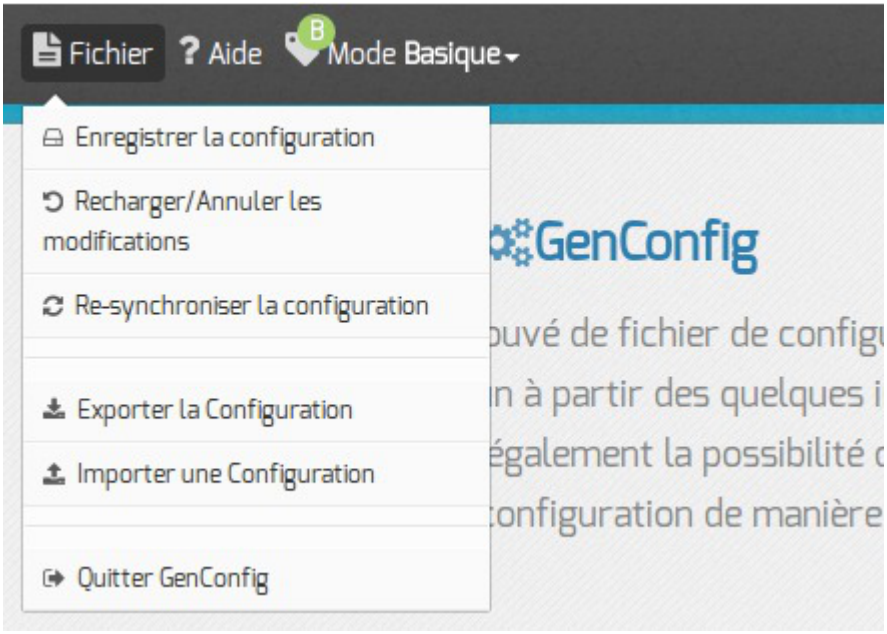
La zone de Menu, en haut de l'interface, propose les items suivants :

- 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-syncroniser la configuration
- Exporter la configuration
- Importer une configuration
- Quitter GenConfig

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

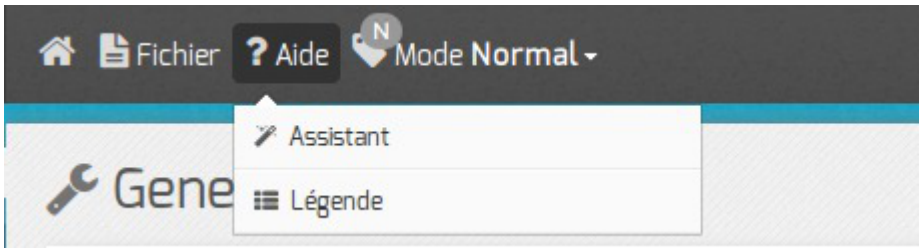
Re-synchroniser la configuration permet de récupérer les informations stockées en session sur le serveur si une coupure arrivait pendant la configuration.

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.

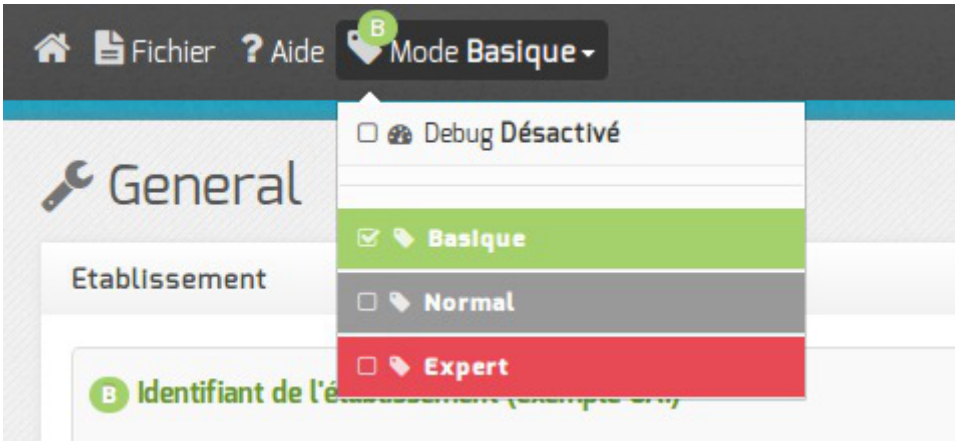
La légende présente un récapitulatif des différentes icônes que l'on peut rencontrer dans l'interface.

Sous-menu Mode

- Debug
- Basique

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

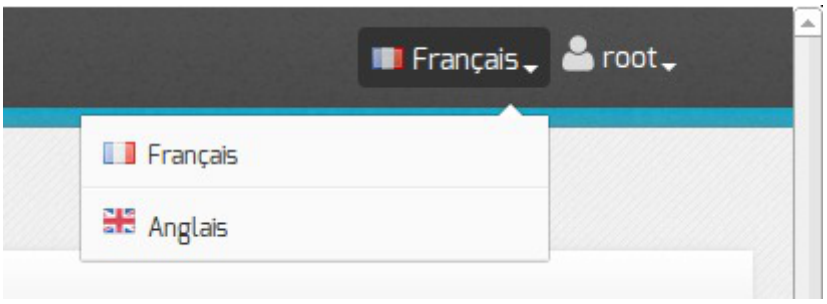
Le mode *Expert* active les onglets et les variables pour une configuration avancée.

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

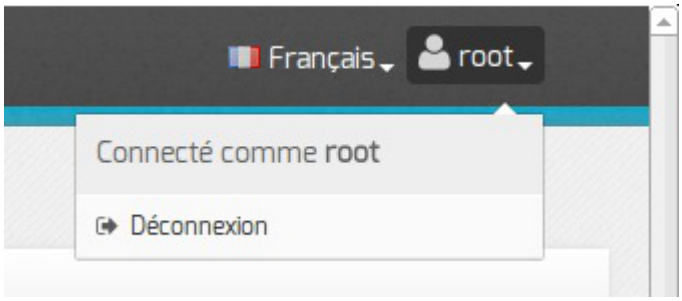


Langue permet de choisir la langue utilisé dans l'interface.

Sous-menu Session

- Connecté comme
- Déconnexion

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



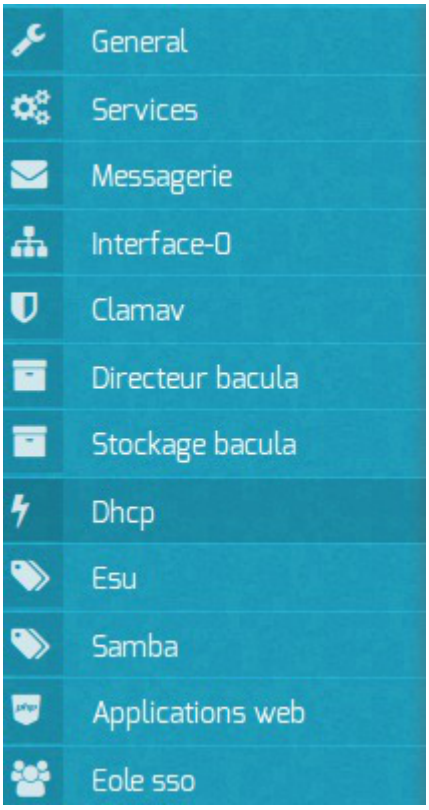
Session permet de connaître l'utilisateur courant et de se déconnecter.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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).



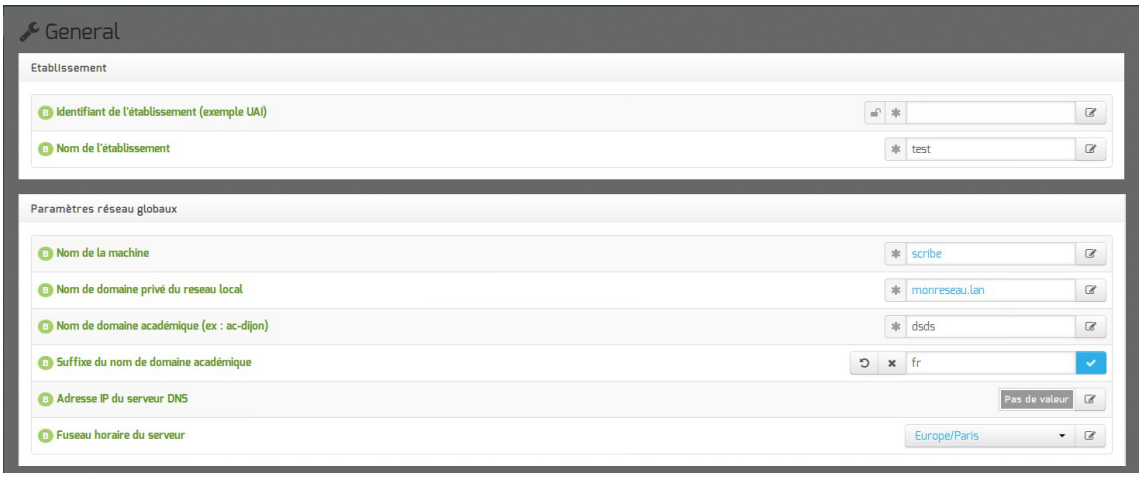
Bouton modifier sur la première ligne à droite, la deuxième ligne a le focus

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.

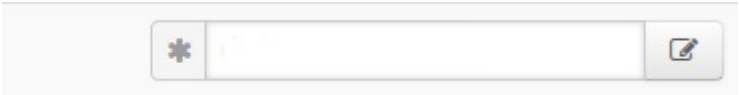


Les blocs thématiques

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les variables des modes basiques, normales et expertes

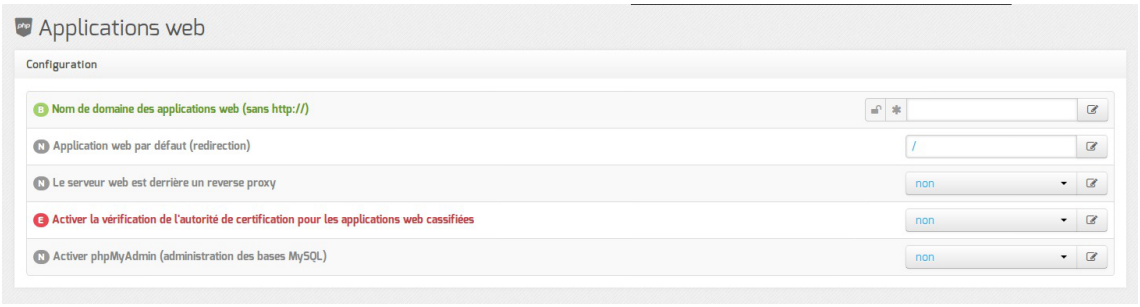
Le mode détermine l'affiche de variable plus ou moins complexes : basiques, normales ou expertes.

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.

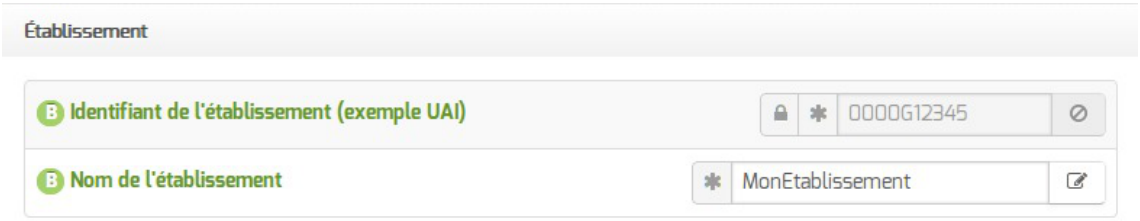


Les variables et leur niveau de complexité

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).



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.



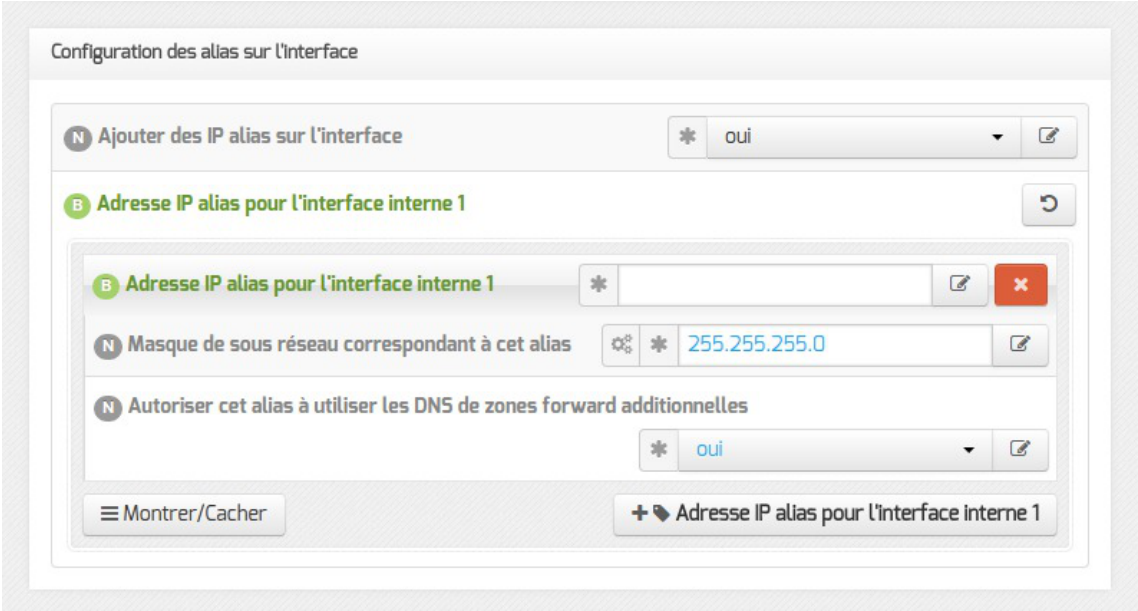
Édition d'une variable multiple

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 :

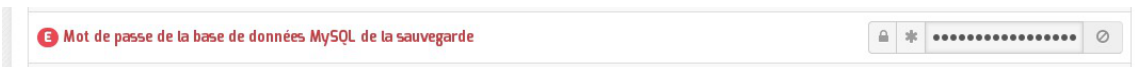
- bleu pour une variable dont la valeur est la valeur par défaut ;
- noir pour une variable dont la valeur est modifiée par l'utilisateur et validée.



Les variables brouillées

Certaines variables sensibles ont un affichage brouillé dès lors qu'elles sont validées. Le contenu de la variable est remplacé par une série de points.

Ces variables sont de nouveau visibles lorsqu'elles sont éditées.



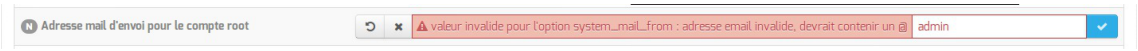
Validation des variables

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.



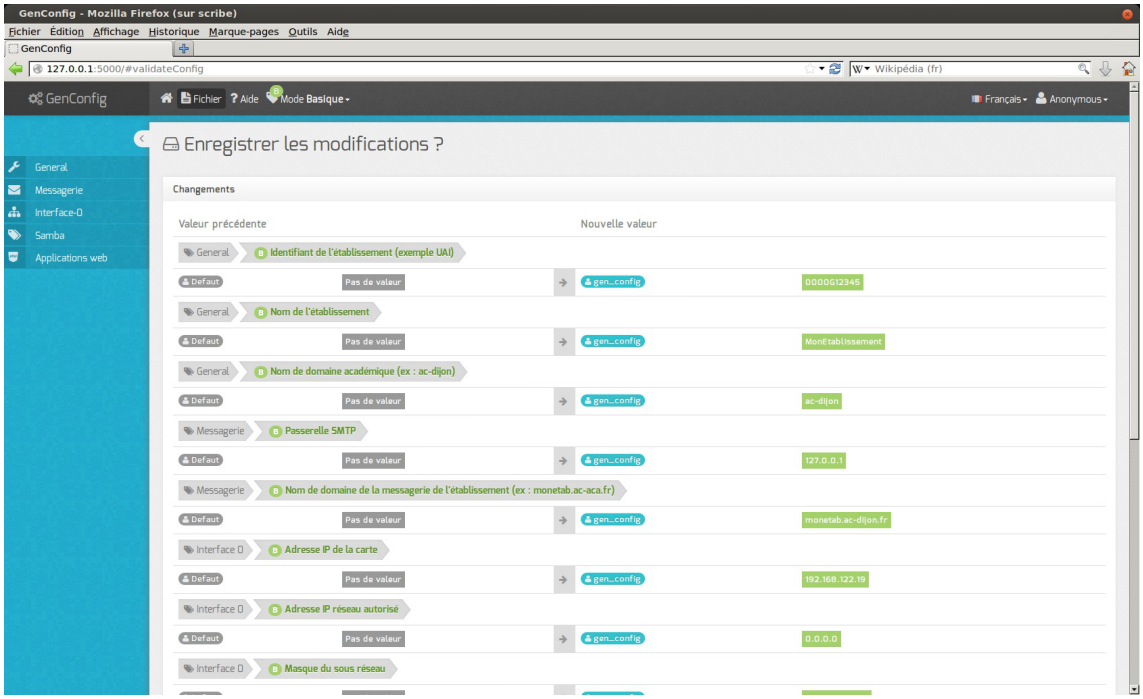
Validation d'une variable

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.

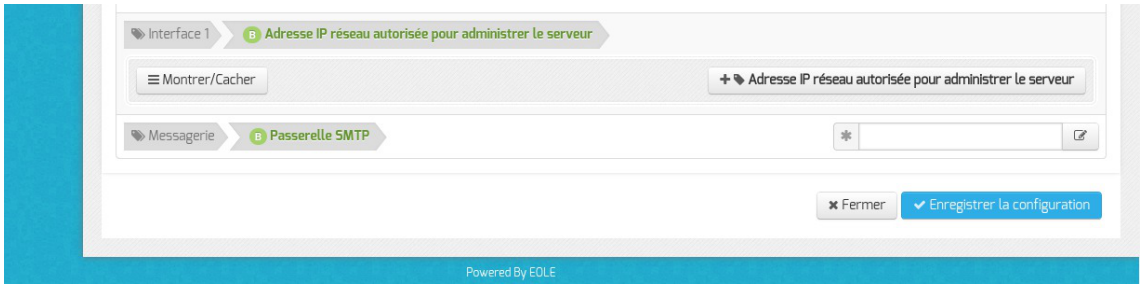
Lors d'une réédition de la configuration cette zone ne montre que les changements qui ont eu lieu.



Zone de validation

1.1.6. Enregistrer la configuration

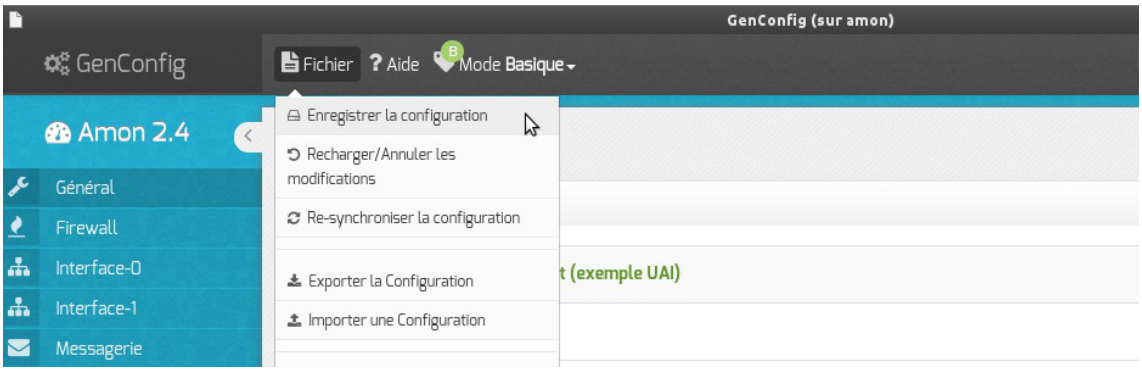
L'utilisation du mode assistant propose l'enregistrement de la configuration en bas de page avec le bouton `Enregistrer la configuration`.



Dans les autres cas l'enregistrement de la configuration se fait en cliquant sur `Enregistrer` la

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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.716] 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 sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.
>
> Cela permet de conserver la dernière configuration fonctionnelle du serveur.
>
> À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.
>
> S'il existe une différence entre `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'a pas encore été 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.733] 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.713].

> 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`) ;
- `forced` : valeur par défaut enregistrée d'office pour les variables à verrouillage automatique (**auto_freeze**) ou à enregistrement obligatoire (**auto_save**) ;
- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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"}
```

Le mode *Debug* permet également d'afficher les valeurs des variables verrouillées de type *password*, dont l'affichage est normalement brouillé.



Lorsque le champ est trop petit par rapport à la valeur, celle-ci est tronquée. L'info-bulle qui s'affiche au survol du champ permet toutefois de prendre connaissance de la valeur complète.



Voir aussi...

La zone Menu [p.60]

1.1.8. Édition synchronisée avec l'application Zéphir

Lorsque le module est enregistré sur un module Zéphir, il est possible de gérer la configuration en mode synchronisé.

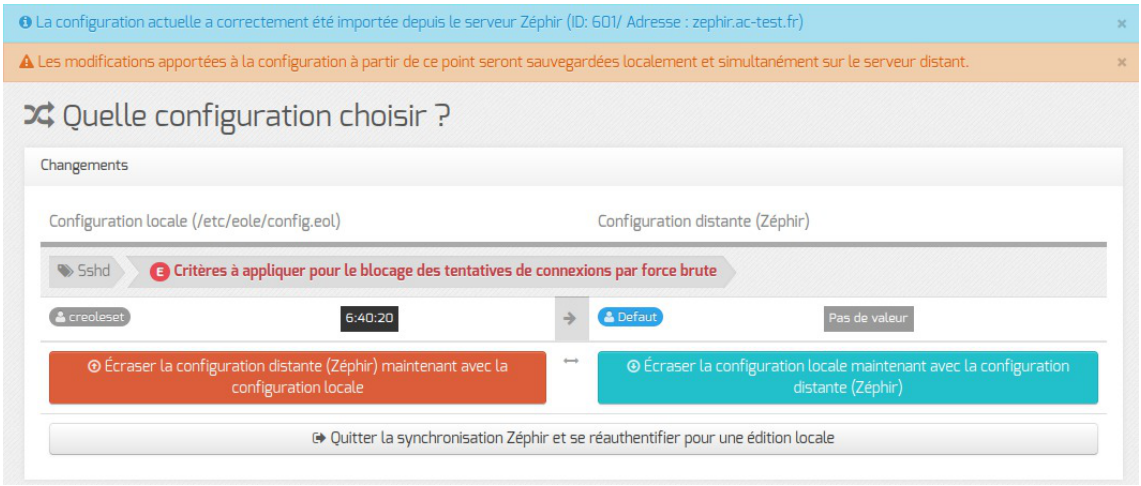
Pour cela, il est nécessaire de se connecter à l'application de configuration du module avec un compte de l'application Zéphir disposant des droits suffisants (`Lecture` et `Configuration et action sur les serveurs`). La mire de connexion de l'application de configuration du module propose cette option.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



En mode synchronisé, la configuration locale du module est comparée à la configuration associée au module dans l'application Zéphir.

En cas de différence, une page spéciale est affichée avant de pouvoir accéder à la modification de la configuration.



Cette page indique que la configuration a correctement été importée depuis l'application Zéphir en rappelant l'ID associé au module dans cette même application, ainsi que l'adresse du serveur Zéphir interrogé.

Cette page avertit également que le mode synchronisé, activé depuis la mire de connexion, implique que les modifications apportées à la configuration seront appliquées localement et sur l'application Zéphir.

Cette synchronisation interdisant la divergence entre la configuration appliquée localement et la configuration associé au module dans l'application Zéphir, la page propose de choisir quelle version,

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

globalement, doit devenir la nouvelle référence en l'utilisant pour remplacer l'autre.

Les différences sont affichées sous la forme d'un tableau avec l'origine en colonnes et les variables en lignes. Seules les variables dont les valeurs sont différentes localement et dans l'application Zéphir sont affichées.

Sous la colonne de gauche, reprenant les valeurs locales, le bouton rouge permet de remplacer les valeurs de l'application Zéphir par ces valeurs locales.

Symétriquement, sous la colonne de droite, reprenant les valeurs de l'application Zéphir, le bouton bleu permet de remplacer les valeurs locales par ces valeurs de l'application Zéphir.

Dans le cas très particulier où la synchronisation n'est finalement pas souhaitée, la page des différences permet de se déconnecter et de quitter ainsi le mode synchronisé et donner l'occasion de se connecter avec un compte d'administration local, avant que les configurations, locale et distante, ne soient altérées.



Les droits attribués aux utilisateurs de l'application Zéphir dissocient la lecture et la sauvegarde de la configuration. Ainsi, le droit `Lecture` est nécessaire et suffisant pour se connecter en mode synchronisé et afficher la configuration. Par contre il ne permet pas de mettre à jour la configuration associée au module sur l'application Zéphir.

1.1.9. 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`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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>/genconfig/`

ou : `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.eol.bak` est sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.733] 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.713].



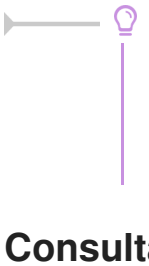
La valeur de timeout peut être changée à la ligne `timeout = '120'` dans le fichier de configuration de eoleflask : `/etc/eole/flask/eoleflask.conf`. Celui-ci n'est pas templatisé et n'est donc pas écrasé en cas de reconfiguration du serveur.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

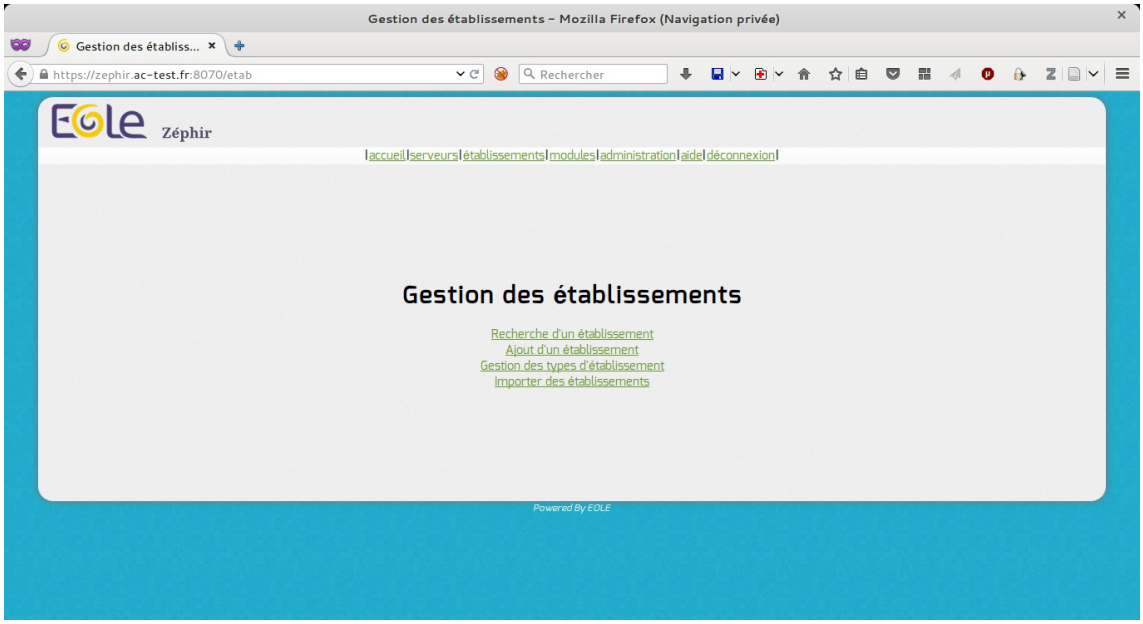
L'établissement d'appartenance du serveur doit déjà exister dans la base des serveurs.



La procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

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`.



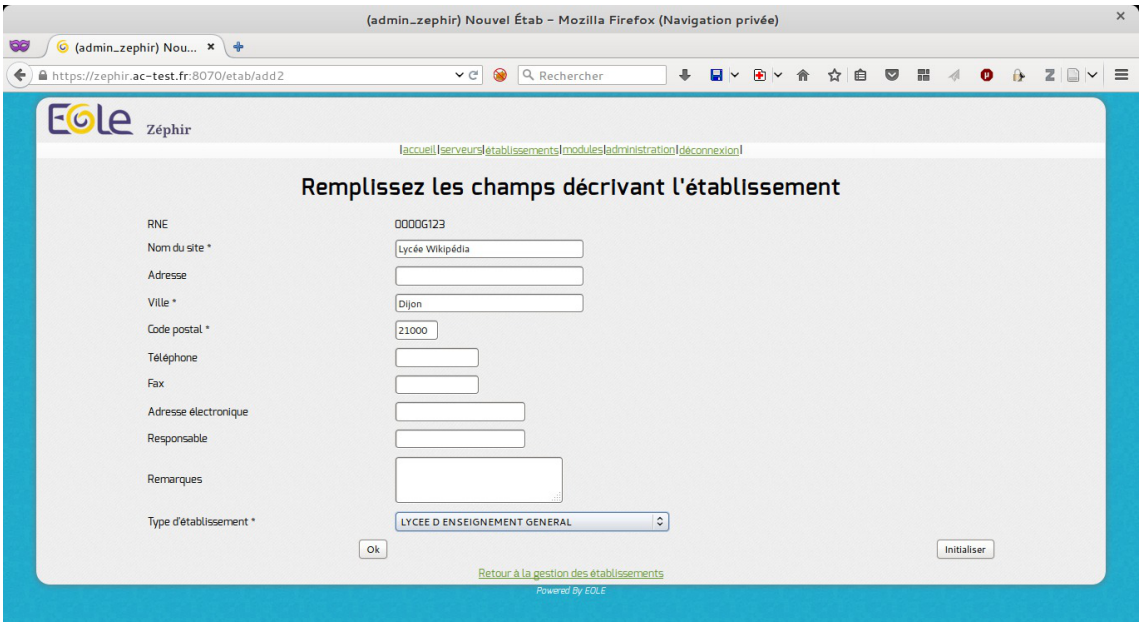
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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, ...).



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.



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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'importation nécessite un fichier (par exemple extrait de la base de donnée Ramsese[p.728]) CSV[p.708] 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.



L'enregistrement d'un serveur

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.



Dans le cas d'utilisation de certificats non reconnus par une autorité de certification la procédure d'enregistrement nécessite d'être en possession du certificat de la CA locale du serveur Zéphir ou d'avoir les droits suffisants pour le récupérer en SSH.

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 (ens4 par défaut) :
adresse_ip ens4 : 192.168.240.100
masque de réseau pour ens4 : 255.255.255.0
adresse de la passerelle : 192.168.240.254
adresse du serveur DNS (ou rien) : 192.168.240.1
root@scribe:~#
```

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 une configuration réseau particulière est nécessaire au moment de l'enregistrement, exécuter la commande `enregistrement_zephir` avec l'option `--force`.

Déroulement de l'enregistrement

- lancer la procédure d'enregistrement à l'aide de la commande `enregistrement_zephir` ;
- 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 ;
- dans le cas d'utilisation de certificats non reconnus par une autorité de certification, il faut, pour procéder à l'enregistrement d'un serveur, copier le certificat de la CA locale du serveur Zéphir `/etc/ssl/certs/ca_local.crt` sur la machine à enregistrer dans le répertoire `/usr/local/share/ca-certificates/` et mettre à jour les certificats sur la machine locale à l'aide de la commande `update-ca-certificates` ;
- relancer la procédure d'enregistrement avec la commande `enregistrement_zephir` ;
- si le serveur n'a pas été pré-créé sur le serveur Zéphir, répondre `oui` à la question `Créer le serveur dans la base Zéphir ?` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

Certificat de Zéphir non validé !

 utiliser sur Zéphir un certificat signé par une autorité reconnue,
  ou
 Copier le fichier /etc/ssl/certs/ca_local.crt de Zéphir dans
 /usr/local/share/ca-certificates et lancer update-ca-certificates.
root@eolebase:~#

root@eolebase:~# scp root@zephir.ac-test.fr:/etc/ssl/certs/ca_local.crt /usr/local/share/ca-certificates/
Warning: Permanently added 'zephir.ac-test.fr,192.168.0.20' (ECDSA) to the list of known hosts.
root@zephir.ac-test.fr's password:
ca_local.crt
100% 1736     1.7KB/s   00:00
root@eolebase:~#

root@eolebase:~# update-ca-certificates
Updating certificates in /etc/ssl/certs...
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate eole.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate infrastructures.pem
WARNING: Skipping duplicate certificate ca.crt
WARNING: Skipping duplicate certificate ca.crt
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
root@eolebase:~#

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 **
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
84
85 1 -> Ne rien faire
86 2 -> Récupérer les fichiers de variante sur le serveur Zéphir
87 3 -> Sauver la configuration actuelle sur le serveur Zéphir
88 4 -> Modifier la variante du serveur
89
90 Entrez le numéro de votre choix : 3
91 Pour l'enregistrement il faut choisir l'option 3.
92
93 -- sauvegarde en cours (veuillez patienter) --
94 -- OK --
95
96 --récupération des patchs et dictionnaires (veuillez patienter)--
97 ** le numéro attribué à ce serveur sur le serveur Zéphir est : 1 **
98 root@eolebase:~#
```

Le module est correctement enregistré sur le serveur Zéphir.

Enregistrement sans question

Il est possible d'enregistrer un module sans interagir avec la commande `enregistrement_zephir`.

Pour cela, il suffit de passer en argument les réponses aux questions normalement posées par la commande.

Les arguments possibles à donner dans la commande sont :

`-h, --help` Affiche le message d'aide

`-c, --check` Vérification seulement, affiche l'identifiant du serveur stocké dans l'application Zéphir et retourne 0 si le serveur est enregistré, 1 sinon

`-p, --pppoe` Si le réseau n'est pas encore configuré, cette option permet la mise en place d'une connexion par PPPoE

`-f, --force` Force la mise en place d'un configuration minimale du réseau même si le serveur est déjà configuré

`--adresse_zephir ADRESSE_ZEPHIR` Nom DNS du serveur Zéphir

`--user USER` Login pour l'application Zéphir

`--password PASSWORD` Mot de passe pour l'application Zéphir

`--id_serveur ID_SERVEUR` N° identifiant le serveur l'application Zéphir

`--choix {1,2,3,4}` Numéro de votre choix d'échange avec le Zéphir

`--force_enregistrement` Force l'enregistrement même si un serveur est déjà enregistré

Les 4 choix possibles sont :

1 -> Ne rien faire

2 -> Utiliser la configuration définie sur le serveur Zéphir

3 -> Sauver la configuration actuelle sur le serveur Zéphir

4 -> Modifier la variante du serveur



Exemple : pour enregistrer mon serveur numéro 25 et sauver la configuration actuelle sur le serveur Zéphir, je me connecte sur mon serveur (n°25) puis :

```
1 root@eolebase:~# enregistrement_zephir --adresse_zephir zephir.ac-test.fr
  --user admin_zephir --password mdp_admin_zephir --id_serveur 25 --choix 3
2  Procédure d'enregistrement sur le serveur Zéphir
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
** utilisation d'un serveur existant dans la base du serveur Zéphir **

Vérification des informations sur le matériel

Mise à jour des informations sur le matériel
** Configuration des communications vers le serveur Zéphir **

  -- sauvegarde en cours (veuillez patienter) --
INFO:zephir-client:save_files()
  -- OK --
 --récupération de la configuration en cours (veuillez patienter)--
** attente de la mise en place des fichiers **
** Vérification des dictionnaires et de la configuration **
** le numéro attribué à ce serveur sur le serveur Zéphir est : 25 **

```

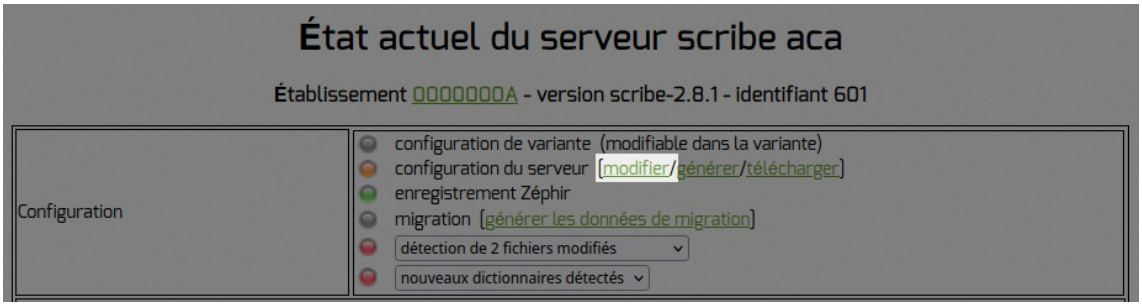
Il n'est pas possible de désinscrire un module avec un `enregistrement_zephir` sans question.

Il n'est pas possible d'enregistrer un module déjà enregistré à moins qu'il n'ait été désinscrit entre temps. Si le module a bien été désinscrit, l'utilisation de l'argument `--force_enregistrement` est alors nécessaire pour un nouvel enregistrement.

Lancement de l'interface de configuration

Une fois la procédure terminée, la configuration du module peut être effectuée depuis le serveur selon le mode autonome synchronisé (cf. Édition synchronisée avec l'application Zéphir) [p.70] ou depuis l'application Zéphir.

Sur l'application Zéphir, l'application de configuration du module est accessible depuis la page d'état du serveur via le lien `modifier` affiché dans la section Configuration du tableau,

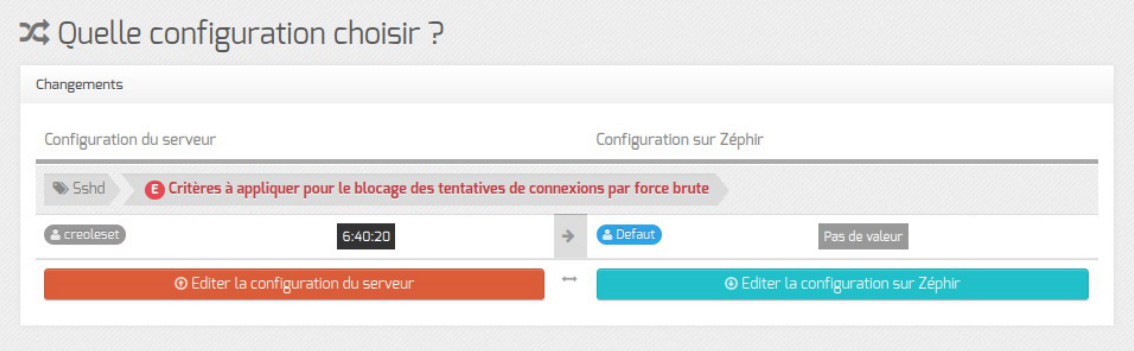


Cette application de configuration du module se comporte de manière semblable à celle exécutée depuis le serveur lui-même à quelques détails près :

- certains calculs et contraintes nécessitant l'accès direct au serveur configuré sont désactivés ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- la page de différences entre la configuration appliquée sur le module et la configuration associée au module dans l'application Zéphir n'est disponible que pour les modules à jour à partir de la version 2.8.1 et à condition qu'une première synchronisation ait été effectuée sans erreur.
- cette page de différences est simplifiée.



En cas de différences entre la configuration appliquée sur le module et la configuration associée au module dans l'application Zéphir, il est demandé à l'administrateur de choisir quelle version, globalement, servira comme base de configuration pour l'édition.

La configuration éditée via cette application de configuration du module intégrée à l'application Zéphir n'est pas directement synchronisée avec celle du serveur mais nécessite une action pour l'envoyer.

Désinscription d'un serveur

Pour désinscrire un serveur il faut exécuter la commande `enregistrement_zephir` et la désinscription est proposée.

```
root@eolebase:~# enregistrement_zephir

  Procédure d'enregistrement sur le serveur Zéphir


** Ce serveur est déjà enregistré sur le serveur Zéphir **

 - n°identifiant : 454
 - adresse de Zéphir : zephir.ac-test.fr

1 -> Désinscrire ce serveur du serveur Zéphir
2 -> Relancer l'enregistrement
3 -> Ne rien faire

  Entrez le numéro de votre choix : 1

Désinscription auprès du serveur Zéphir terminée

root@eolebase:~#
```

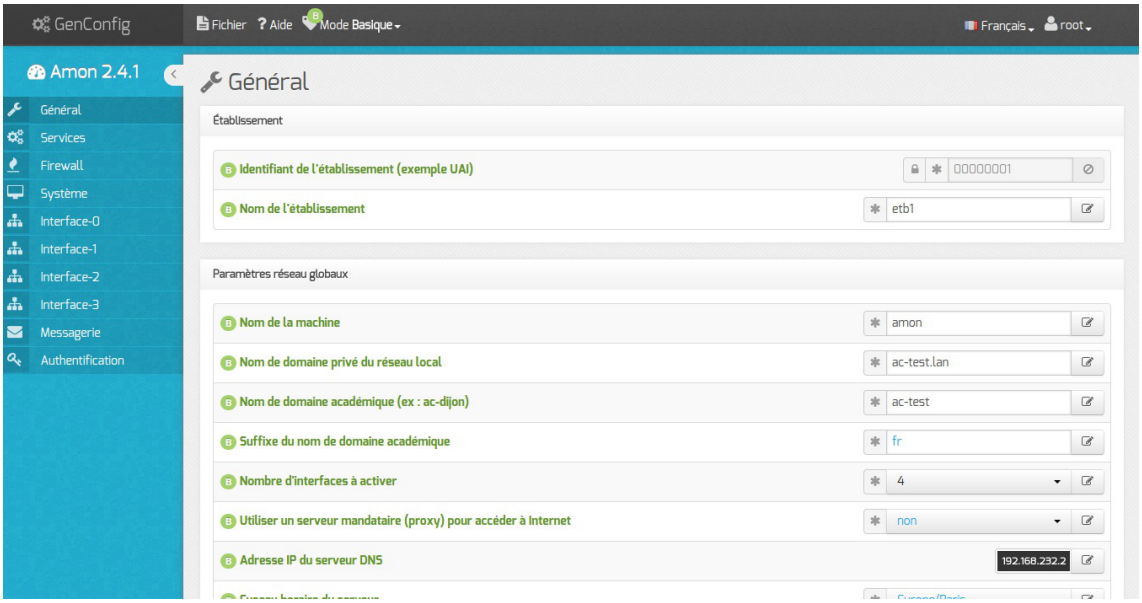
2. Configuration en mode basique

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

- `Général` ;
- `Firewall` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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



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.

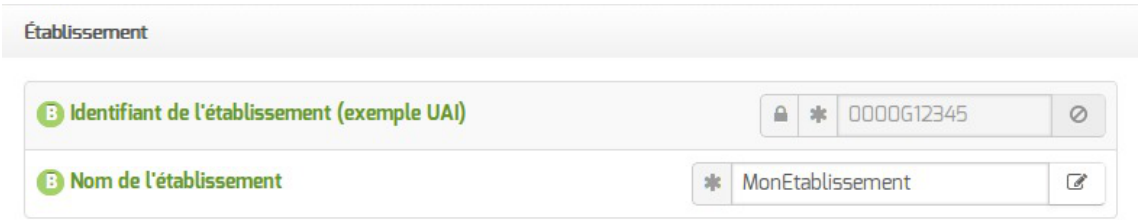
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

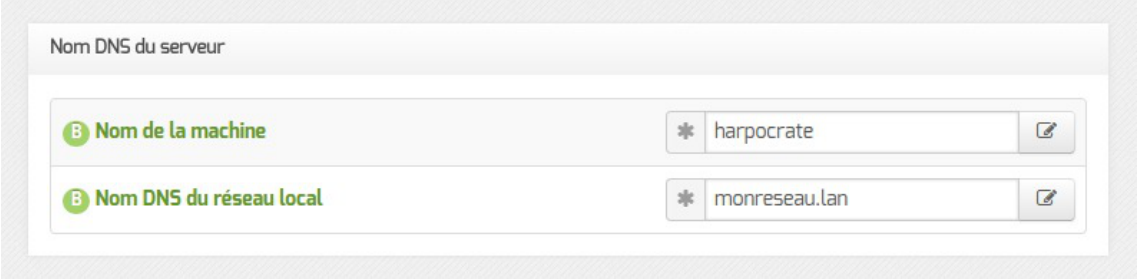
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.717] 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.

Nom DNS du serveur



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Si l'authentification `NTLM/KERBEROS` est activée sur le proxy, le `Nom de machine` ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.

Le `Nom DNS du serveur` utilise fréquemment des domaines de premier niveau du type `.lan` .

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.

Rappel : les outils mDNS (Avahi, Bonjour, ...) utilise la racine '.local'. Pour éviter les problèmes de DNS, nous vous déconseillons d'utiliser cette racine.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Paramètres réseau globaux



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

Cette information est découpée en plusieurs champs :

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

Nombre d'interfaces

Un module Amon ou AmonEcole 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait protégé par un module Amon.

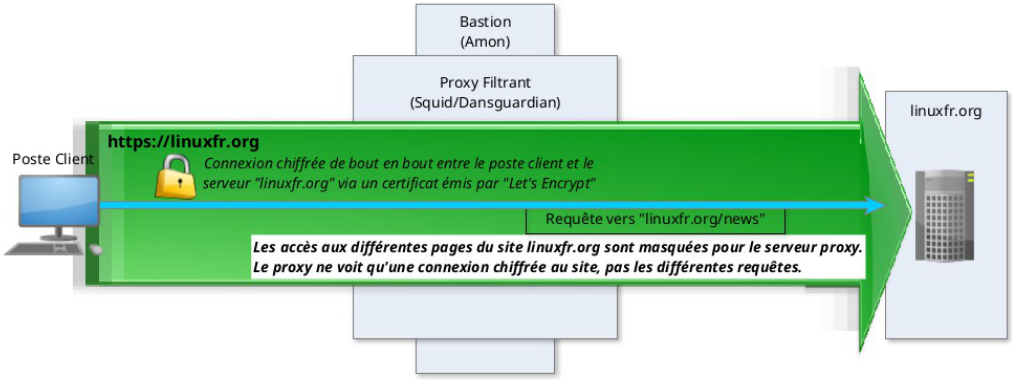
Déchiffrement et interception du protocole HTTPS

Par rapport au protocole HTTP[p.714], le protocole HTTPS permet de chiffrer la communication entre le navigateur du poste client et le serveur du site distant.

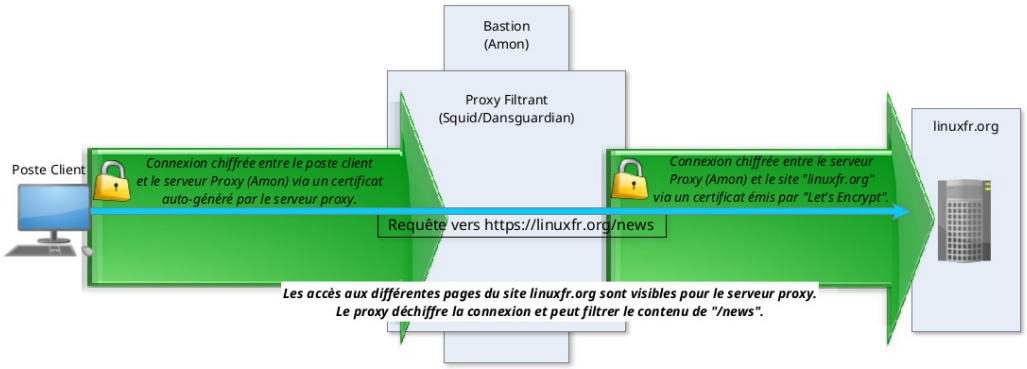
Dans ce cas, le serveur proxy ne journalise qu'une seule connexion vers le site distant (exemple : https://pcll.ac-dijon.fr) mais pas les différentes requêtes d'accès aux pages ou aux fichiers se trouvant sur ce serveur (exemple : https://pcll.ac-dijon.fr/eole/).

En HTTPS, le serveur Proxy ne peut pas filtrer le contenu des pages consultées ni scanner les fichiers téléchargés avec un antivirus.

Le déchiffrement HTTPS sur le serveur Proxy permet d'intercepter l'ensemble des requêtes et de les journaliser, de filtrer le contenu des pages visitées et de scanner les fichiers téléchargés.



Fonctionnement HTTPS normal



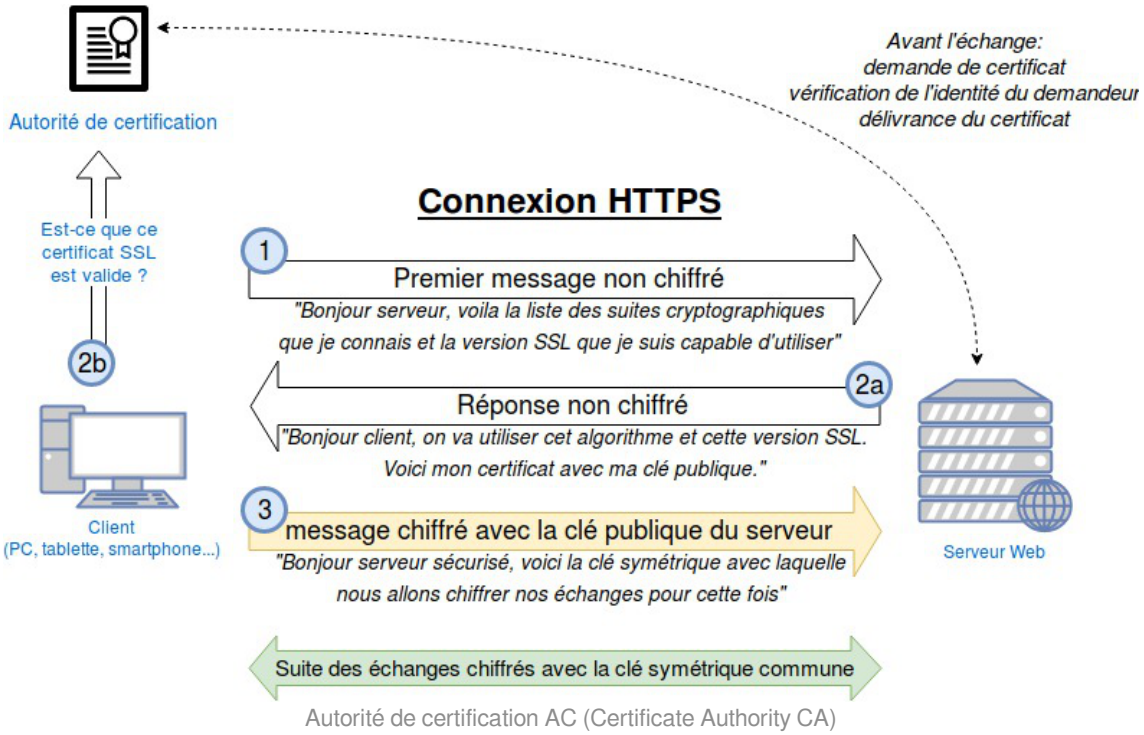
Fonctionnement HTTPS déchiffré par le Proxy

Certificat Racine de l'autorité de certification

Un certificat HTTPS est émis par une autorité de certification[p.704].

Let's Encrypt[p.717], par exemple, est une autorité de certification publique et connue des navigateurs ; son certificat racine est pré-installé dans les navigateurs et les systèmes d'exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Autorité de certification AC (Certificate Authority CA)

À partir de la version 2.8.1, le module Amon est équipé d'une fonctionnalité d'interception du trafic HTTPS. Il est possible de déclarer son certificat racine servant à sur-signer les ressources servies par le protocole HTTPS et transitant par le proxy filtrant. Cette déclaration permet d'en automatiser l'intégration dans le magasin de certificats local.

Si la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` est passée à `oui`, la variable `Le serveur mandataire intercepte les communications HTTPS` est proposée et permet elle-même de faire apparaître deux variables permettant d'identifier le certificat racine employé par le proxy filtrant.



En passant la variable `Le serveur mandataire intercepte les communications HTTPS` à `oui`, il est possible de renseigner les variables suivantes en utilisant les données affichées par la commande `diagnose` sur le module Amon :

- `Type d'empreinte du certificat racine du proxy` : SHA256 (par défaut sur Amon 2.8.1)
- `Empreinte du certificat racine du proxy` : information donnée par le diagnose du serveur Amon dans le cas où celui-ci fait office de proxy filtrant

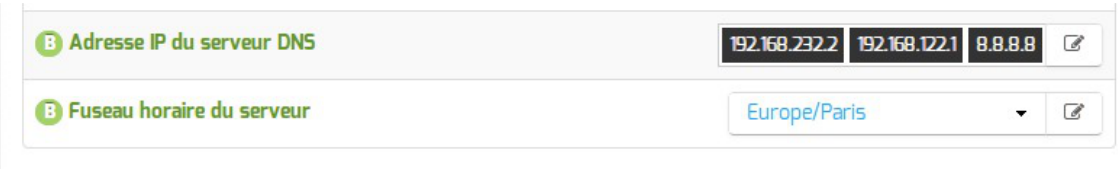
Cette configuration est nécessaire uniquement lorsque le module Amon est configuré pour l'interception des communications HTTPS.

Sur un module Amon configuré pour l'interception des communications HTTPS, la commande `diagnose` permet de connaître le chemin et l'empreinte du certificat :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
*** Validité du certificat racine du proxy (/etc/eole/squid_CA.crt)
.                signingCA.crt => Ok
.                    Empreinte => SHA256 Fingerprint=62
:1B:BF:25:28:44:31:02:7E:09:31:A6:EA:FD:A5:A8:7C:D4:EB:B6:3D:83:88:62:0F:98:85:

```

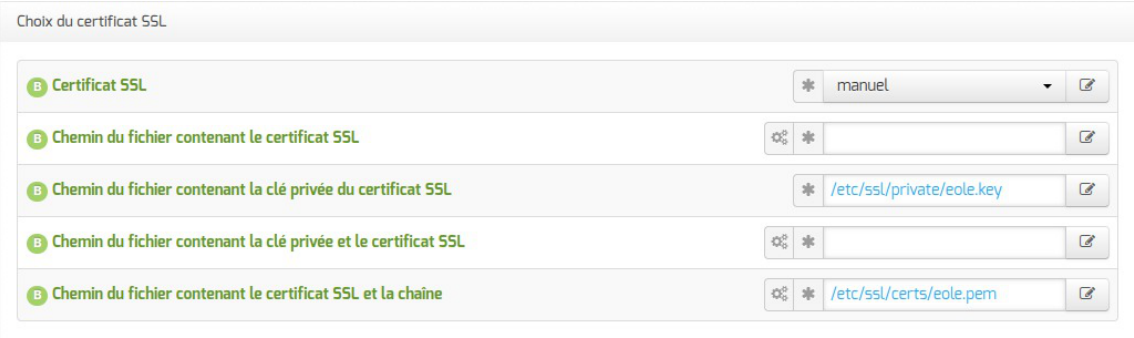
DNS et fuseau horaire



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.709].

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

Choix du certificat SSL



Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.733] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.704] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.717] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour ce faire, il faut disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

Le système de certificat utilisé repose sur une clé privée et une clé publique (le certificat) contre-signée par une autorité de certification.

Selon le contexte d'utilisation, les différents éléments de la chaîne de certification (clé privée, certificats du service ou de l'autorité de certification) doivent être combinés selon différents modes.

En mode `letsencrypt` et `autosigné`, le détail de ces combinaisons est automatique et caché.

En mode `manuel`, les variables suivantes permettent d'identifier l'emplacement des fichiers contenant les différentes combinaisons de fichiers utiles :

- `Chemin du fichier contenant le certificat SSL` : emplacement du fichier contenant uniquement le certificat ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Chemin du fichier contenant la clé privée du certificat SSL` : emplacement du fichier contenant uniquement la clé privée ;
- `Chemin du fichier contentant la clé privée et le certificat SSL` : emplacement du fichier contenant la concaténation du certificat SSL puis de la clé privée ;
- `Chemin du fichier contenant le certificat SSL et la chaîne` : emplacement du fichier contenant la concaténation du certificat SSL et des certificats intermédiaires formant la chaîne de certification à l'exclusion du certificat racine.

Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.

Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

Pour plus d'informations, consulter la partie consacrée à l'`onglet expert` `Certificats ssl` (cf. Onglet Certificats ssl : gestion des certificats SSL) [p.233].

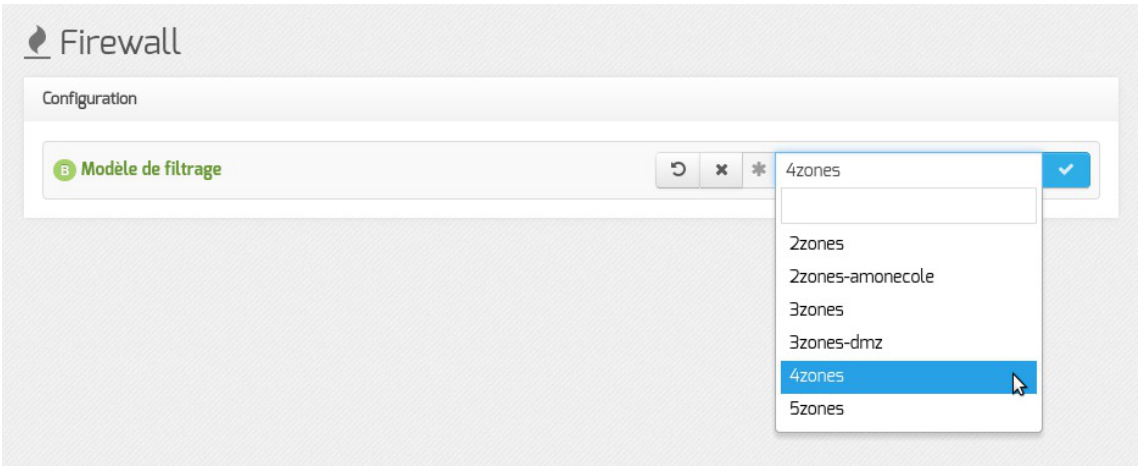
Voir aussi...

Onglet Interface-n [p.95]

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 l'interface 1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur l'interface 1) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

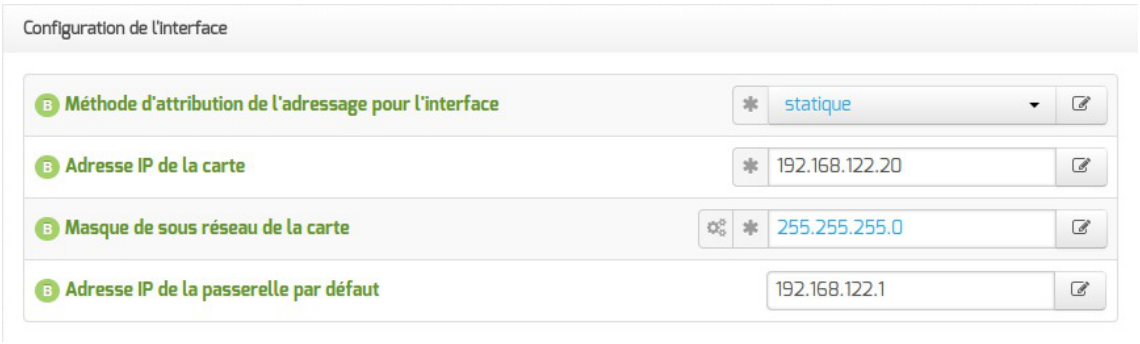
- **3zones** : gestion d'une zone admin sur l'interface 1 et d'une zone pedago sur l'interface 2 ;
- **3zones-dmz** : gestion d'une zone pedago sur l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.

Chaque modèle de zone proposé 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.

2.3. Onglet Interface-0

Configuration de l'interface



Avant toute chose, il faut décider comment la carte réseau est configurée.

Pour cela, il existe trois possibilités : statique[p.702], DHCP[p.708] ou `non géré`.

Méthode d'attribution statique

Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.

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

Méthode d'attribution DHCP

La configuration DHCP ne nécessite aucun paramétrage particulier.

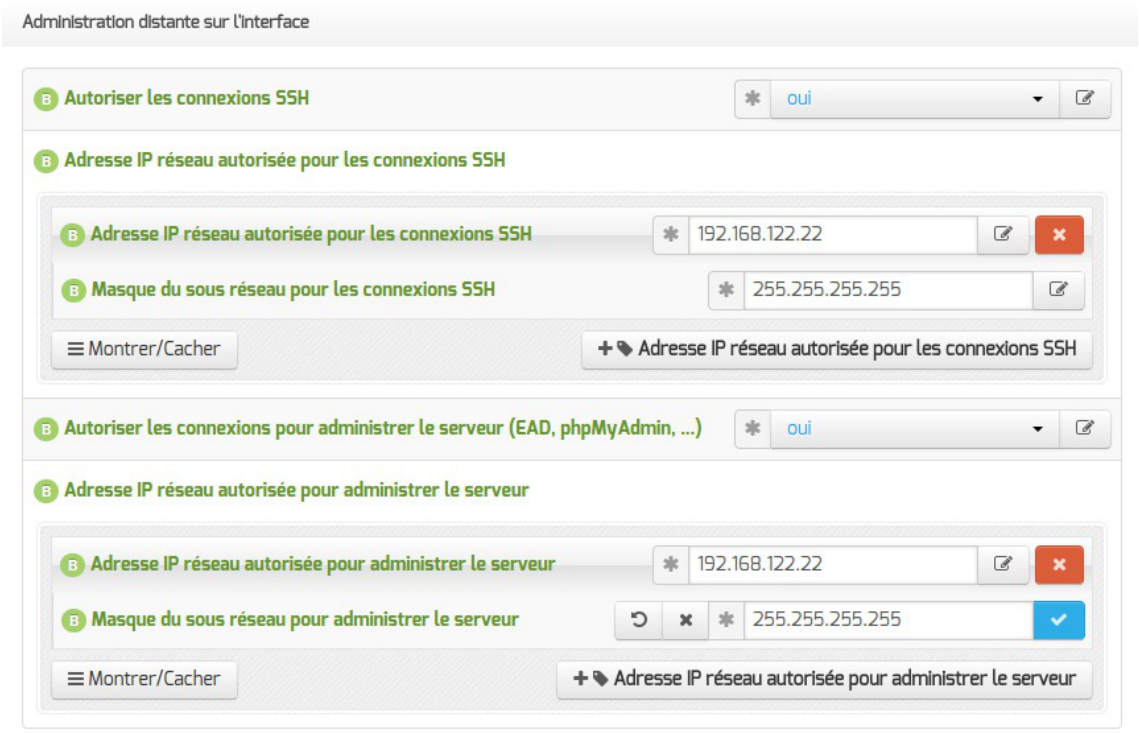
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Lors du passage d'une configuration statique à une configuration DHCP, il faut procéder à deux reconfigure successifs.

Méthode d'attribution "non géré"

L'utilisation de la nouvelle valeur `non gérée` permet de déléguer la configuration réseau à cloud-init[p.714] ou à un autre outil de contextualisation.

Administration à distance



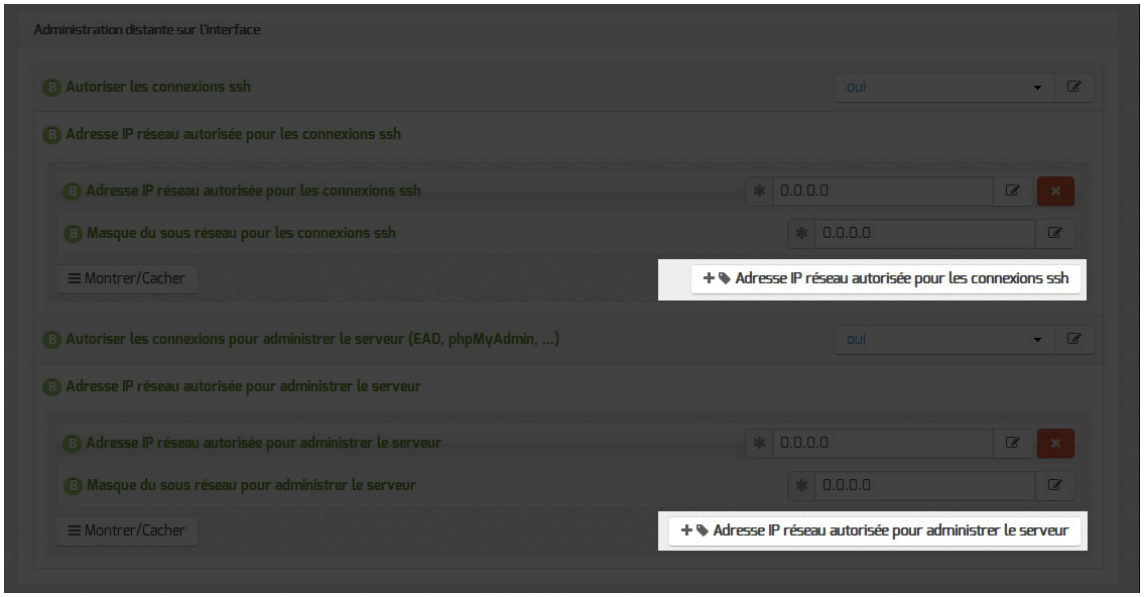
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

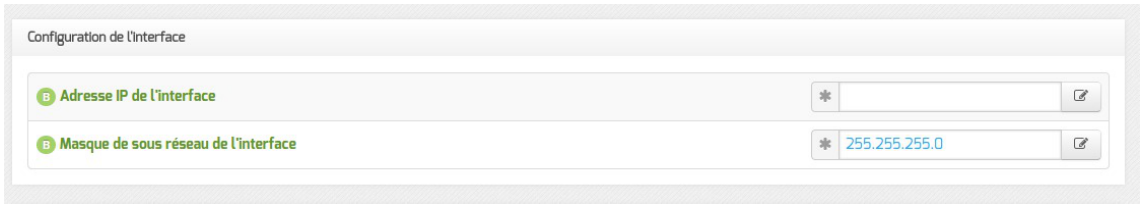
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

2.4. Onglet Interface-1

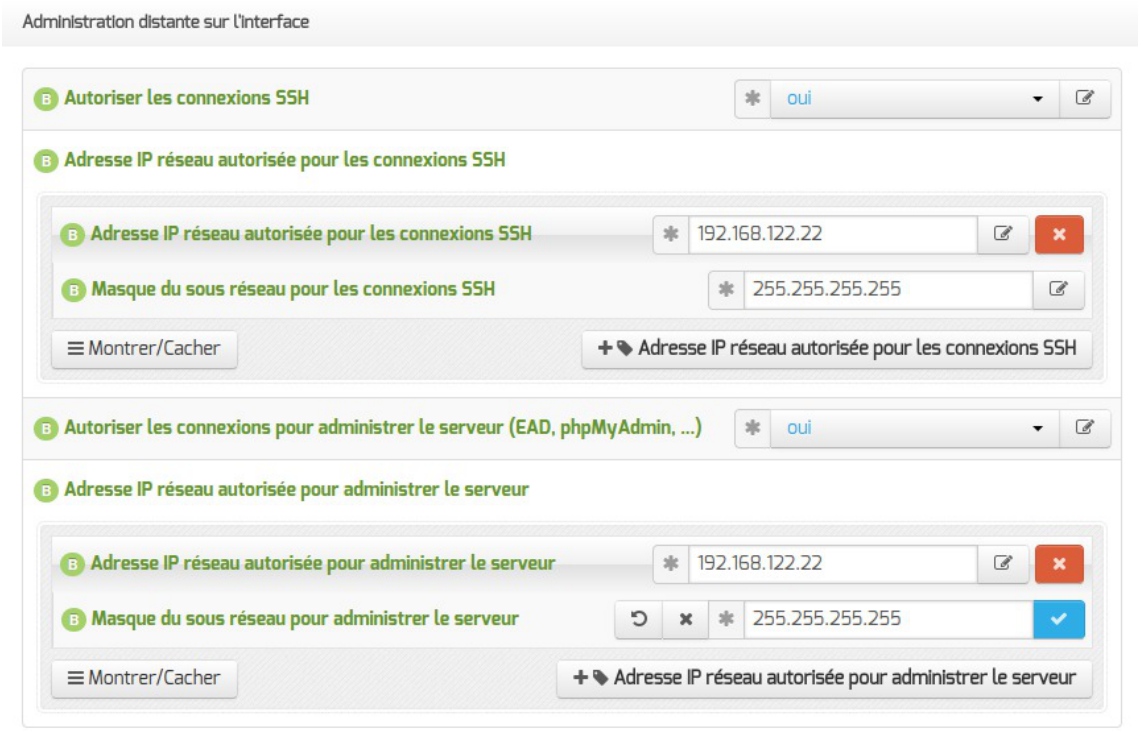
Configuration de l'interface



Dans les modes basique et normal, un adressage statique[p.702] 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

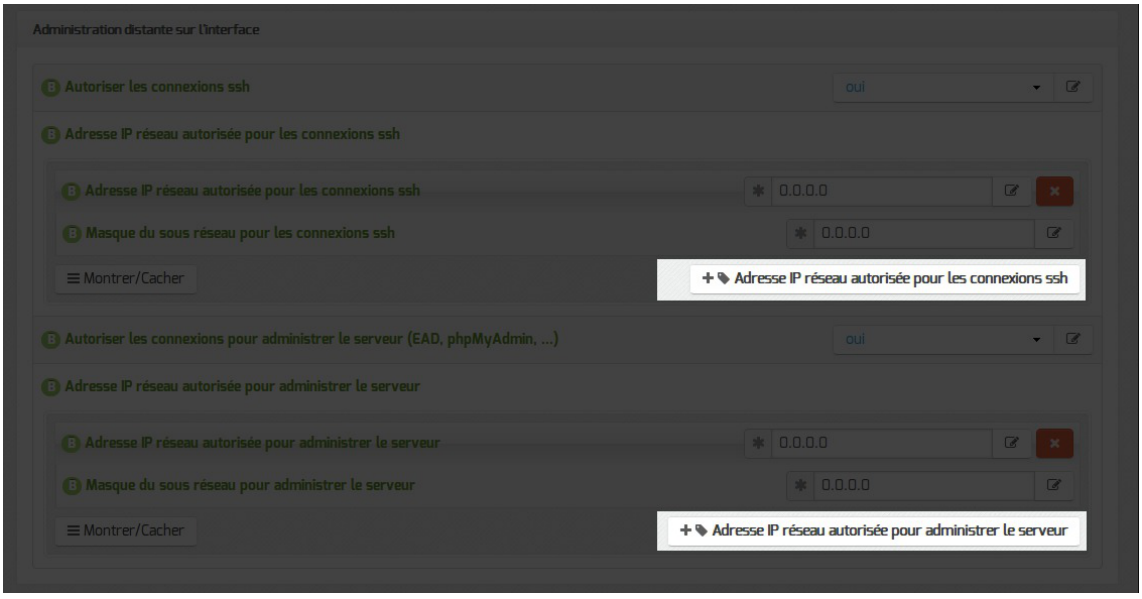


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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



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

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> `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 -ni $(CreoleGet nom_carte_eth0) port 22`

> Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

2.5. Onglet Interface-n

Nombre d'interfaces

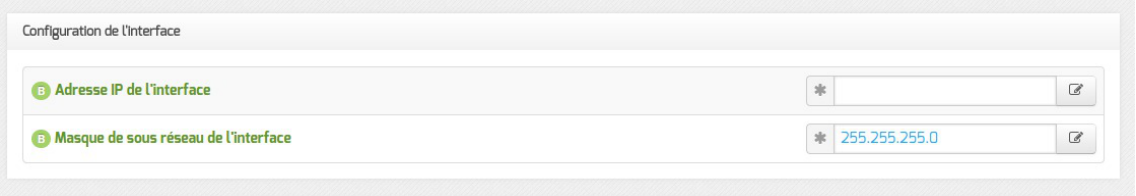
Un module Amon ou AmonEcole peut avoir de 2 à 5 cartes réseau.

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

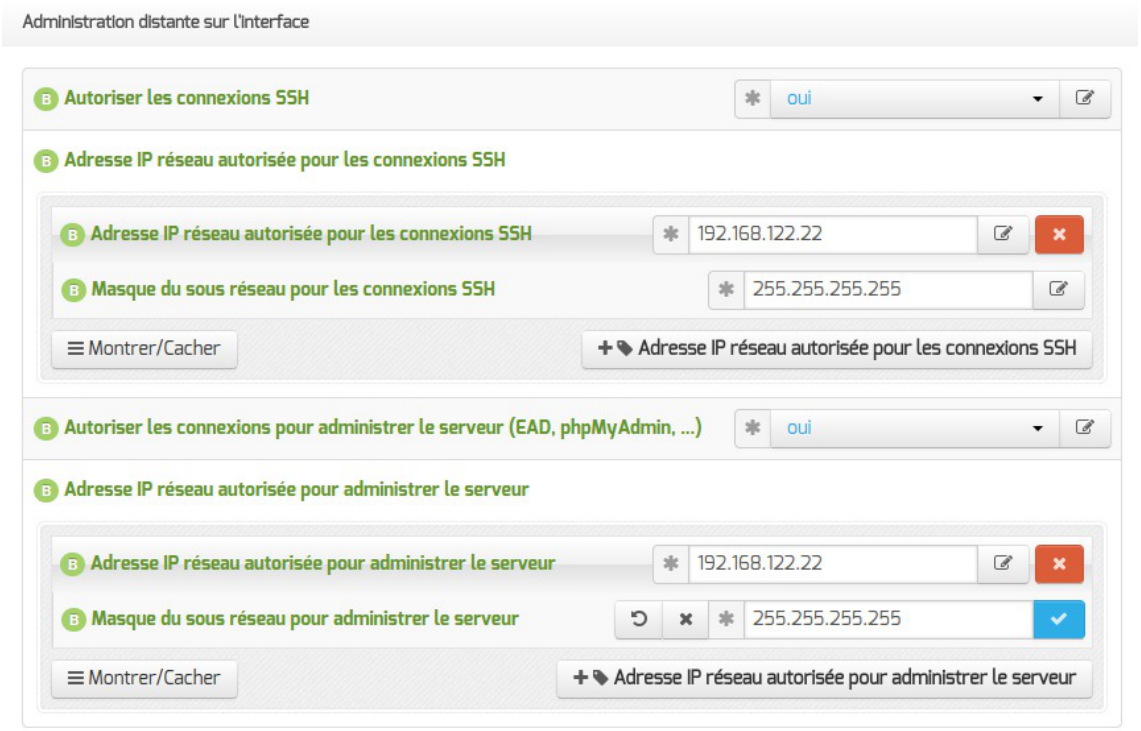


Dans les modes basique et normal, un adressage statique[p.702] est proposé pour l'interface réseau.

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

Administration à distance

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

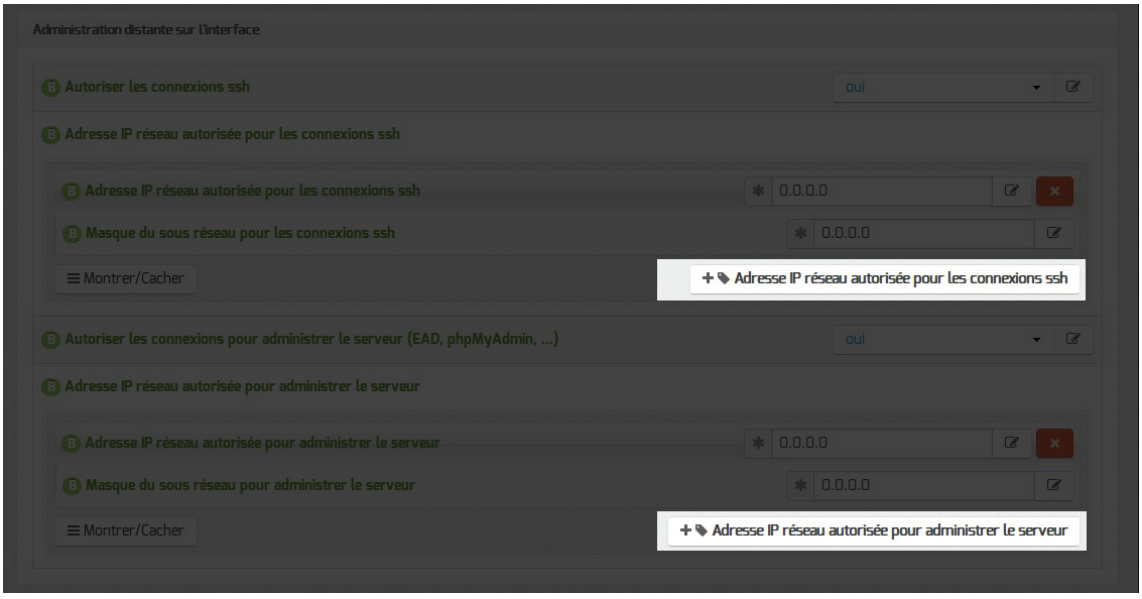


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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



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

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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 -ni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

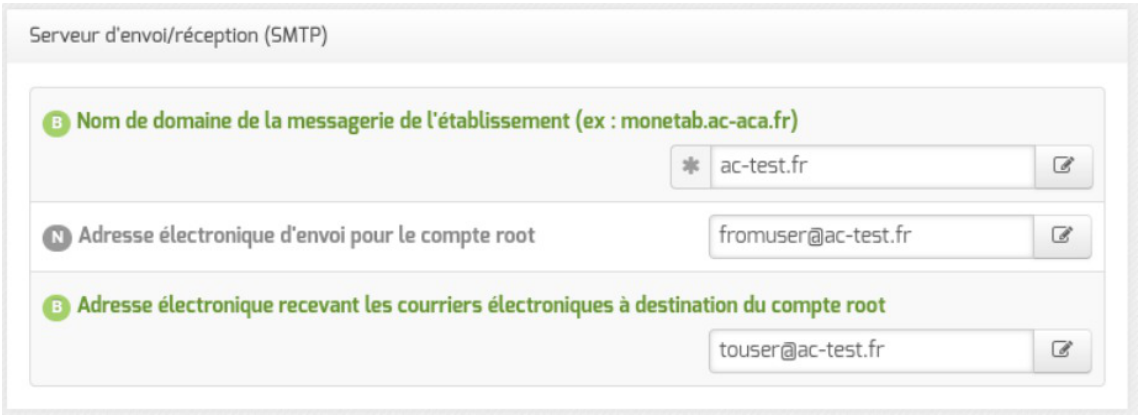
2.6. Onglet Messagerie

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 courriers électroniques.

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

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

Serveur d'envoi/réception (SMTP)



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 d'envoi pour le compte root` , saisir l'adresse que l'on souhaite utiliser pour l'envoi de courriers électroniques depuis le compte root.
- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

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

Dans le cas où le `Nom de domaine de la messagerie de l'établissement` n'est pas le même que la concaténation du `Nom de la machine` et du `Nom DNS du réseau local`, il peut être nécessaire d'activer la réécriture des en-têtes (cf. Onglet Messagerie) [p.276] pour avoir des informations cohérentes avec l'enveloppe des courriels.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

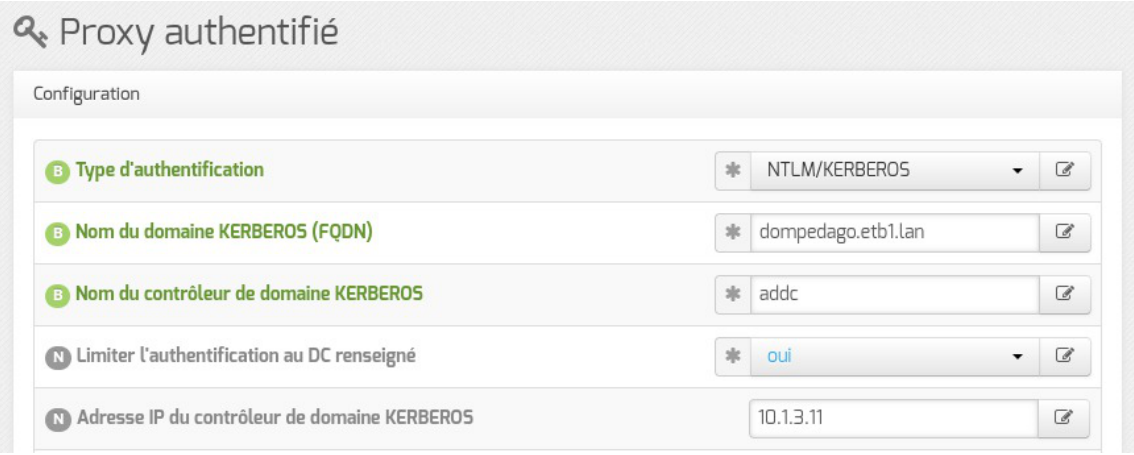


Cinq méthodes d'authentification sont alors disponibles dans l'onglet Proxy authentifié.

Authentification NTLM/KERBEROS

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory[p.702].

Cette configuration est à choisir si vous disposez d'un serveur Scribe ou Horus en mode AD ou d'un serveur Microsoft AD.



Si l'authentification NTLM/KERBEROS est activée sur le proxy, le Nom de machine, qui se paramètre dans l'onglet Général, ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.

À partir d'EOLE 2.8.1,

- il n'est plus obligatoire de fournir explicitement l'Adresse IP du contrôleur de domaine KERBEROS ;
- il est possible de désactiver la limitation de l'authentification au DC renseigné dans Nom du contrôleur de domaine KERBEROS.

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 ?
```

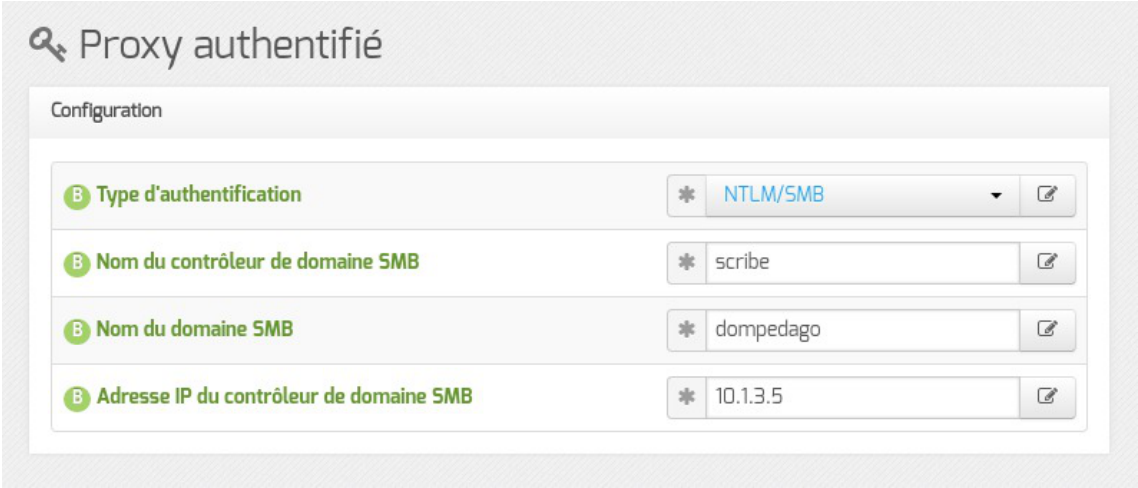

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Si la configuration de l'authentification 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/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba[p.730] NT.

Cette configuration est à choisir si vous disposez d'une version ancienne du serveur pédagogique Scribe ou du serveur administratif Horus.



Cette méthode d'authentification nécessite l'intégration du serveur au domaine Samba.

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 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`.

L'enregistrement au domaine étant proposé lors de l'instanciation du module, de ce fait l'authentification NTLM/SMB n'est plus proposée pour une deuxième authentification.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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

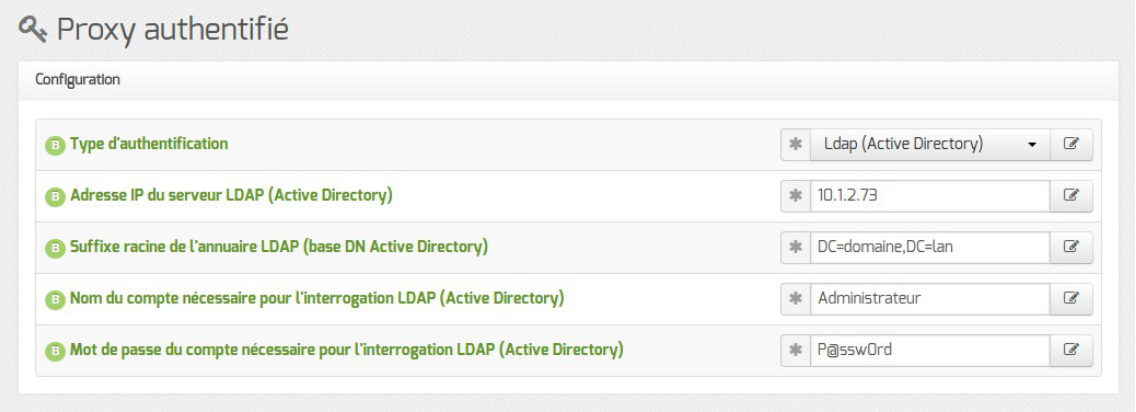
Authentification LDAP

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



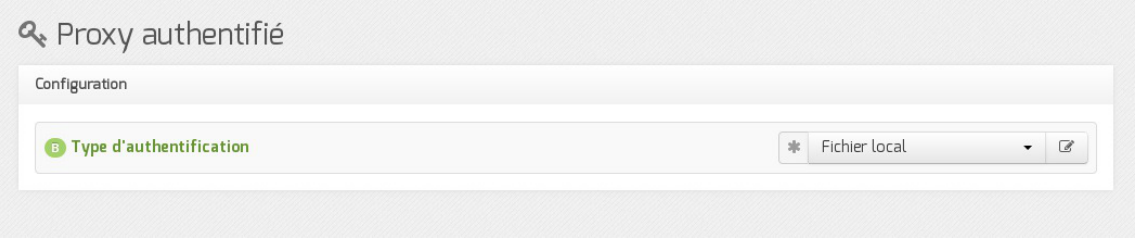
Ce type d'authentification est recommandé pour les postes hors domaine.

Authentification LDAP (Active Directory)



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

Authentification sur Fichier local



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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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



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

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

ou

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

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors interface 0 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 de l'interface 2, il faut aller dans l'onglet `Interface-2` et répondre `non` à la question `Activer l'authentification sur cette interface (s'applique aussi aux VLAN)`.

2.8. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (Mode Basique)

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les serveurs EOLE.

Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur certains des modules.

Installation de LemonLDAP::NG

Installation sur Scribe, AmonEcole ou Seth Éducation

Pour activer le serveur LemonLDAP::NG[p.717] sur les modules Scribe, AmonEcole ou Seth Éducation, il faut installer le paquet **eole-lemonldap-ng-auto**.

```
1 apt install eole-lemonldap-ng-auto
```

Le service sera alors pré-configuré pour utiliser l'annuaire du module.

Installation sur les autres modules

Pour activer le serveur LemonLDAP::NG sur les autres modules EOLE (Eolebase par exemple), il faut installer le paquet **eole-lemonldap-ng**.

```
1 apt install eole-lemonldap-ng
```

Les sources d'authentification seront à saisir dans l'interface de configuration du module.



Module Seth

L'installation du paquet eole-lemonldap-ng-auto sur un module Seth transformera ce dernier en Seth Éducation !

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

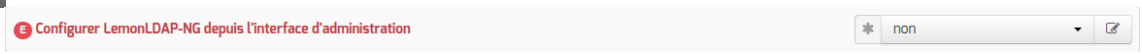
LemonLDAP vs EoleSSO

L'installation des paquets eole-lemonldap-ng et/ou eole-lemonldap-ng-auto entraîne la désinstallation du paquet **eole-sso-server** par le jeu des dépendances de paquets (dpkg[p. 704]).

Partie Configuration



1



Configurer LemonLDAP-NG depuis l'interface d'administration

Permet d'activer l'interface d'administration fournie par le projet LemonLDAP::NG.

Par défaut, cette interface est désactivée, les cas classiques de configuration étant pris en charge via les mécanismes EOLE.

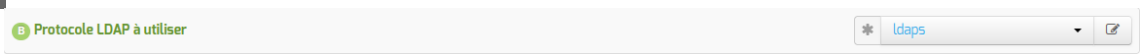
Conflit des modes de configuration

La configuration de LemonLDAP::NG depuis son interface d'administration écrase et remplace celle générée via les mécanismes EOLE.

Nom interne de la variable

ll_activer_manager

2



Protocole LDAP à utiliser

Il est possible d'adapter le protocole à utiliser selon les capacités du serveur LDAP associé.

Les choix proposés sont **ldaps** et **ldap**.

Nom interne de la variable

ldapScheme

La variable `Configurer LemonLDAP-NG depuis l'interface d'administration` permet d'activer l'interface d'administration de LemonLDAP::NG.

Si la variable est à oui une nouvelle variable apparaît en mode Normal et deux en mode Expert.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La variable `Protocole LDAP à utiliser` permet de choisir entre `LDAP` et `LDAPS`.

Le serveur LemonLDAP::NG prend en charge LDAP over SSL (LDAPS). La fonction Strict SSL est définie par défaut. La fonction Strict SSL nécessite une certification de serveur.

Documentation annexe

Site officiel : LemonLDAP::NG [https://lemonldap-ng.org/]

Documentation officielle (en anglais) : Documentation [https://lemonldap-ng.org/documentation/latest/]

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.

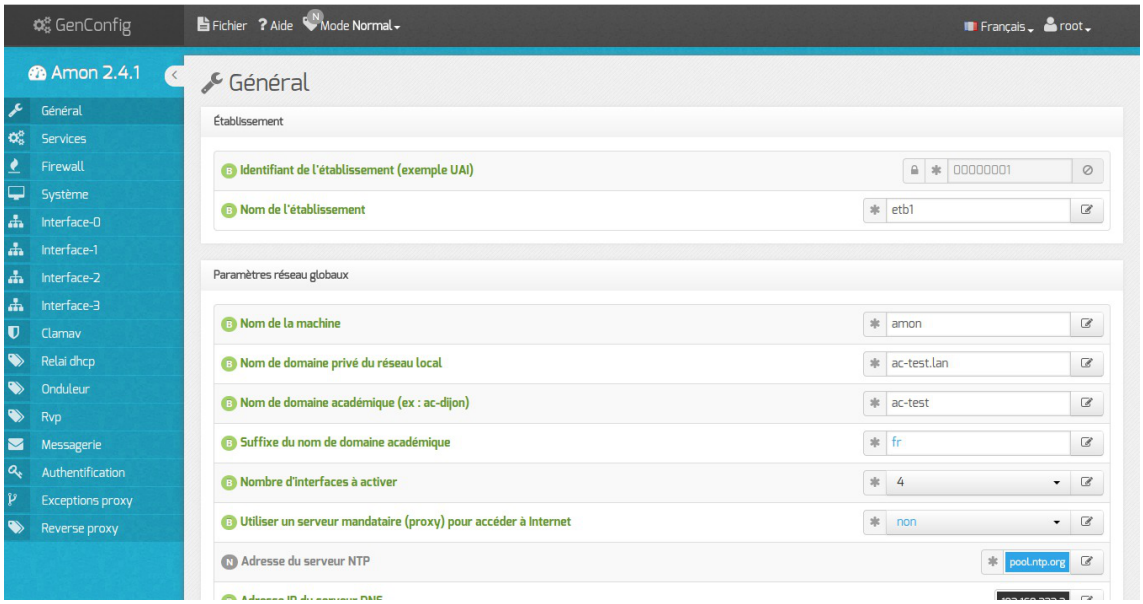
Dans l'interface de configuration du module voici les onglets propres à la configuration du module Amon :

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Agrégation` * ;
- `Clamav` * ;
- `Relai dhcp` * ;
- `Onduleur` * ;
- `Rvp` * ;
- `Eole sso` * ;
- `Mode restreint` ;
- `Messagerie` ;
- `Authentification` ;
- `Squid` ;
- `Squid2` ;
- `Proxy authentifié` * ;
- `Proxy authentifié 2` * ;
- `Exceptions proxy` ;
- `Wpad` ;
- `Nginx` ;
- `Reverse proxy` * ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Freeradius` *.
- `Lemonldap`

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.

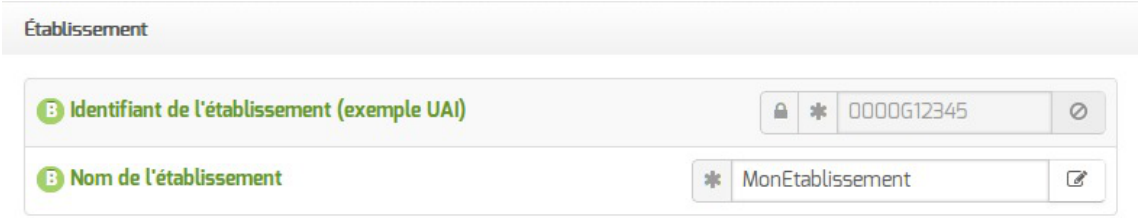
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- le `Nom de l'établissement`.

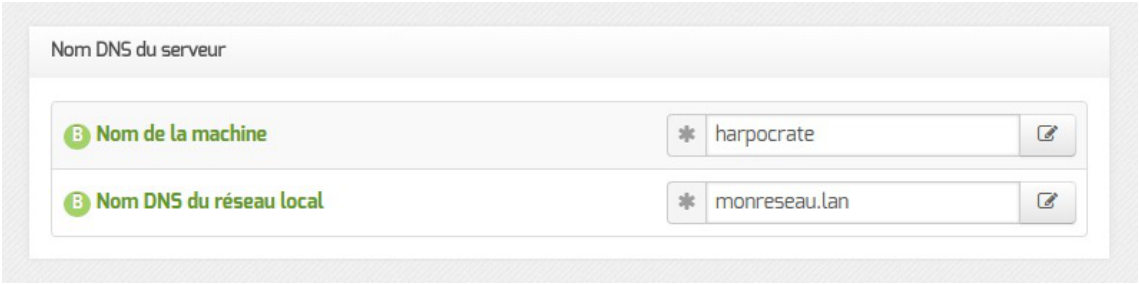
Ces informations sont notamment utiles pour Zéphir, les applications web locales, ...

Sur les modules fournissant un annuaire LDAP[p.717] 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.

Nom DNS du serveur



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Si l'authentification `NTLM/KERBEROS` est activée sur le proxy, le `Nom de machine` ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.

Le `Nom DNS du serveur` utilise fréquemment des domaines de premier niveau du type `.lan` .

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.

Rappel : les outils mDNS (Avahi, Bonjour, ...) utilise la racine '.local'. Pour éviter les problèmes de DNS, nous vous déconseillons d'utiliser cette racine.

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.

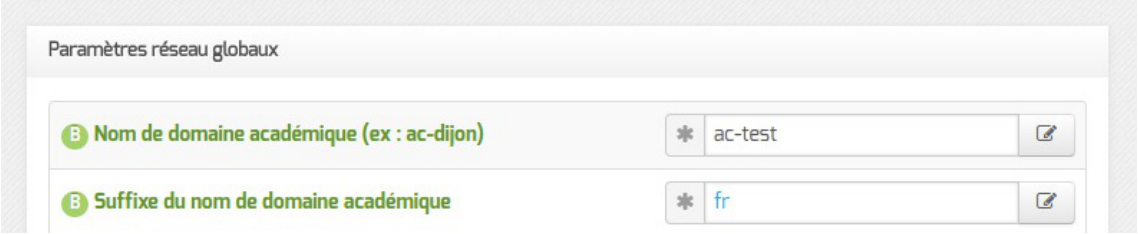
Les informations sur les noms de domaine sont importantes car elles sont notamment

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Paramètres réseau globaux



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

Cette information est découpée en plusieurs champs :

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

Nombre d'interfaces

Un module Amon ou AmonEcole 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.

La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> protégé par un module Amon.

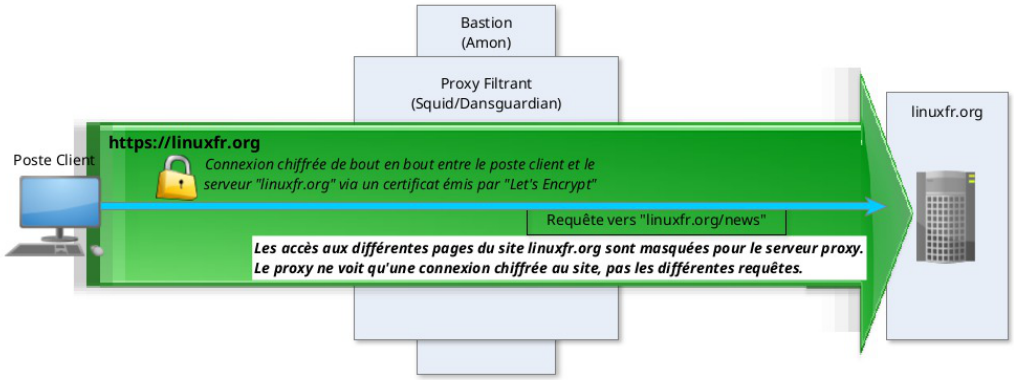
Déchiffrement et interception du protocole HTTPS

Par rapport au protocole HTTP[p.714], le protocole HTTPS permet de chiffrer la communication entre le navigateur du poste client et le serveur du site distant.

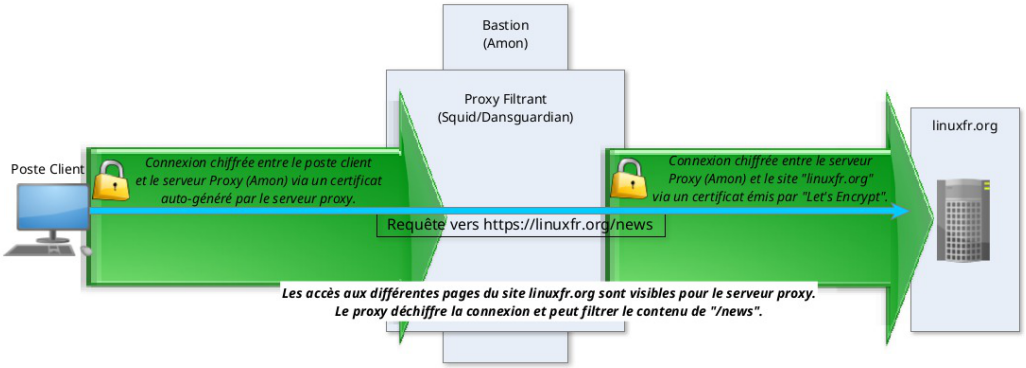
Dans ce cas, le serveur proxy ne journalise qu'une seule connexion vers le site distant (exemple : https://pcll.ac-dijon.fr) mais pas les différentes requêtes d'accès aux pages ou aux fichiers se trouvant sur ce serveur (exemple : https://pcll.ac-dijon.fr/eole/).

En HTTPS, le serveur Proxy ne peut pas filtrer le contenu des pages consultées ni scanner les fichiers téléchargés avec un antivirus.

Le déchiffrement HTTPS sur le serveur Proxy permet d'intercepter l'ensemble des requêtes et de les journaliser, de filtrer le contenu des pages visitées et de scanner les fichiers téléchargés.



Fonctionnement HTTPS normal



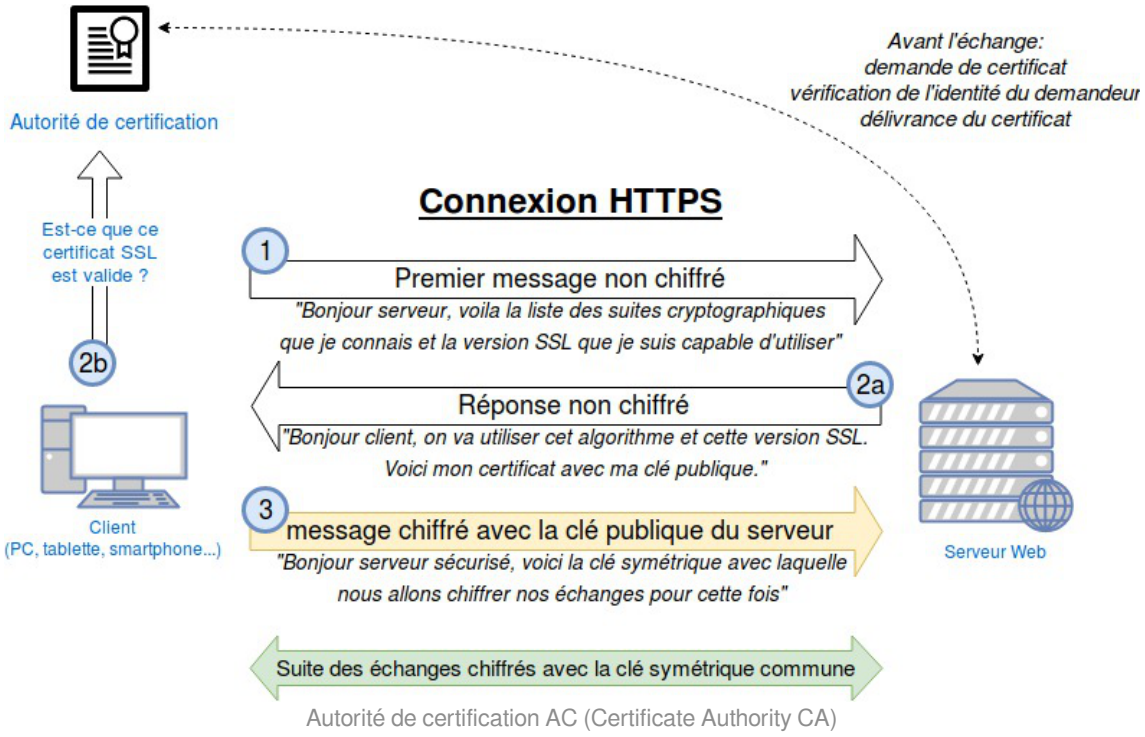
Fonctionnement HTTPS déchiffré par le Proxy

Certificat Racine de l'autorité de certification

Un certificat HTTPS est émis par une autorité de certification[p.704].

Let's Encrypt[p.717], par exemple, est une autorité de certification publique et connue des navigateurs ; son certificat racine est pré-installé dans les navigateurs et les systèmes d'exploitation.

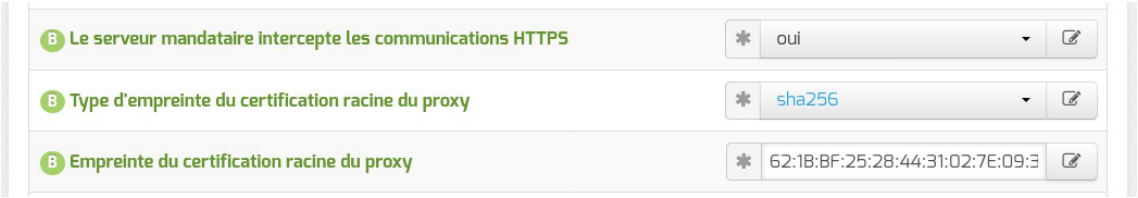
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Autorité de certification AC (Certificate Authority CA)

À partir de la version 2.8.1, le module Amon est équipé d'une fonctionnalité d'interception du trafic HTTPS. Il est possible de déclarer son certificat racine servant à sur-signer les ressources servies par le protocole HTTPS et transitant par le proxy filtrant. Cette déclaration permet d'en automatiser l'intégration dans le magasin de certificats local.

Si la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` est passée à `oui`, la variable `Le serveur mandataire intercepte les communications HTTPS` est proposée et permet elle-même de faire apparaître deux variables permettant d'identifier le certificat racine employé par le proxy filtrant.



En passant la variable `Le serveur mandataire intercepte les communications HTTPS` à `oui`, il est possible de renseigner les variables suivantes en utilisant les données affichées par la commande `diagnose` sur le module Amon :

- `Type d'empreinte du certificat racine du proxy` : SHA256 (par défaut sur Amon 2.8.1)
- `Empreinte du certificat racine du proxy` : information donnée par le diagnose du serveur Amon dans le cas où celui-ci fait office de proxy filtrant

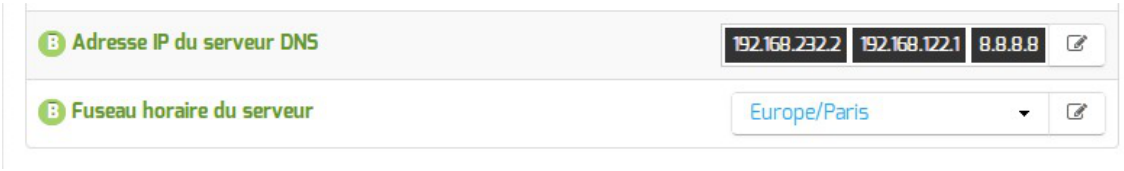
Cette configuration est nécessaire uniquement lorsque le module Amon est configuré pour l'interception des communications HTTPS.

Sur un module Amon configuré pour l'interception des communications HTTPS, la commande `diagnose` permet de connaître le chemin et l'empreinte du certificat :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
*** Validité du certificat racine du proxy (/etc/eole/squid_CA.crt)
.               signingCA.crt => Ok
.                   Empreinte => SHA256 Fingerprint=62
:1B:BF:25:28:44:31:02:7E:09:31:A6:EA:FD:A5:A8:7C:D4:EB:B6:3D:83:88:62:0F:98:85:

```

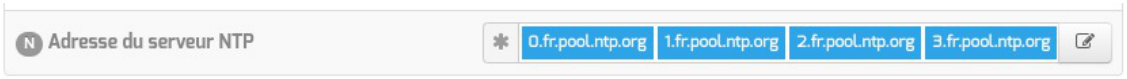
DNS et fuseau horaire



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.709].

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

NTP



Une liste de serveurs de temps (NTP[p.723]) à utiliser est proposée par défaut.

Il est possible de modifier ces valeurs afin d'utiliser un serveur de temps personnalisé.

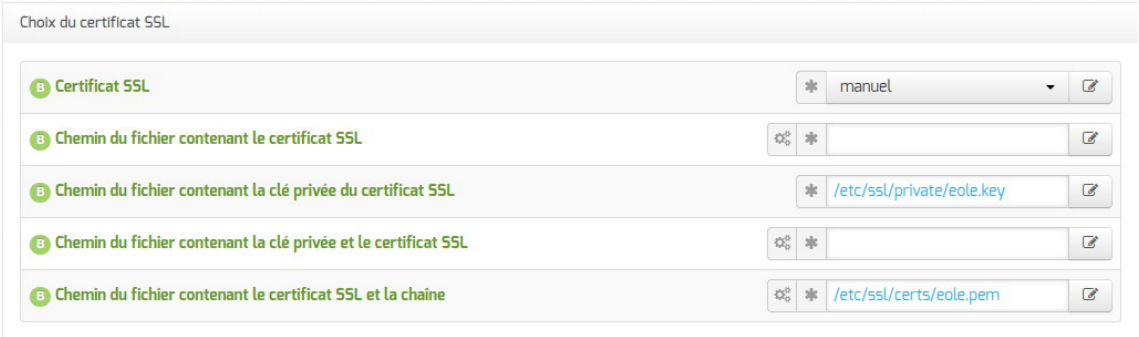
Ports utilisés par ntpdate

Le service `ntp` utilisant et bloquant le port 123, `ntpdate` utilise un port source aléatoire dans la plage des ports non privilégiés.

Les éventuelles règles de pare-feu ne peuvent donc pas présumer que le port source est le port 123.

Par contre, le port de destination reste inchangé (port : 123).

Choix du certificat SSL



Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.733] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.704] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.717] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour ce faire, il faut

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

Le système de certificat utilisé repose sur une clé privée et une clé publique (le certificat) contre-signée par une autorité de certification.

Selon le contexte d'utilisation, les différents éléments de la chaîne de certification (clé privée, certificats du service ou de l'autorité de certification) doivent être combinés selon différents modes.

En mode `letsencrypt` et `autosigné`, le détail de ces combinaisons est automatique et caché.

En mode `manuel`, les variables suivantes permettent d'identifier l'emplacement des fichiers contenant les différentes combinaisons de fichiers utiles :

- `Chemin du fichier contenant le certificat SSL` : emplacement du fichier contenant uniquement le certificat ;
- `Chemin du fichier contenant la clé privée du certificat SSL` : emplacement du fichier contenant uniquement la clé privée ;
- `Chemin du fichier contentant la clé privée et le certificat SSL` : emplacement du fichier contenant la concaténation du certificat SSL puis de la clé privée ;
- `Chemin du fichier contenant le certificat SSL et la chaîne` : emplacement du fichier contenant la concaténation du certificat SSL et des certificats intermédiaires formant la chaîne de certification à l'exclusion du certificat racine.

Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.

Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

Pour plus d'informations, consulter la partie consacrée à l'`onglet expert` `Certificats ssl` (cf. Onglet Certificats ssl : gestion des certificats SSL) [p.233].

Mise à jour



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

Voir aussi...

- Onglet Interface-n [p.95]
- Les différents types de mises à jour [p.449]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

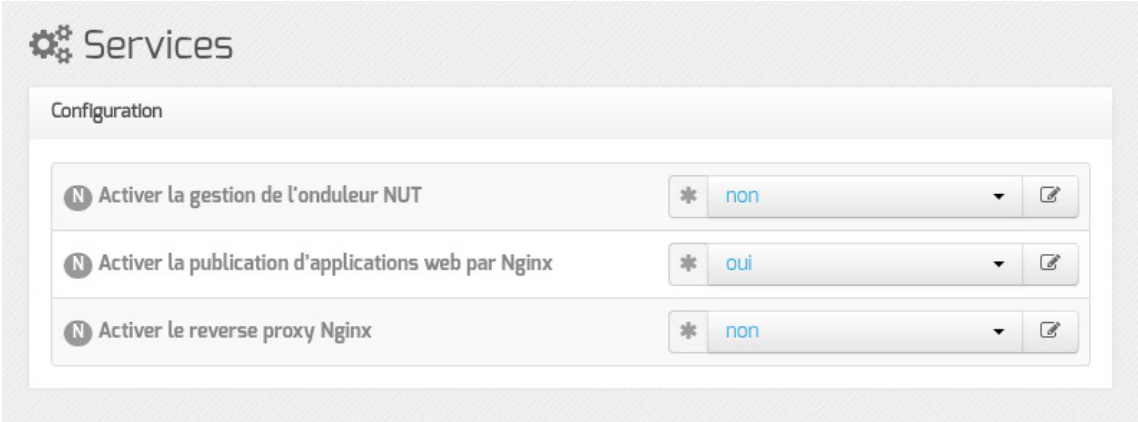
3.2. Onglet Services

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.723].

L'activation d'applications web par Nginx[p.722] et du proxy inverse sont également disponibles sur ce module.

Les autres services propres au module Amon en mode normal sont les suivants :

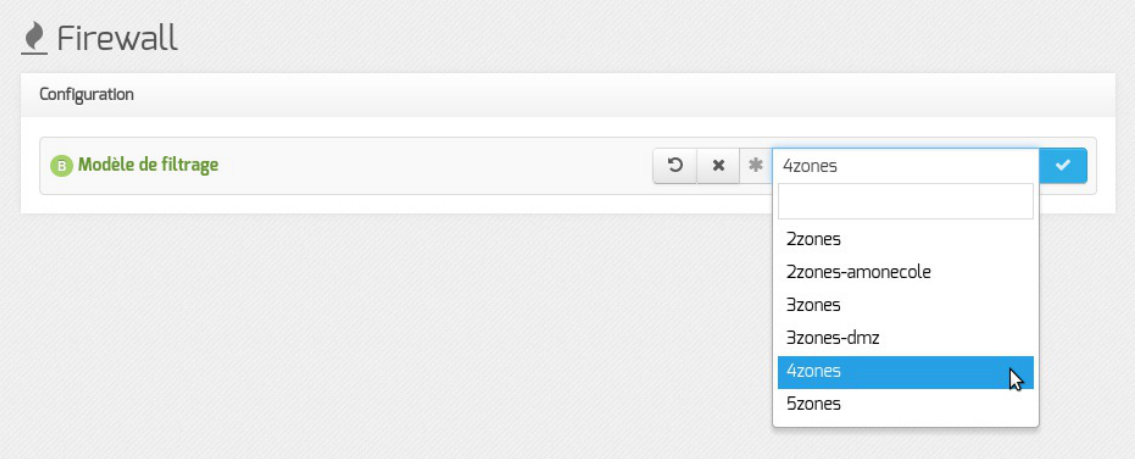
- l'anti-virus ClamAv ;
- le relai DHCP ;
- le réseau virtuel privé RVP ;
- le serveur EoleSSO ;
- le support WPAD.

3.3. Onglet Firewall

Modèle de filtrage

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 :

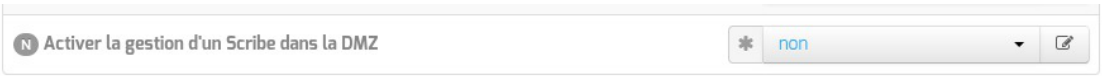
- **2zones** : gestion d'une zone admin ou pedago sur l'interface 1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur l'interface 1) ;
- **3zones** : gestion d'une zone admin sur l'interface 1 et d'une zone pedago sur l'interface 2 ;
- **3zones-dmz** : gestion d'une zone pedago sur l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.

Chaque modèle de zone proposé 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.

Déclaration d'un module Scribe en DMZ

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.704] des règles propres à la DMZ[p.709].



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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).

Interdire des accès réseaux



Par défaut, l'accès à des réseaux extérieurs pour des réseaux autres que l'interface 1 (l'interface 1 étant généralement *admin*) n'est pas interdit.



Si on passe l'option `Interdire les interfaces autres que 1 à accéder à des réseaux extérieurs` à `oui`, il est possible d'interdire l'accès

pour la ou les adresse(s) réseau et le ou les masque(s) souhaités.

Pour les réseaux RVP, il est habituel de ne pas conserver les données téléchargées par les utilisateurs dans le cache du proxy. C'est pour cela que l'option `Désactiver le cache du proxy pour les accès à ce réseau` est à `oui` par défaut. Cela signifie qu'en cas de téléchargement de page web, d'image, ... ces informations seront automatiquement re-téléchargées depuis le site source plutôt que conservées dans le cache du proxy.

Enfin, l'option `En plus de l'interdiction proxy, interdire tous les protocoles` permet de bloquer, via des règles iptables tout accès à ces réseaux.

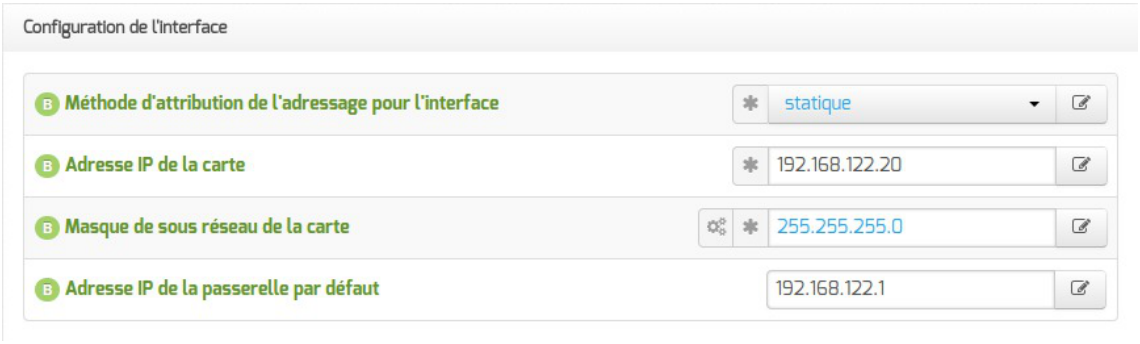
Voir aussi...

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Configuration du module Amon avec le module Scribe en DMZ [p.337]

3.4. Onglet Interface-0

Configuration de l'interface



Avant toute chose, il faut décider comment la carte réseau est configurée.

Pour cela, il existe trois possibilités : statique[p.702], DHCP[p.708] ou `non géré`.

Méthode d'attribution statique

Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.



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

Méthode d'attribution DHCP

La configuration DHCP ne nécessite aucun paramétrage particulier.



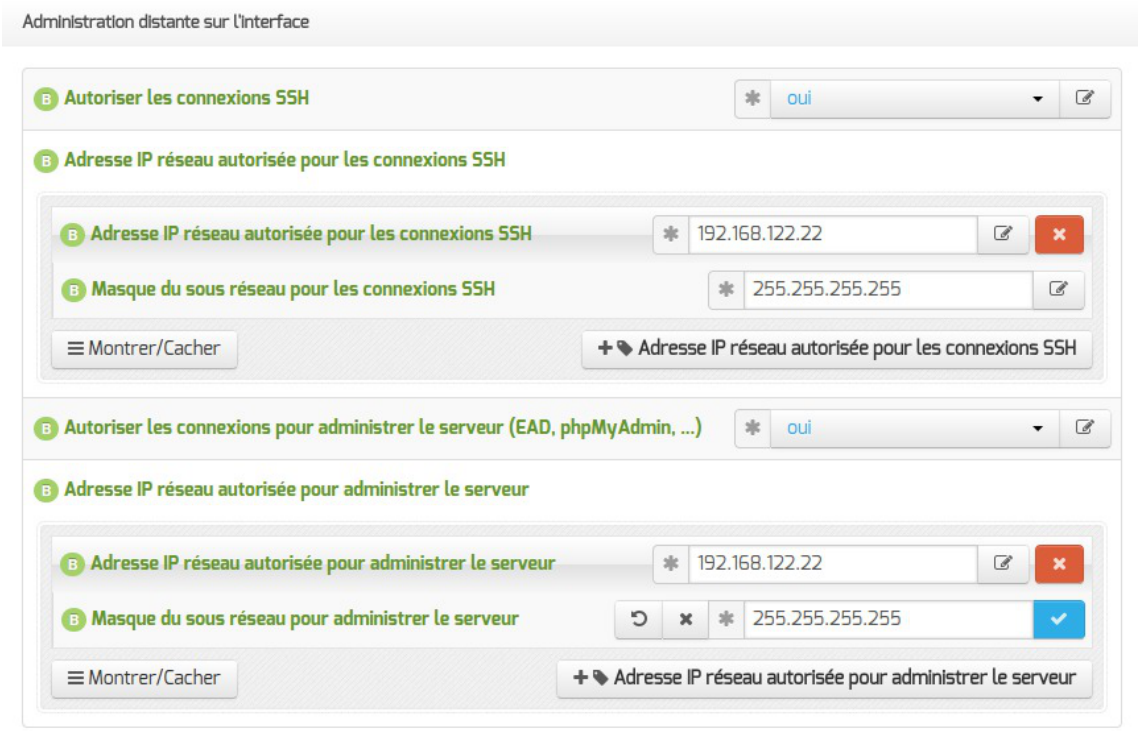
Lors du passage d'une configuration statique à une configuration DHCP, il faut procéder à deux reconfigure successifs.

Méthode d'attribution "non géré"

L'utilisation de la nouvelle valeur `non gérée` permet de déléguer la configuration réseau à cloud-init[p.714] ou à un autre outil de contextualisation.

Administration à distance

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

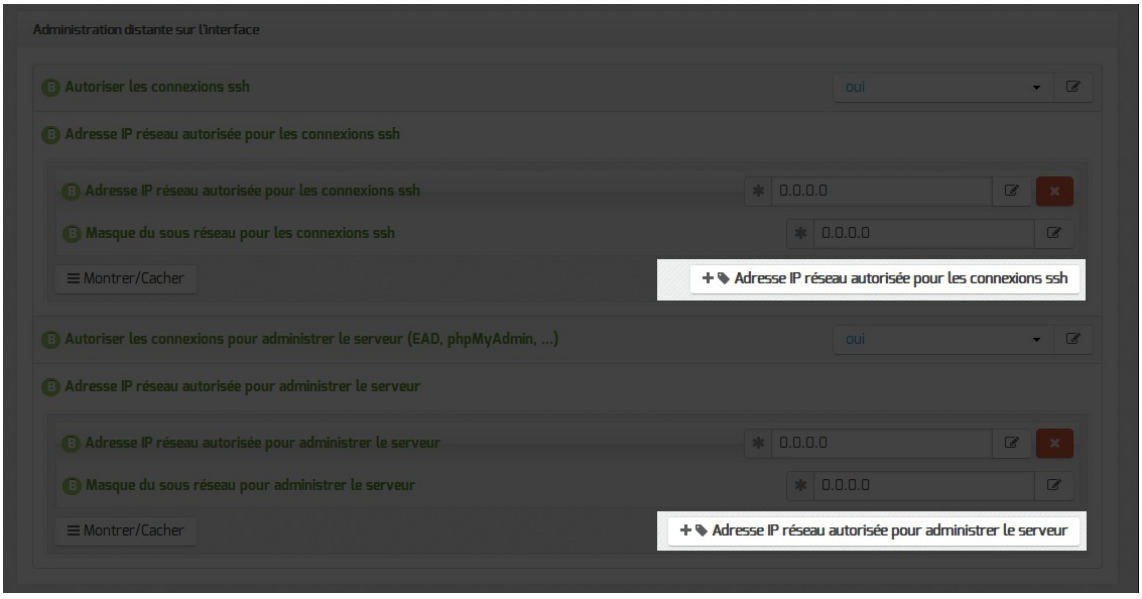


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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



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

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

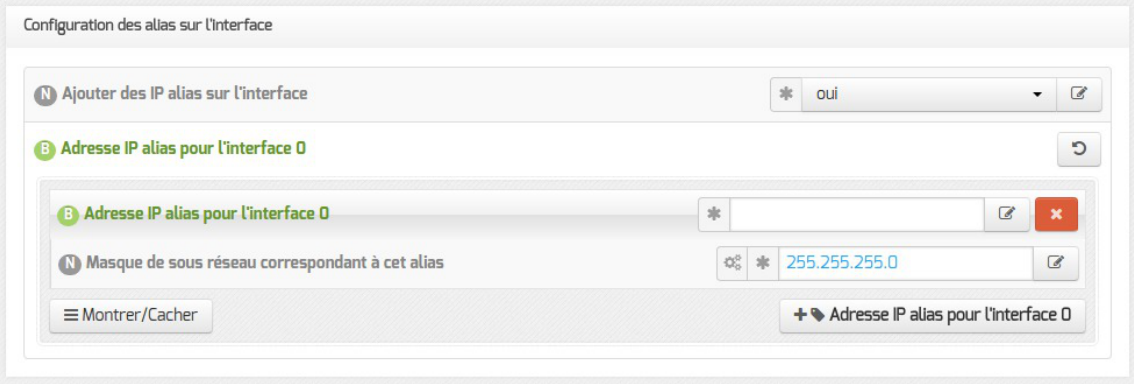
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

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.



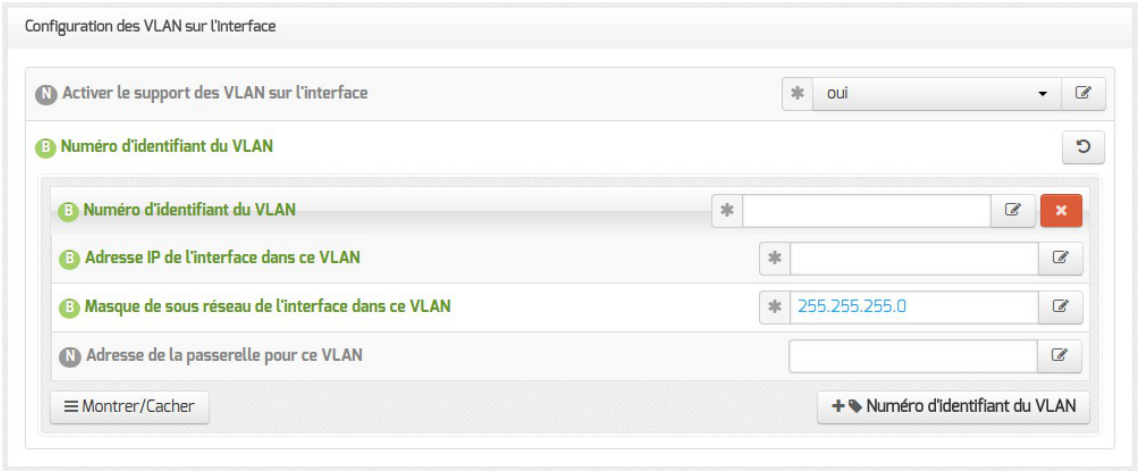
Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.734] (réseau local virtuel) sur une interface déterminée du module.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous-réseau de l'interface dans ce VLAN.

Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Agrégation de routes IP

L'activation d'un alias IP, fait apparaître un nouveau paramètre : `Répartition de charge entre 2 lignes Internet`.



Pour activer l'agrégation de routes IP[p.702] (niveau 3), il faut passer ce nouveau paramètre à `oui`.

Un nouvel onglet : `Agrégation` est alors disponible.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Voir aussi...

Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.128]

3.5. Onglet Interface-1

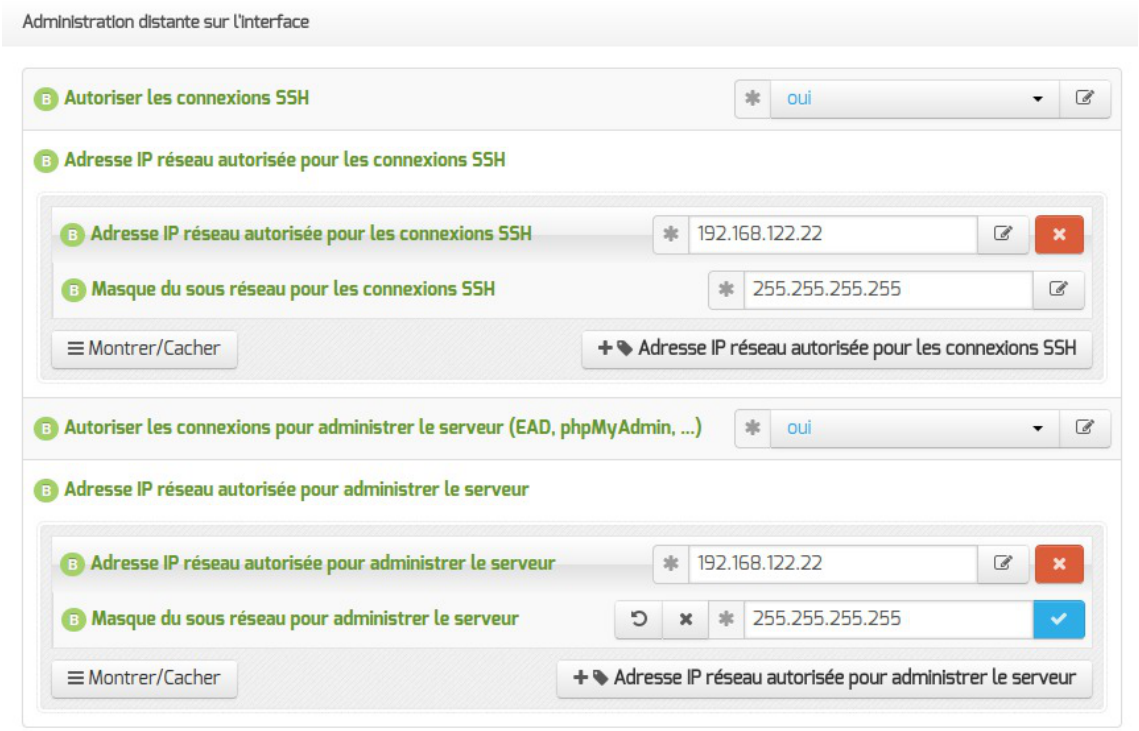
Configuration de l'interface



Dans les modes basique et normal, un adressage statique[p.702] est proposé pour l'interface réseau. Il faut renseigner l'adresse IP et le masque de sous-réseau associés à l'interface.

Administration à distance

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

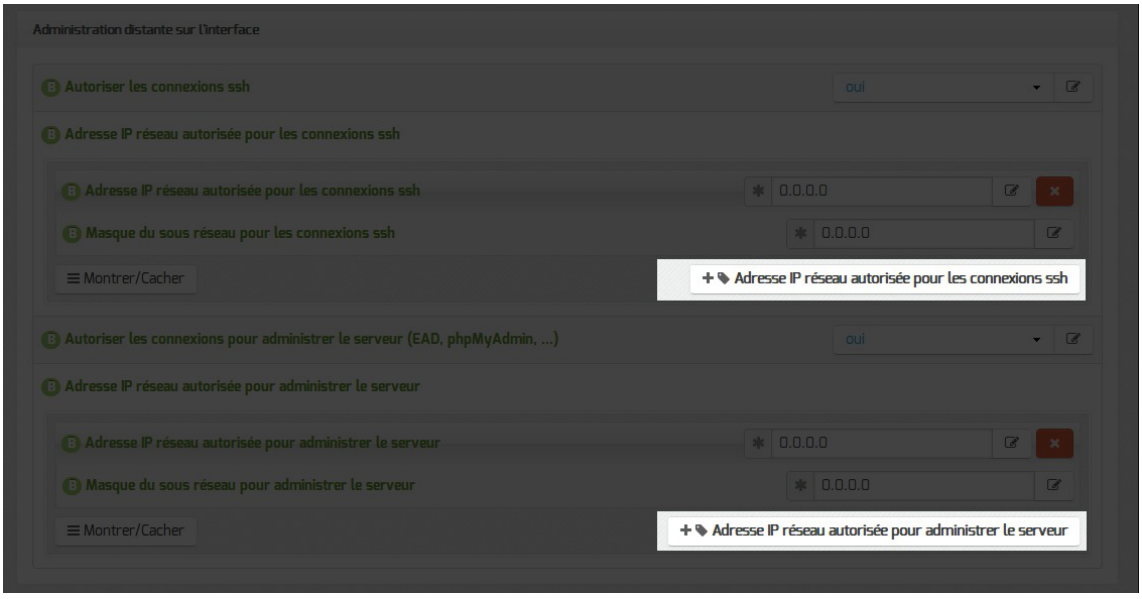


Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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



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

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

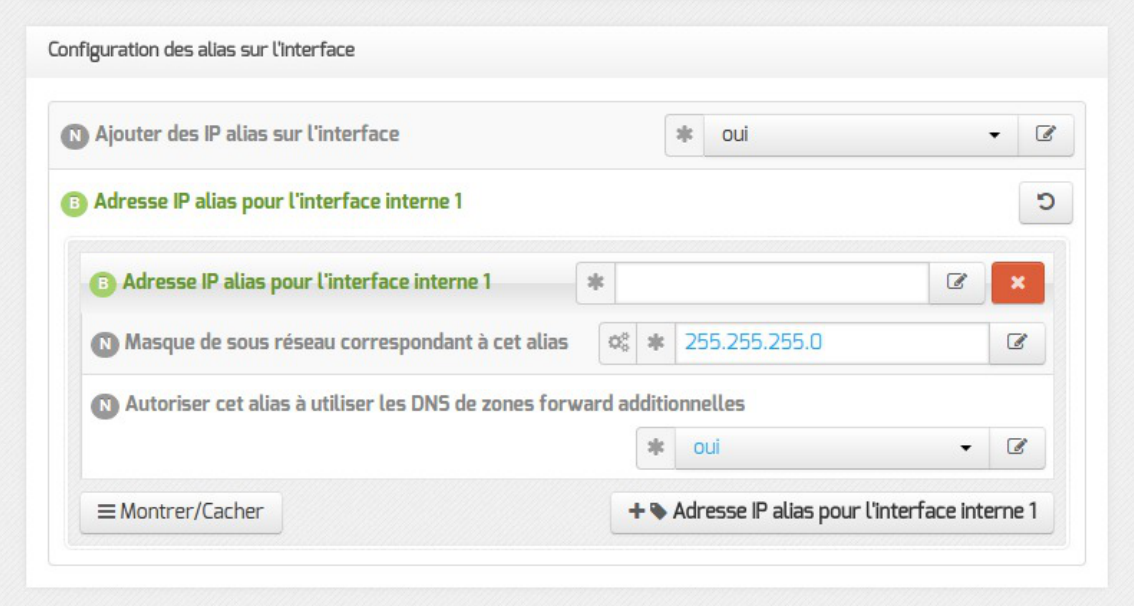
`Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

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

La variable `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`.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

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

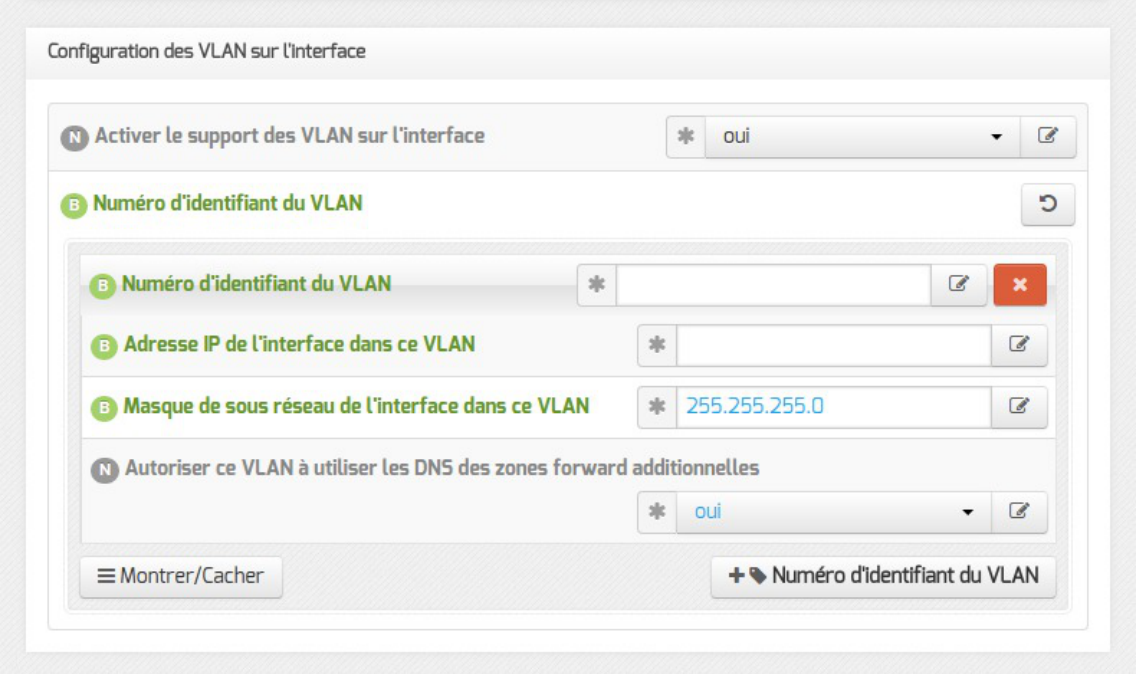
- `Autoriser cet alias à utiliser les DNS de Forward RVP/AGRIATES` : Si le service RVP est activé (onglet `Services`) et que le serveur est membre du réseau

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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[p.734] (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

La variable `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`.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

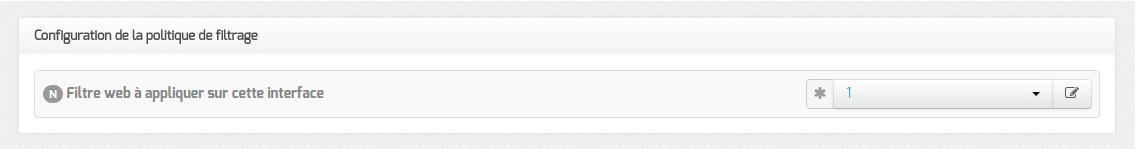


- `Nom de la zone (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface. Le nom (par défaut admin pour l'interface 1) doit être différent pour chacune des interfaces.

Configuration des zones de filtrage

La solution de filtrage permet de différencier 2 zones, ce qui permet de dissocier 2 politiques de filtrage majeures et distinctes comme par exemple une zone réseau administratif et une zone réseau pédagogique.

Il faut choisir à quelle zone appartient une interface. Cela s'effectue dans la configuration de chaque interface réseau en sélectionnant le numéro de la zone souhaité dans le champ `Filtre Web à appliquer à cette interface`.



> Les zones `Filtre web 1` et `Filtre web 2` correspondent chacun à une instance du logiciel de filtrage. La configuration de chacune des instances s'effectue dans l'onglet `Filtrage web`.

Voir aussi...

> Onglet Filtrage web : Configuration du filtrage web [p.285]

3.6. Onglet Interface-n

Nombre d'interfaces

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

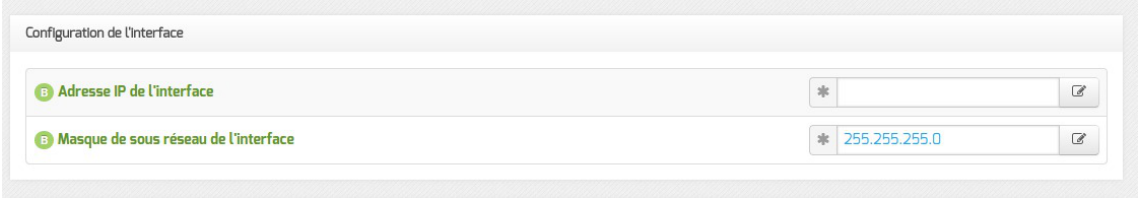
Le nombre d'interfaces activées se définit dans l'onglet `Général` de l'interface de configuration du module.



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

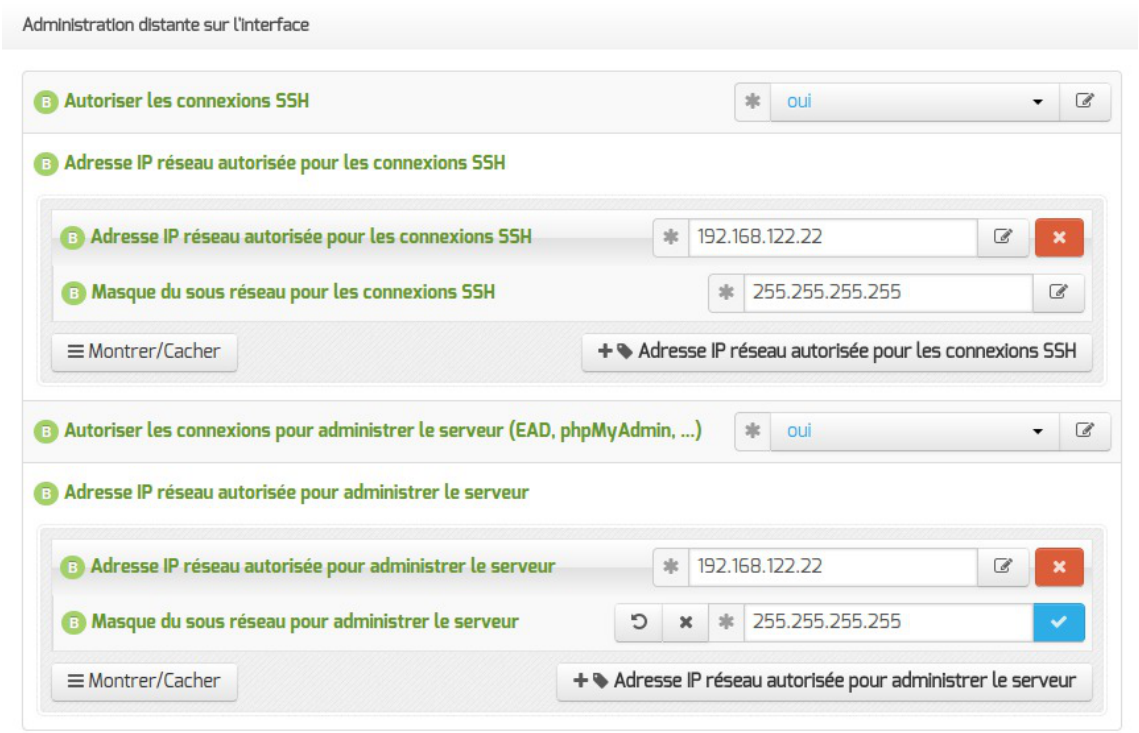
Configuration de l'interface



Dans les modes basique et normal, un adressage statique[p.702] 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



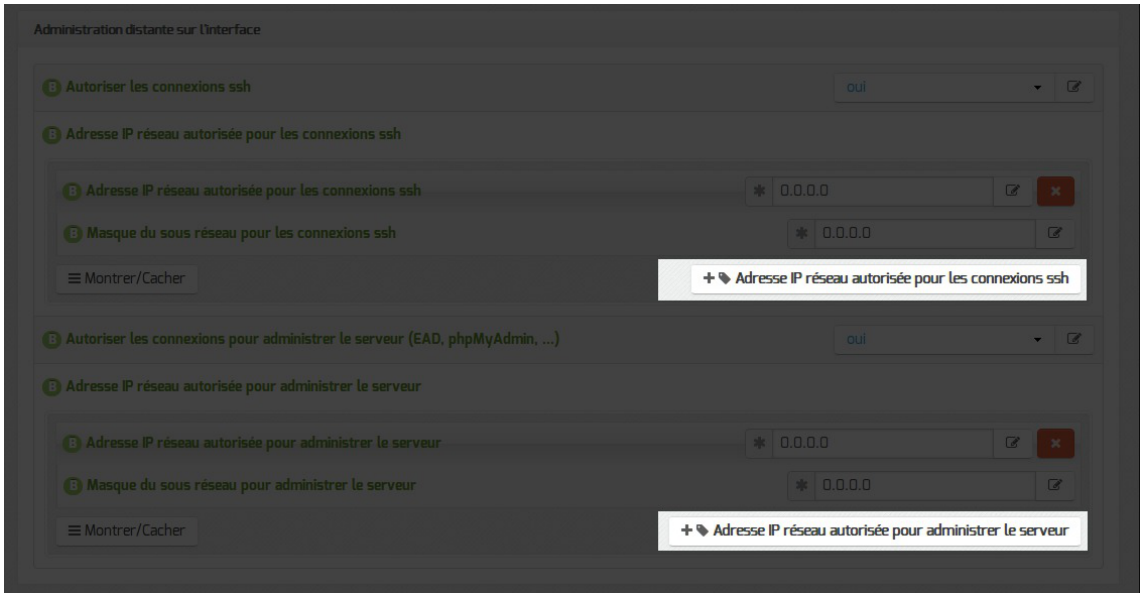
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

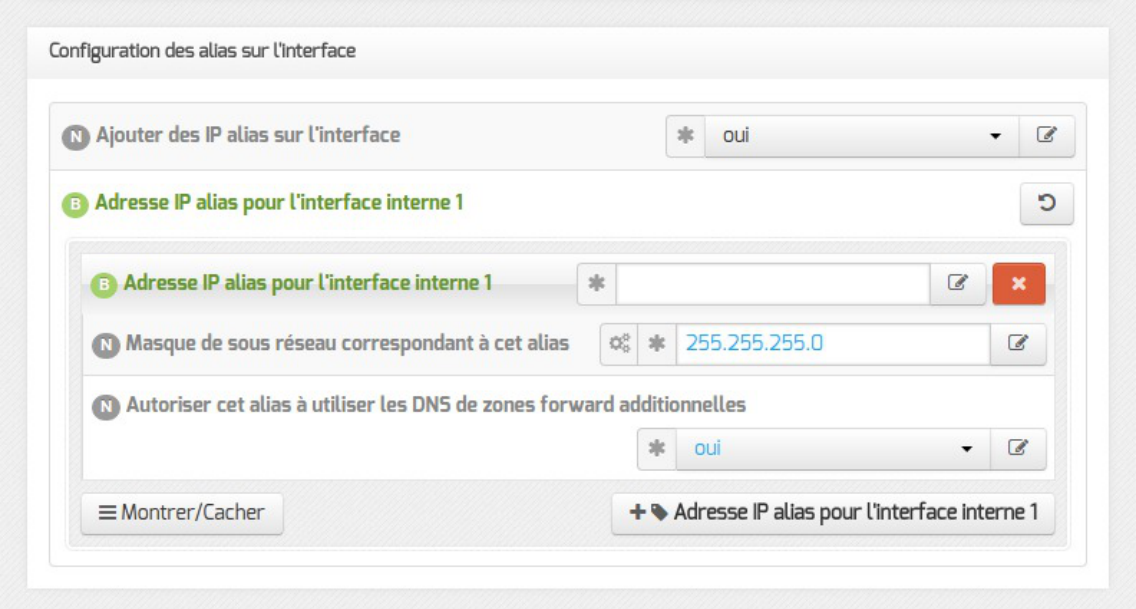
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -ni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

Configuration des alias sur l'interface

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

La variable `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`.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

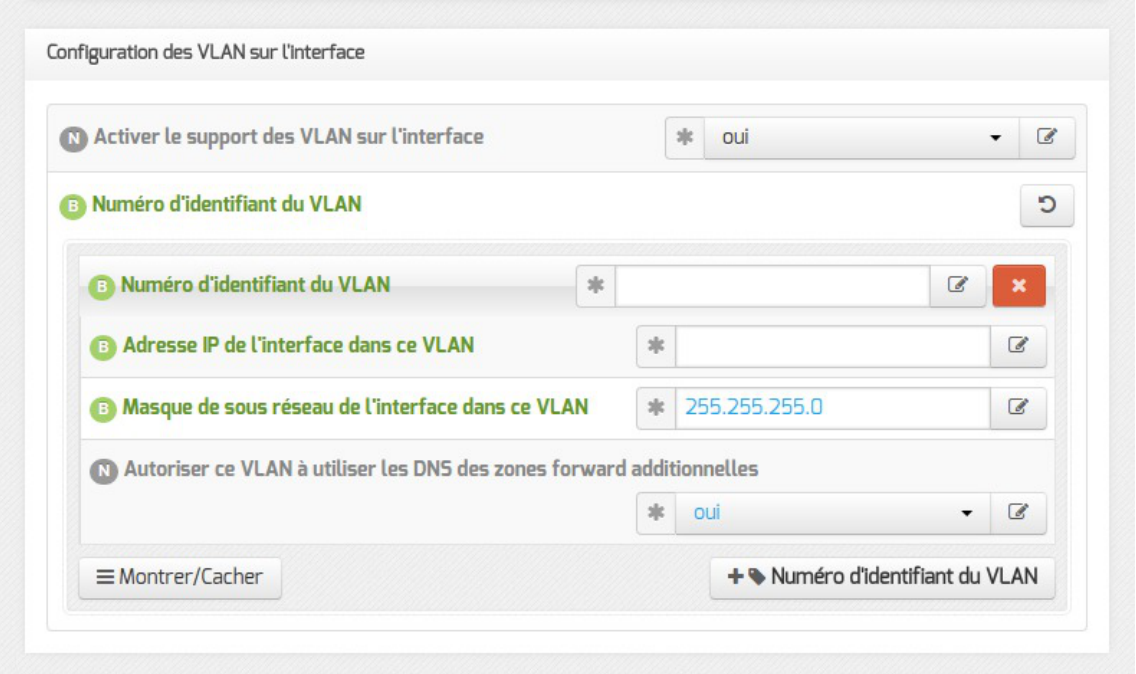
Si le support du RVP est activé une option supplémentaire est disponible :

- `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[p.734] (réseau local virtuel) sur une interface déterminée du module.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

La variable `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`.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

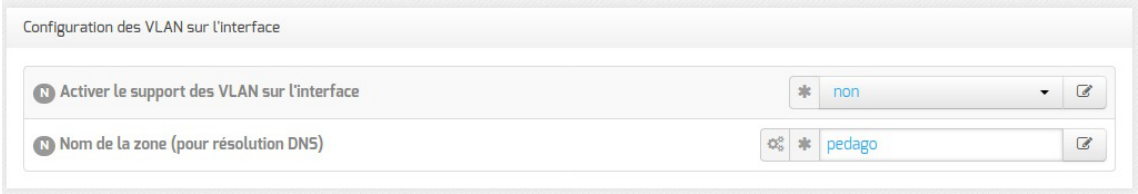
Si le support du RVP est activé une option supplémentaire est disponible :

- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

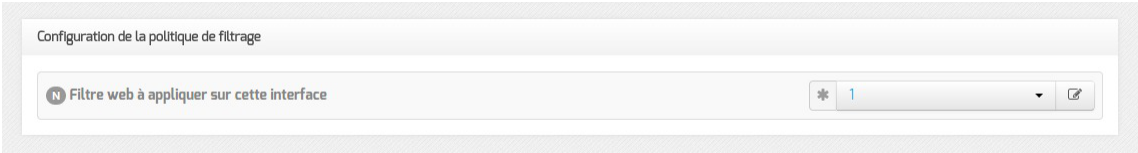


- `Nom de la zone (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface. Le nom (par défaut admin pour l'interface 1) doit être différent pour chacune des interfaces.

Configuration des zones de filtrage

La solution de filtrage permet de différencier 2 zones, ce qui permet de dissocier 2 politiques de filtrage majeures et distinctes comme par exemple une zone réseau administratif et une zone réseau pédagogique.

Il faut choisir à quelle zone appartient une interface. Cela s'effectue dans la configuration de chaque interface réseau en sélectionnant le numéro de la zone souhaité dans le champ `Filtre Web à appliquer à cette interface`.



Les zones `Filtre web 1` et `Filtre web 2` correspondent chacun à une instance du logiciel de filtrage. La configuration de chacune des instances s'effectue dans l'onglet Filtrage web.

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.285]

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 routes IP

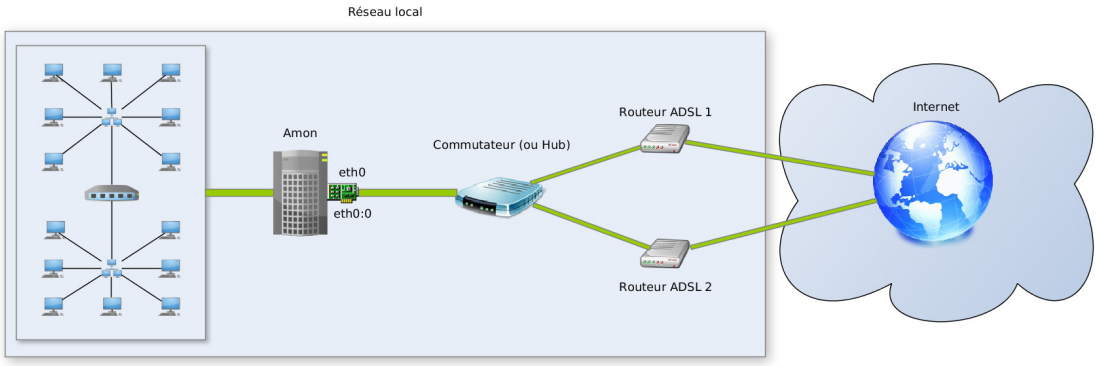
L'agrégation de routes IP (niveau 3) permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

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

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP[p.728] et OSPF[p.724] ;
- il faut un service qui surveille l'état de chacun des liens.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



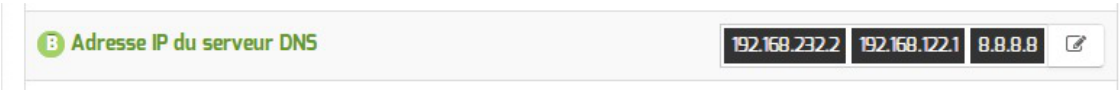
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

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

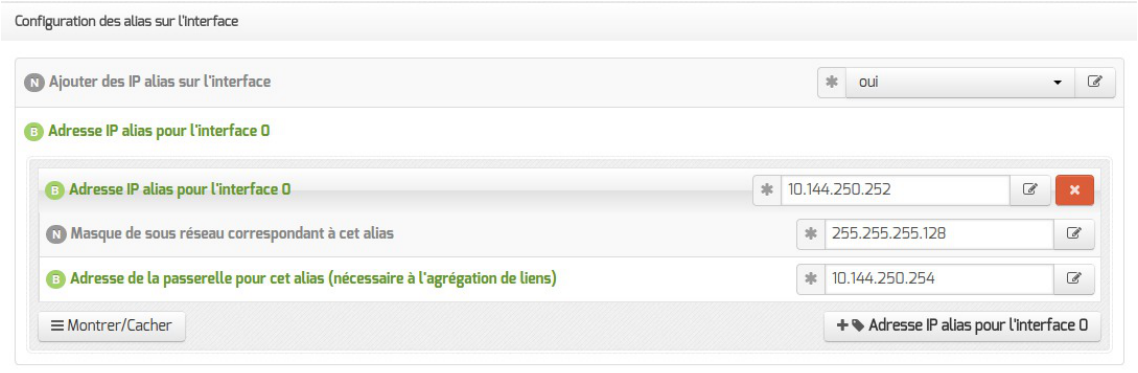
Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

Il faut, en premier lieu, déclarer un alias sur l'interface 0 dans la section `Configuration des alias sur l'interface`.

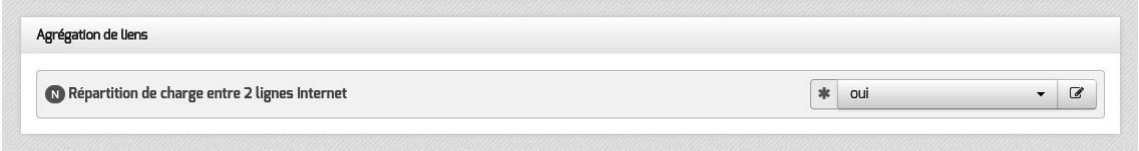
Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

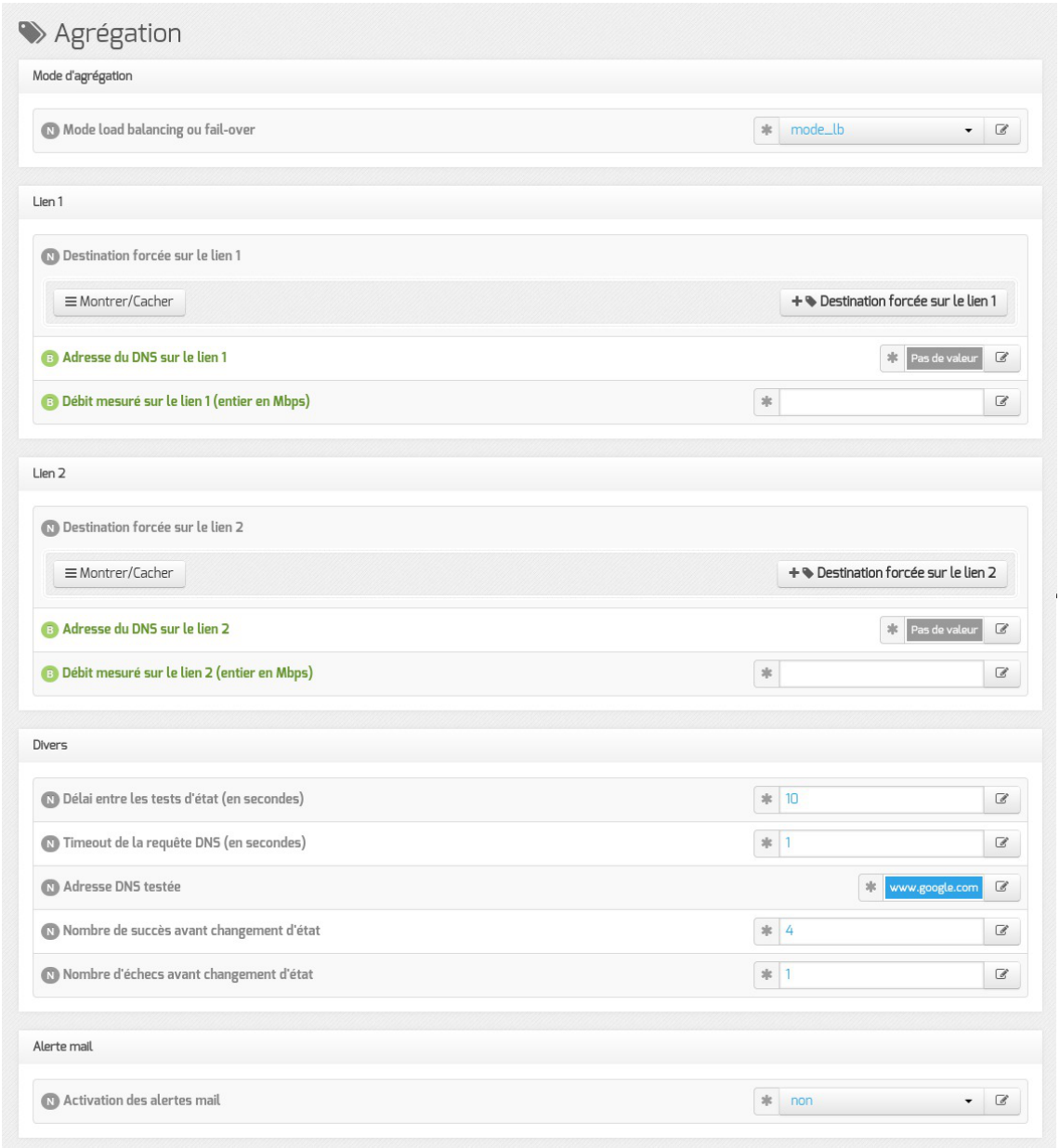
L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.



Un nouvel onglet, `Agrégation`, est disponible.

Onglet Agrégation : Configuration de l'agrégation de routes IP

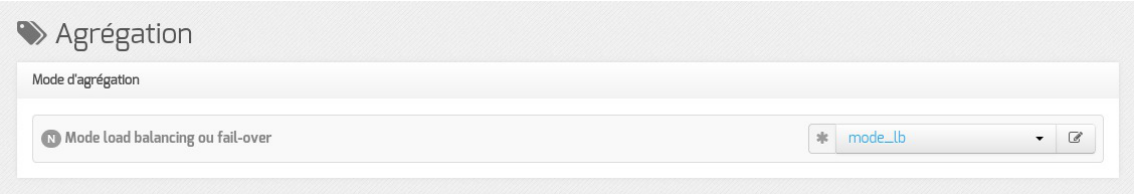
Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.



Paramétrage de l'agrégation de liens

Modes d'agrégation

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Il existe deux modes d'agrégation :

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

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

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



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

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

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

Adresse des DNS

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



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

Adresse DNS testée

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



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

Alerte mail

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

Commandes

L'agrégation peut être suspendue et/ou relancée à l'aide du script `agregation` :

```
root@amon:~# agregation status
le service Agregation n'est pas démarré
root@amon:~#
```

L'option -h affiche l'aide de la commande :

```
root@amon:~# agregation -h
Usage: /usr/share/eole/sbin/agregation {start|stop|status|restart}
root@amon:~#
```

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.

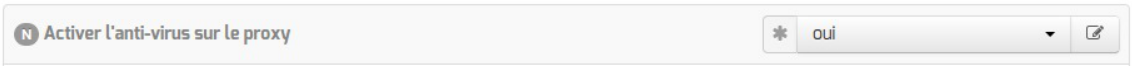


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

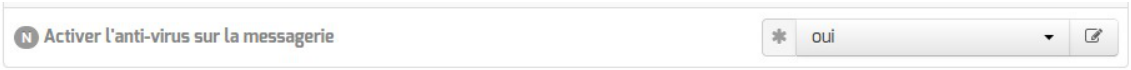


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.708]. 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.728] comme étant des faux positifs.

3.9. Onglet Relai DHCP

Pour des raisons de sécurité, le service DHCP[p.708] 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast[p.705].

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 (interface 3) vers le réseau pédagogique (interface 2).

Il est possible de restreindre le relayage sur un VLAN[p.734] 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.569]
- Configuration du module Amon avec le module Scribe en DMZ [p.337]

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.723]. Il permet d'installer plusieurs clients sur le

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

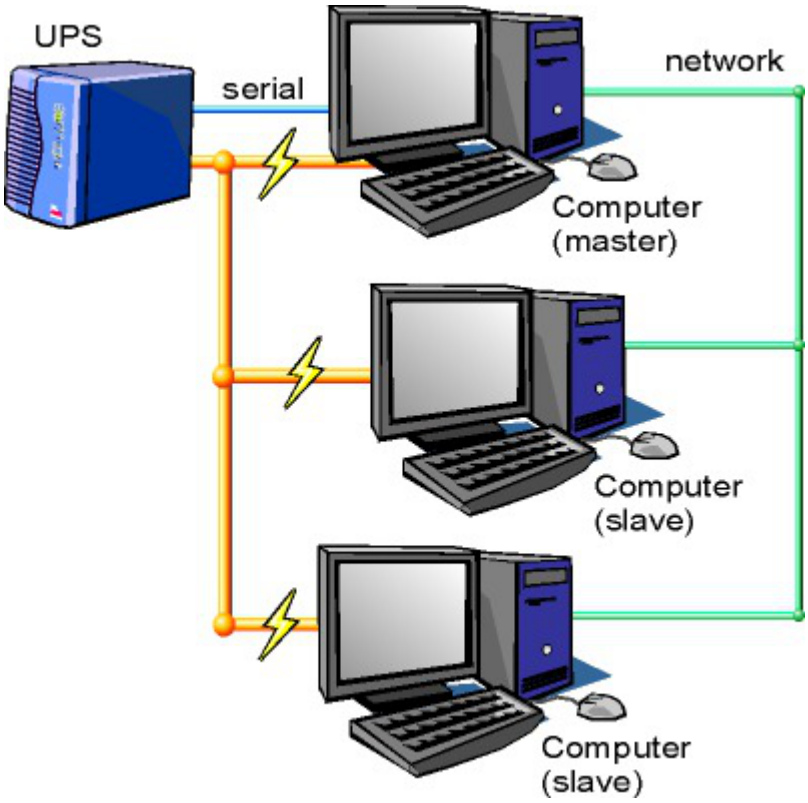


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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

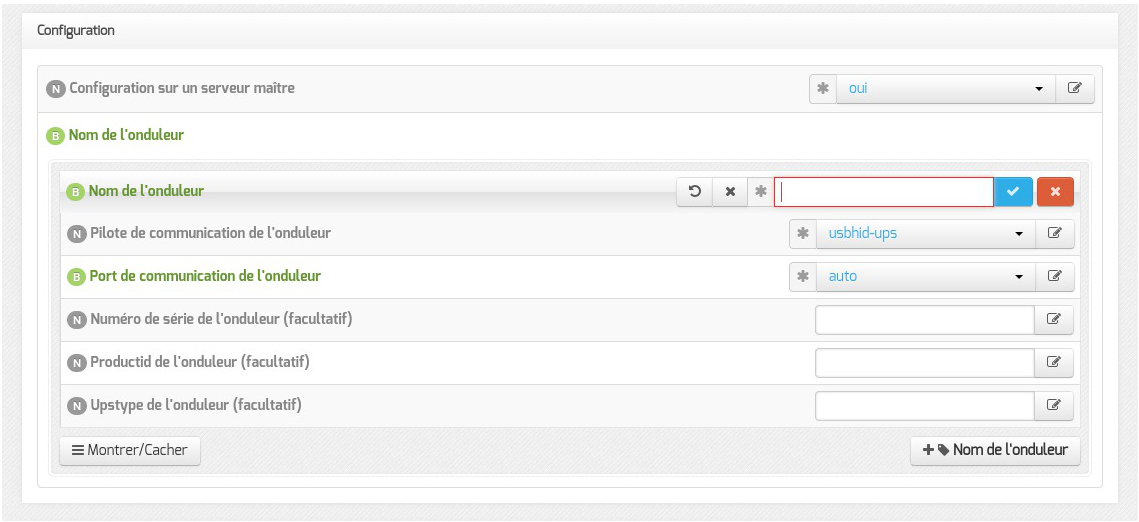
L'onglet `Onduleur` n'est accessible que si le service est activé dans l'onglet `Services`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

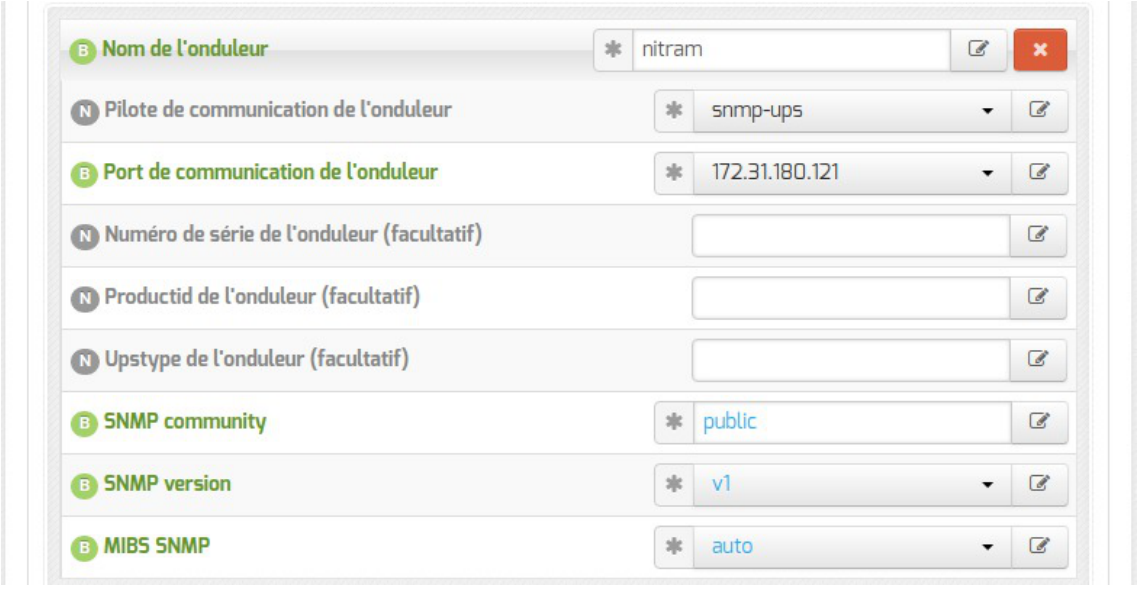
Le nom de l'onduleur ne doit contenir que des chiffres ou des lettres en minuscules : *[a-z][0-9]* sans espaces, ni caractères spéciaux.

NUT SNMP

À partir d'EOLE 2.7.2, les onduleurs utilisant une connexion SNMP[p.731] (driver `snmp-ups`) sont gérés nativement et des variables supplémentaires apparaissent dans l'interface.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La configuration ci-dessous convient, par exemple, pour un onduleur NITRAM Cyberpower :



Si le driver `snmp-ups` est sélectionné, le paramétrage de la `Fréquence d'interrogation de upsmon` est également proposé mais en mode expert uniquement.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 :

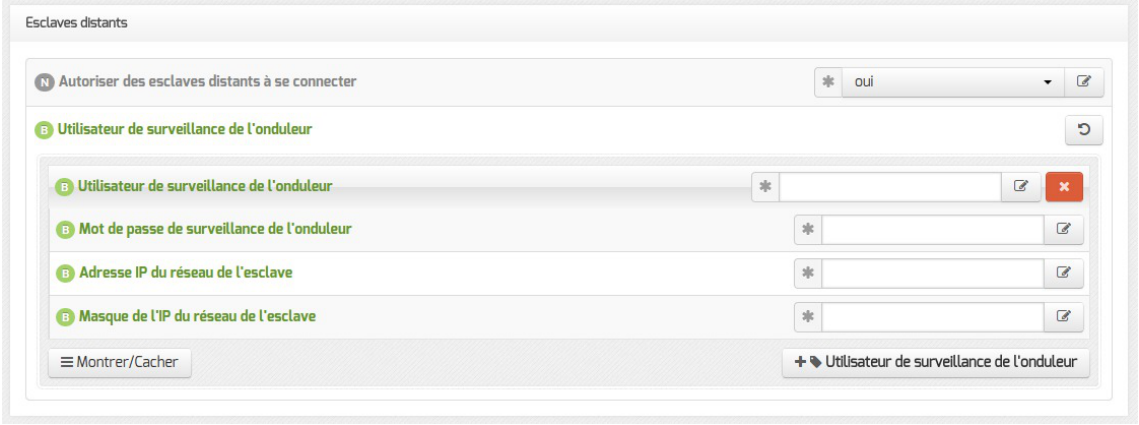
- Nom de l'onduleur : `eoleups` ;
- Pilote de communication de l 'onduleur : `usbhid-ups` ;
- Port de communication de l'onduleur : `auto`.

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 a se connecter avec cet utilisateur.



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 : https://manpages.ubuntu.com/manpages/jammy/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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

serveur maître).

À partir d'EOLE 2.7.2, il est possible de déclarer plusieurs onduleurs distants.

Exemple de configuration

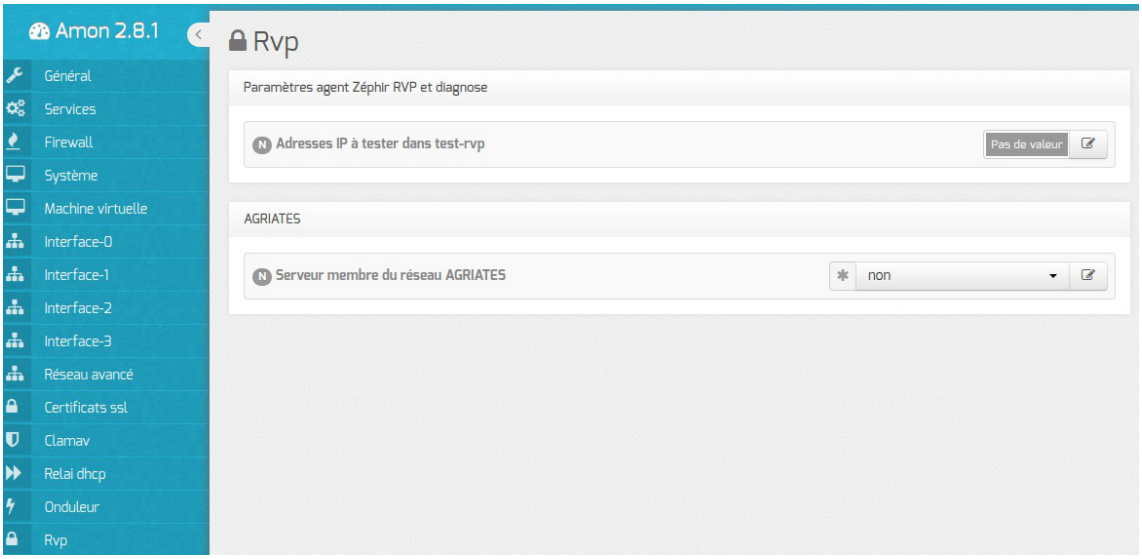
Sur le serveur maître :

- 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

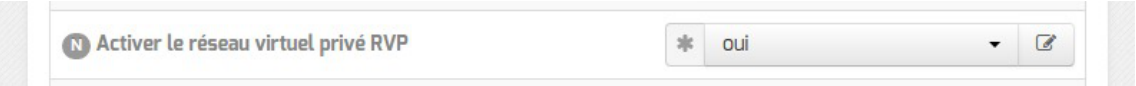


Le réseau virtuel privé[p.728] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur un module Amon déjà en exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

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[p.702] 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] :`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

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

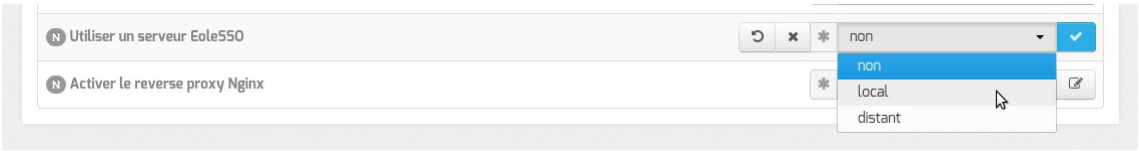
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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 SSO distant (configuration cliente).

Serveur EoleSSO local

À partir d'EOLE 2.9, l'outil EoleSSO s'exécute dans un conteneur[p.707] logiciel Podman[p.726].

L'image `eole-sso-server` est téléchargée depuis le site hub.eole.education [http://hub.eole.educ

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

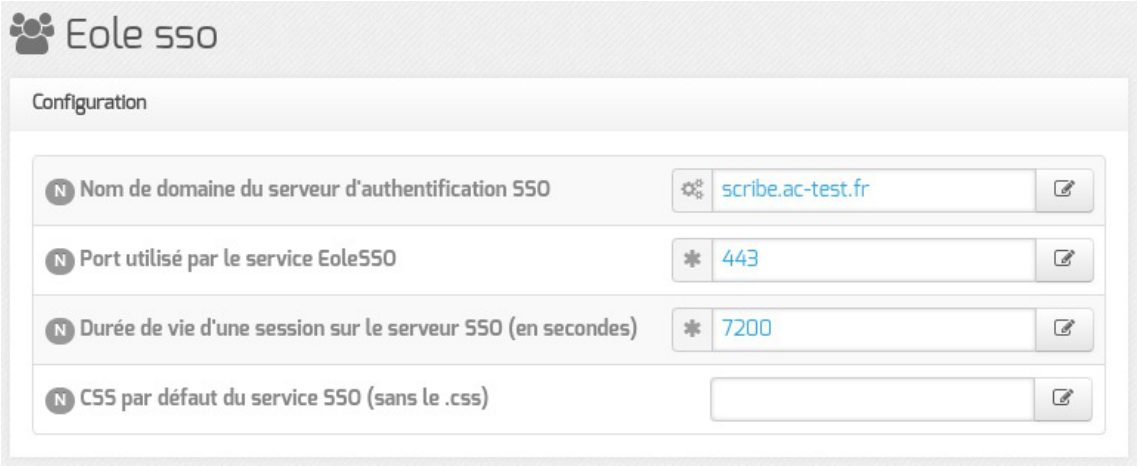
ation] .

Le serveur doit donc pouvoir accéder à ce domaine au même titre qu'aux serveurs de mise à jour des modules.

Adresse et port d'écoute

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



Configuration d'un serveur EoleSSO local

- `Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).
- `CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet*.

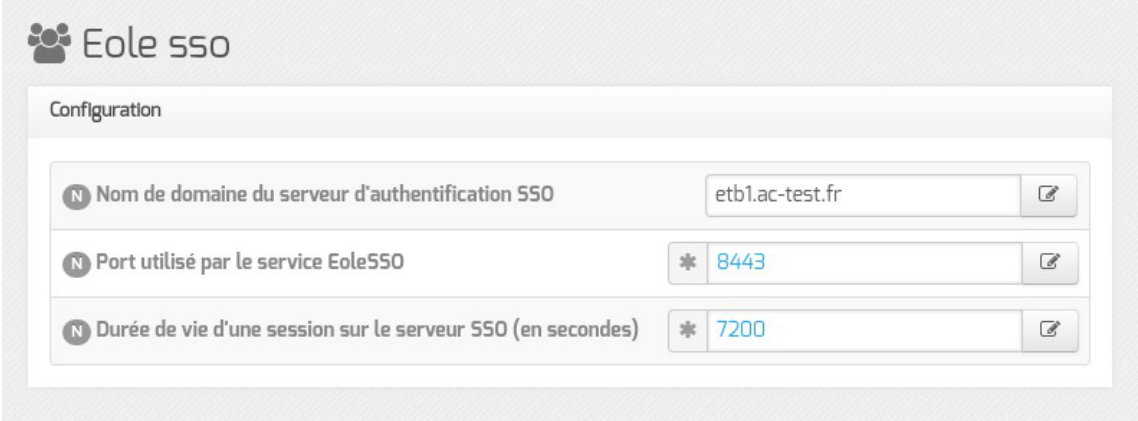
Port 443

Si le port HTTPS (`443`) est déclaré pour ce service, alors celui-ci est uniquement accessible via l'URL `https://<nom du serveur>/sso`.

L'URL de la forme `https://<nom du serveur>:<port>/` reste valable pour les autres valeurs de port que `443`.

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.

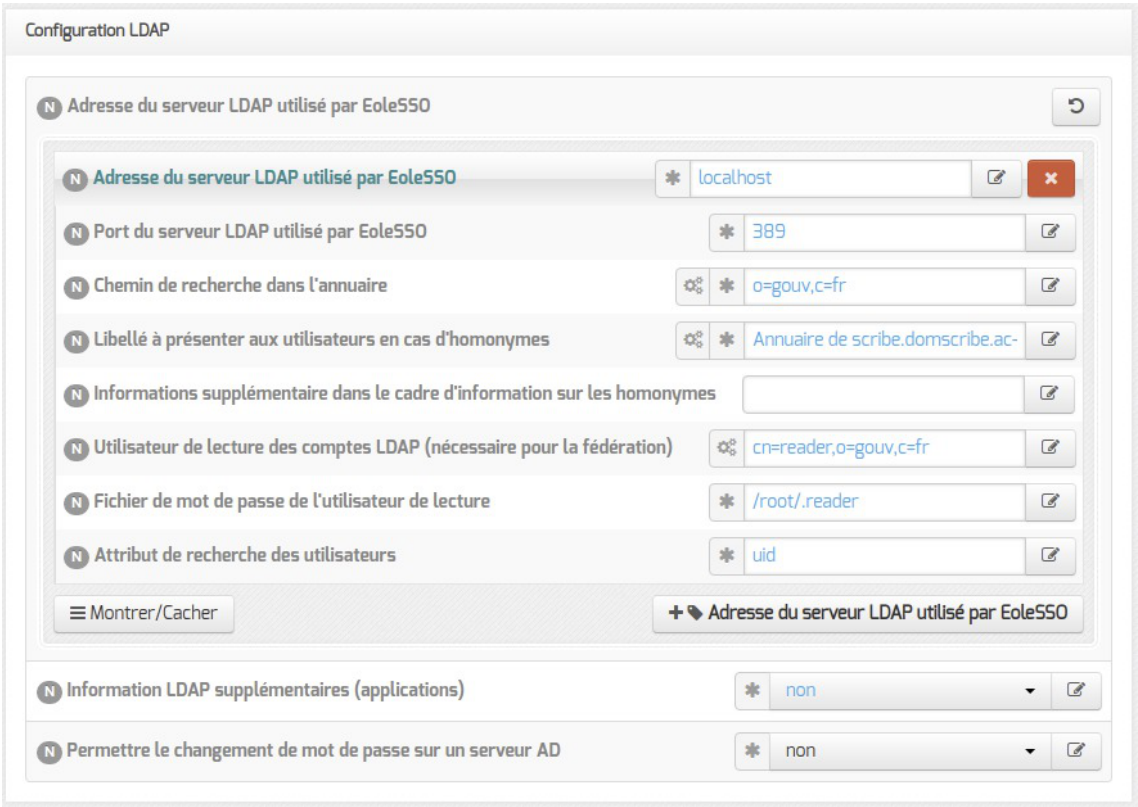
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Configuration d'un serveur EoleSSO distant

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.717] 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 (basedn) ;
- 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 ») ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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[p.709] 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.725] 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…).

Passer la variable `Permettre le changement de mot de passe sur un serveur AD` à `oui` permet à l'utilisateur de changer son mot de passe depuis la mire SSO si ce dernier à expiré.

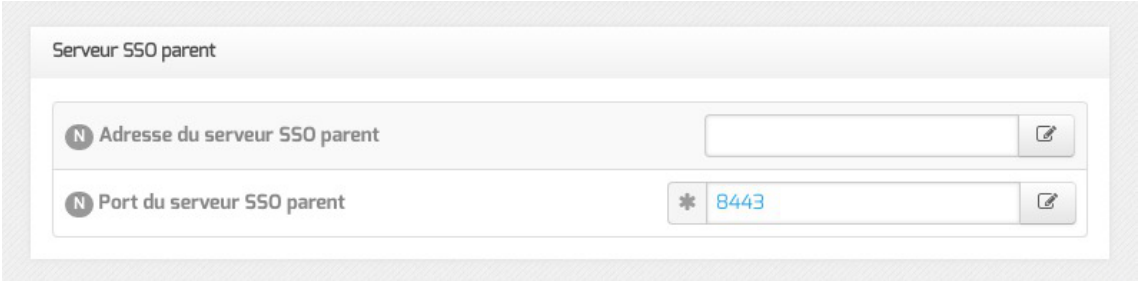
Il est alors nécessaire de renseigner le nom du domaine AD et le nom du serveur AD sur lequel changer le mot de passe.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Serveur SSO parent

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



Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.735] 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.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.730] (version 2).



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

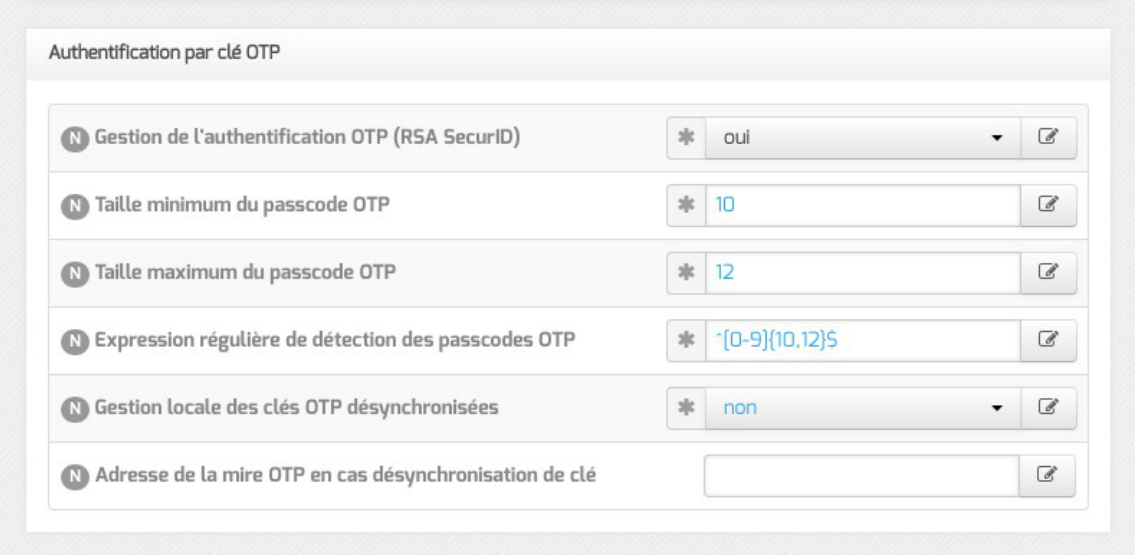
`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant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

Authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

securID[p.730] 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 :

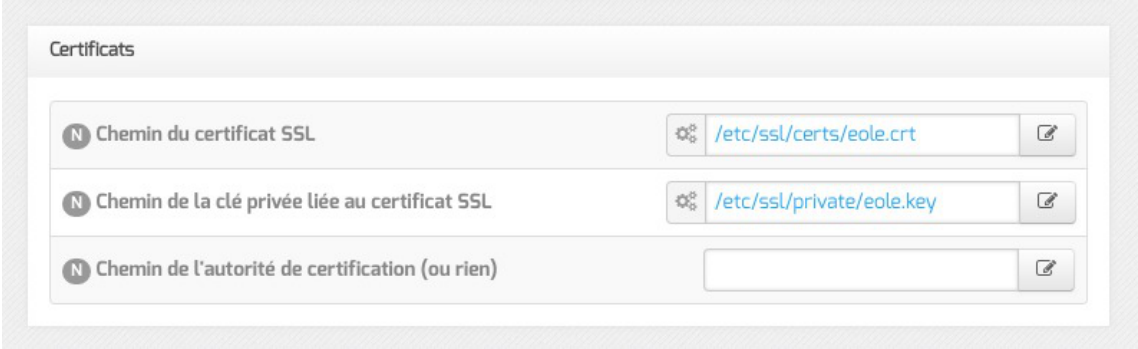
- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également 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.716] du serveur et sont utilisés par défaut.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

Voir aussi...

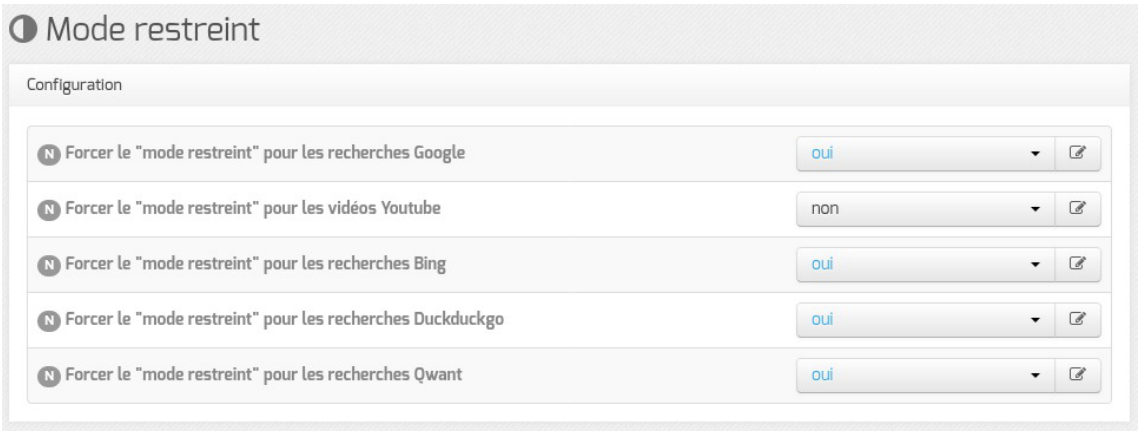
> Gestion des sources d'authentification multiples

3.13. Onglet Mode Restreint : Configuration des restrictions de navigation

Le mode restreint ou safe search[p.729] permet d'activer la navigation restreinte, soit bloquer les contenus "sensibles" pour les utilisateurs du domaine.

Les différentes cibles du mode restreint

L'activation du mode restreint s'effectue dans l'onglet `Mode restreint`.



Il est possible d'activer le mode restreint pour certaines applications

- `Forcer le "mode restreint" pour les recherches Google` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Google ;
- `Forcer le "mode restreint" pour les vidéos Youtube` : bloque les contenus à caractères sensibles pour les vidéos Youtube ;
- `Forcer le "mode restreint" pour les recherches Bing` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Bing ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Forcer le "mode restreint" pour les recherches Duckduckgo` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Duckduckgo ;
- `Forcer le "mode restreint" pour les recherches Qwant` : bloque les contenus à caractères sensibles pour les résultats de recherche sur Qwant ;

> Sur les versions précédentes, la mise en œuvre du mode restreint s'appuyait sur des réécritures d'URL gérées directement dans le logiciel de filtrage e2guardian[p.710].
>
> À partir d'EOLE 2.8.1, ce sont des redirections DNS[p.709] qui sont utilisées. Cela nécessite d'avoir la main sur ce service, ce qui n'est pas le cas sur le module `Eolebase+Proxy`.

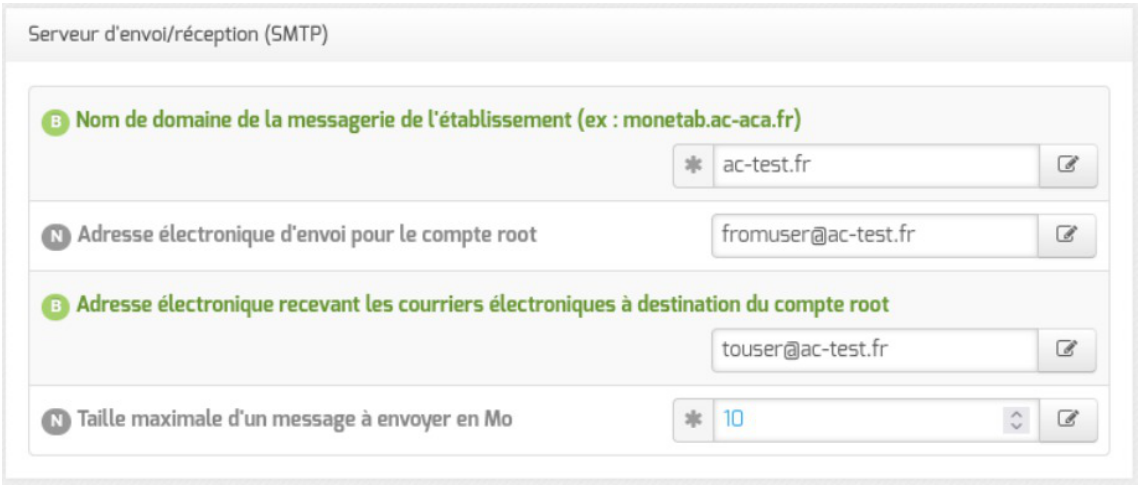
3.14. Onglet Messagerie

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 courriers électroniques.

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

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

Serveur d'envoi/réception (SMTP)



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 d'envoi pour le compte root` , saisir l'adresse que l'on souhaite utiliser pour l'envoi de courriers électroniques depuis le compte root.
- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Taille maximale d'un message à envoyer en Mo`, indiquer la taille maximale des courrier électroniques qui seront envoyés par exim.



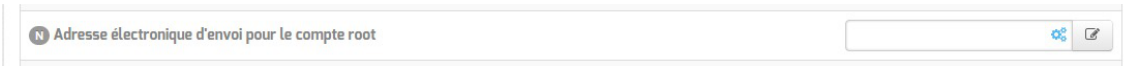
Le `Nom de domaine de la messagerie de l'établissement` (onglet `Messagerie`) ne peut pas être le même que celui d'un conteneur. Le nom de la machine (onglet `Général`) donne son nom au conteneur maître aussi le `Nom de domaine de la messagerie de l'établissement` ne peut pas avoir la même valeur.

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

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



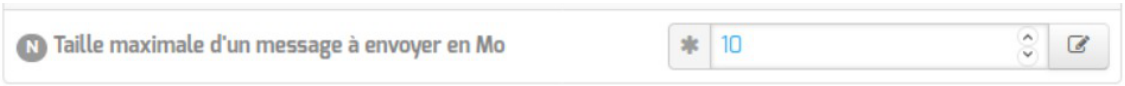
Dans le cas où le `Nom de domaine de la messagerie de l'établissement` n'est pas le même que la concaténation du `Nom de la machine` et du `Nom DNS du réseau local`, il peut être nécessaire d'activer la réécriture des en-têtes (cf. Onglet Messagerie) [p.276] pour avoir des informations cohérentes avec l'enveloppe des courriels.



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.



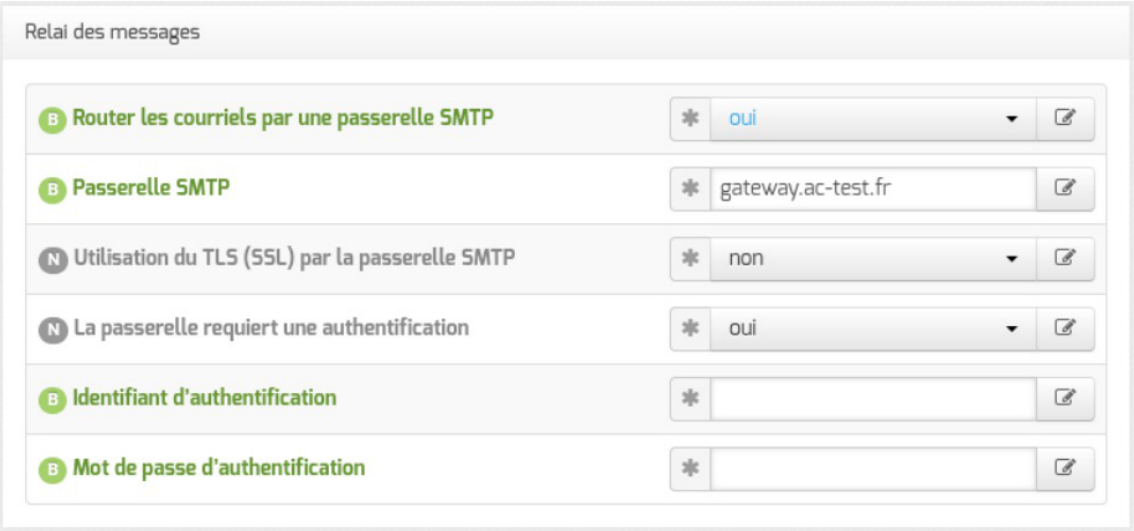
Il est également possible de configurer la taille maximale des messages électroniques.



Sur les modules utilisant le webmail Roundcube, elle ne devrait pas dépasser la taille maximale d'un fichier à charger définie pour Apache.

Relai des messages

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

Il est possible d'activer le support du TLS[p.733] pour l'envoi de messages.

Si la passerelle SMTP[p.731] accepte le TLS, il faut choisir le port en fonction de la prise en charge de la commande STARTTLS[p.732].

Pour cela il suffit d'indiquer le port spécifique dans l'option `Utilisation de TLS (SSL) par la passerelle SMTP` il y a cinq possibilités.

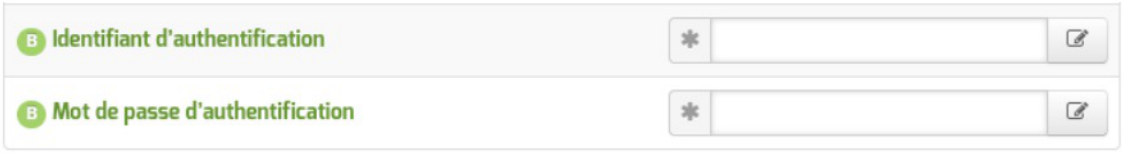
1. non
2. port 25
3. port 465
4. port 587
5. port personnalisé

Le dernier choix permet à l'utilisateur de saisir un port différent de ceux proposés dans une nouvelle option appelée `Port de la passerelle SMTP`.

Dans le cas où la passerelle nécessiterait une authentification il est nécessaire de le signaler en passant la variable `La passerelle requiert une authentification` à `oui`.

Cette action affiche deux nouvelles variables :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



3.15. 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`.



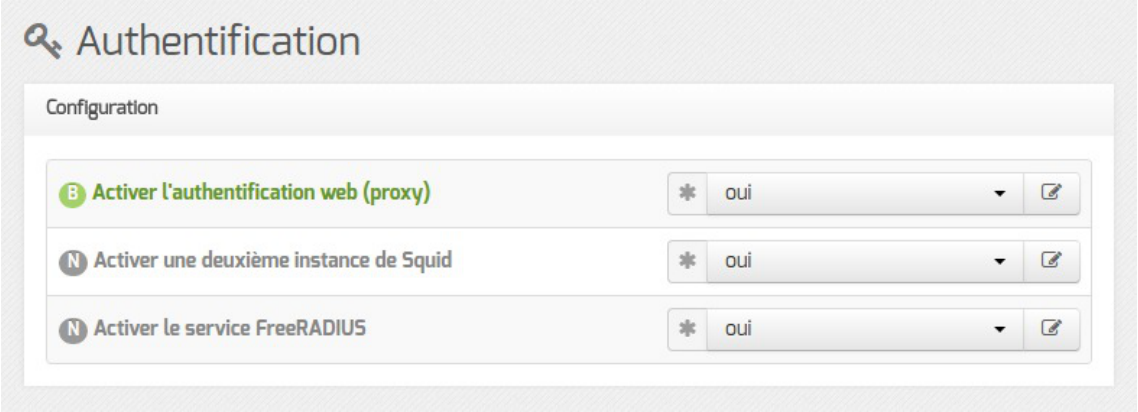
Cela fera apparaître l'onglet `Proxy authentifié 2`.

Activer le service FreeRADIUS

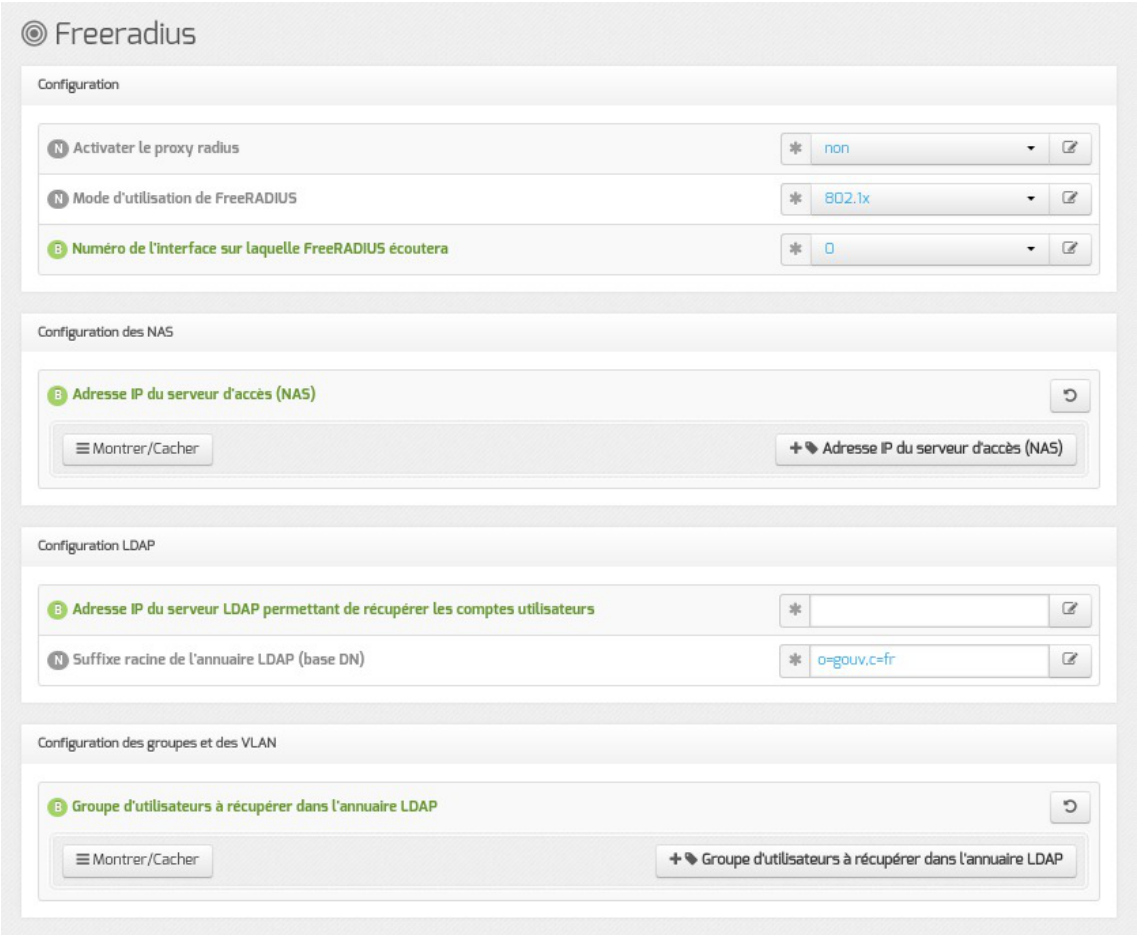
EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.728].

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Cela fera apparaître l'onglet Freeradius.



Voir aussi...

Onglet Proxy authentifié : 4 méthodes d'authentification [p.157]

Onglets Proxy authentifié 2 : Double authentification [p.161]

Onglet Freeradius : Configuration de l'authentification Radius [p.171]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

3.16. Onglets Squid et Squid2 : activation du déchiffrement HTTPS

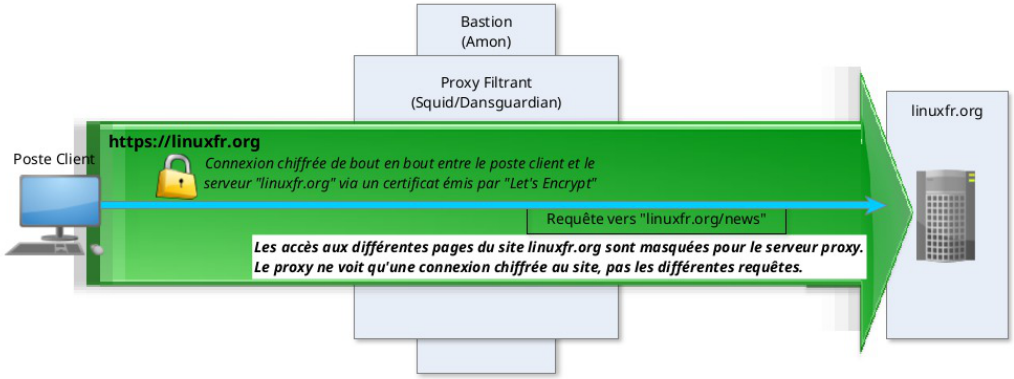
Déchiffrement et interception du protocole HTTPS

Par rapport au protocole HTTP[p.714], le protocole HTTPS permet de chiffrer la communication entre le navigateur du poste client et le serveur du site distant.

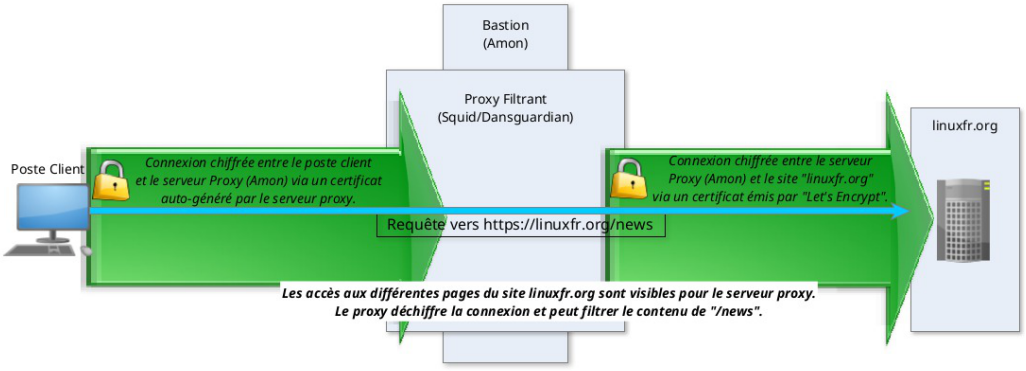
Dans ce cas, le serveur proxy ne journalise qu'une seule connexion vers le site distant (exemple : https://pcll.ac-dijon.fr) mais pas les différentes requêtes d'accès aux pages ou aux fichiers se trouvant sur ce serveur (exemple : https://pcll.ac-dijon.fr/eole/).

En HTTPS, le serveur Proxy ne peut pas filtrer le contenu des pages consultées ni scanner les fichiers téléchargés avec un antivirus.

Le déchiffrement HTTPS sur le serveur Proxy permet d'intercepter l'ensemble des requêtes et de les journaliser, de filtrer le contenu des pages visitées et de scanner les fichiers téléchargés.



Fonctionnement HTTPS normal



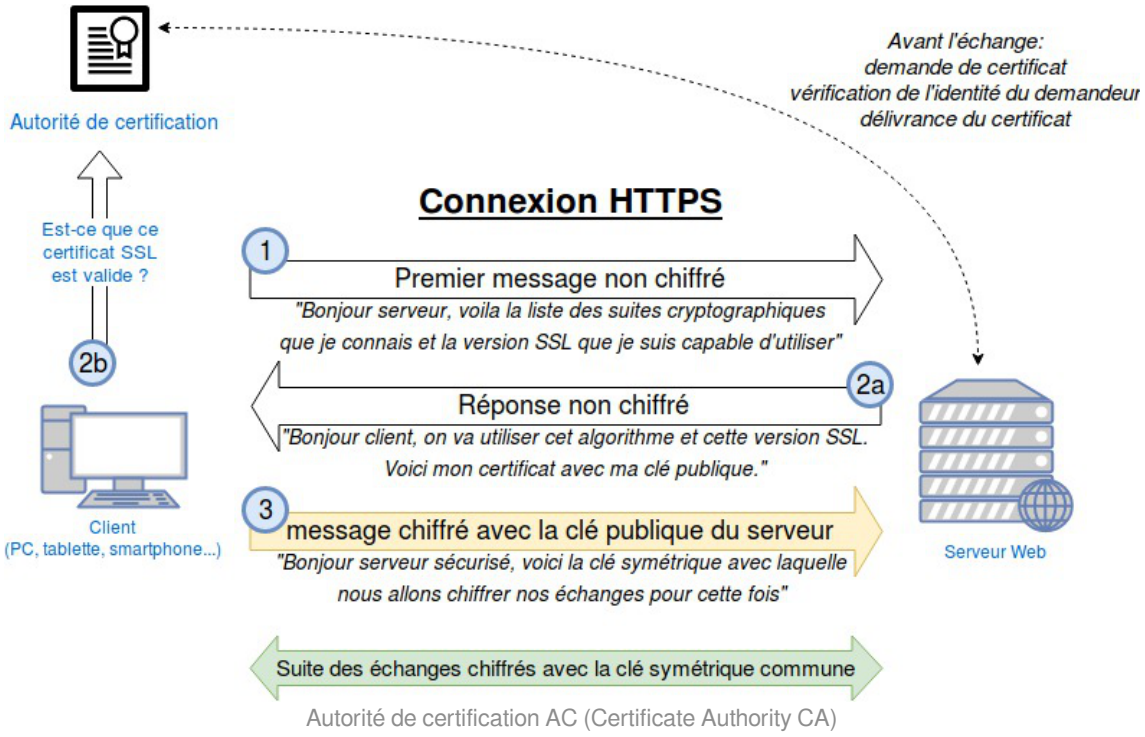
Fonctionnement HTTPS déchiffré par le Proxy

Certificat Racine de l'autorité de certification

Un certificat HTTPS est émis par une autorité de certification[p.704].

Let's Encrypt[p.717], par exemple, est une autorité de certification publique et connue des navigateurs ; son certificat racine est pré-installé dans les navigateurs et les systèmes d'exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



En revanche, le certificat racine utilisé par Amon pour déchiffrer le protocole HTTPS n'est pas public et il faut donc l'installer sur les postes clients dont le trafic doit être déchiffré et intercepté. La procédure est détaillée plus bas.

⚠ ATTENTION AUX LIMITATIONS LÉGALES

Dans la mesure où les connexions sont déchiffrées par le proxy, il convient de prévenir les utilisateurs, en particulier les adultes et le personnel. En effet, la loi reconnaît un droit à la vie privée même sur le lieu de travail : article 9 du Code civil et article L 1121-1 du Code du travail, entre autres.

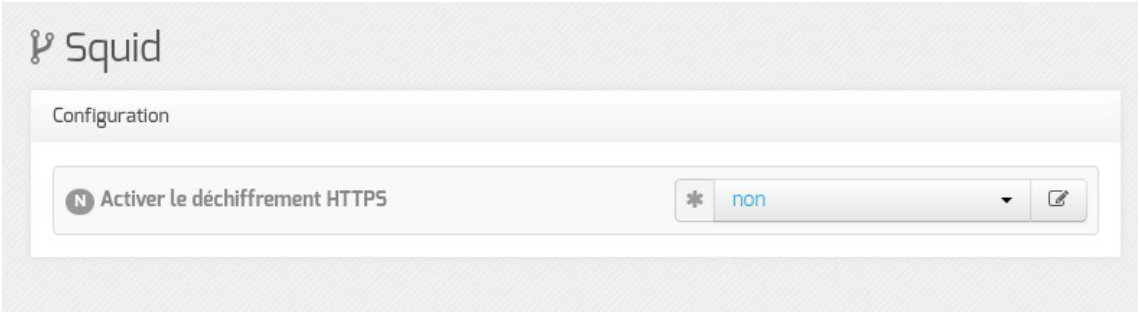
Dans certains cas, comme par exemple lors des accès aux sites bancaires ou aux sites médicaux, il ne semble pas évident que le déchiffrement HTTPS soit légal.

Mise en œuvre

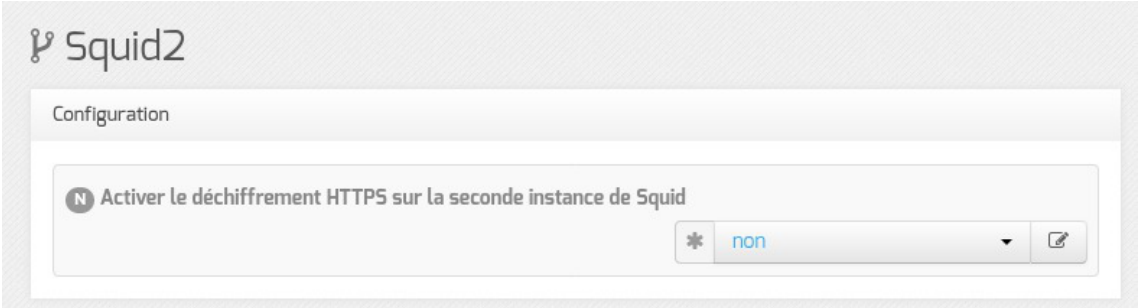
Deux variables ont été ajoutées dans les onglets `Squid` et `Squid2` :

- `Activer le déchiffrement HTTPS` ;
- `Activer le déchiffrement HTTPS sur la seconde instance de Squid`.

Ces deux variables permettent d'activer le déchiffrements des flux HTTPS transitant à travers le proxy.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Une fois le déchiffrement des flux HTTPS activé, le proxy a la capacité de connaître l'ensemble des URL consultées par l'utilisateur. Dans les journaux figureront donc les URL complètes et non uniquement les noms de domaines, comme c'est le cas sans le déchiffrement.

Dans ce mode de fonctionnement, le proxy génère un nouveau certificat pour chaque domaine visité et propose celui-ci à l'utilisateur. Tous ces certificats sont signés par une autorité de certification propre au proxy.

Pour que ces certificats soient perçus comme valides par les différentes applications utilisant le proxy, il est nécessaire de diffuser l'autorité de certification propre au proxy auprès de ces applications.

Sur un module Amon configuré pour l'interception des communications HTTPS, la commande `diagnose` permet de connaître le chemin et l'empreinte du certificat :

```
1 *** Validité du certificat racine du proxy (/etc/eole/squid_CA.crt)
2 .               signingCA.crt => Ok
3 .                   Empreinte => SHA256 Fingerprint=62
  :1B:BF:25:28:44:31:02:7E:09:31:A6:EA:FD:A5:A8:7C:D4:EB:B6:3D:83:88:62:0F:98:85:
4
```

Intégration de l'autorité de certification sur distributions Debian et dérivées

Copier le fichier `/etc/eole/squid_CA.crt` dans le répertoire du client : `/usr/local/share/ca-certificates/` et exécuter la commande :

```
sudo update-ca-certificates
```

Intégration de l'autorité de certification sur Windows

Copier le fichier `/etc/eole/squid_CA.crt` sur le poste. Cliquer droit dessus et faire "installer le certificat". Le certificat doit être mis dans le "magasin de certificat" : "Autorités de certification racines de confiance".

Les applications communes comme Edge, Chromium, les mises à jours, ... reconnaîtront ainsi cette autorité.

Intégration de l'autorité de certification dans le magasin du navigateur Firefox

Dans le "gestionnaire de certificats", présent dans l'onglet "Vie privée" des préférences du logiciel, se rendre dans l'onglet "Autorités". Il est alors nécessaire d'importer le fichier `/etc/eole/squid_CA.crt`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

disponible sur l'Amon. Lors de l'importation, penser à cocher "Confirmer cette AC pour identifier des sites web".

L'intégration du certificat peut être automatisée pour les postes joints à un domaine contrôlé par un module EOLE avec le paquet `eole-workstation-manager` installé.

Dans ce cas précis, la configuration du module contrôleur de domaine propose l'option `Activer la configuration de Firefox` qui met en place la procédure de déploiement du certificat sur les postes clients salt.

Pour plus d'informations, se reporter à la documentation des modules AmonEcole et Scribe, onglet `Workstation`.

3.17. Onglet Proxy authentifié : 4 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)`.



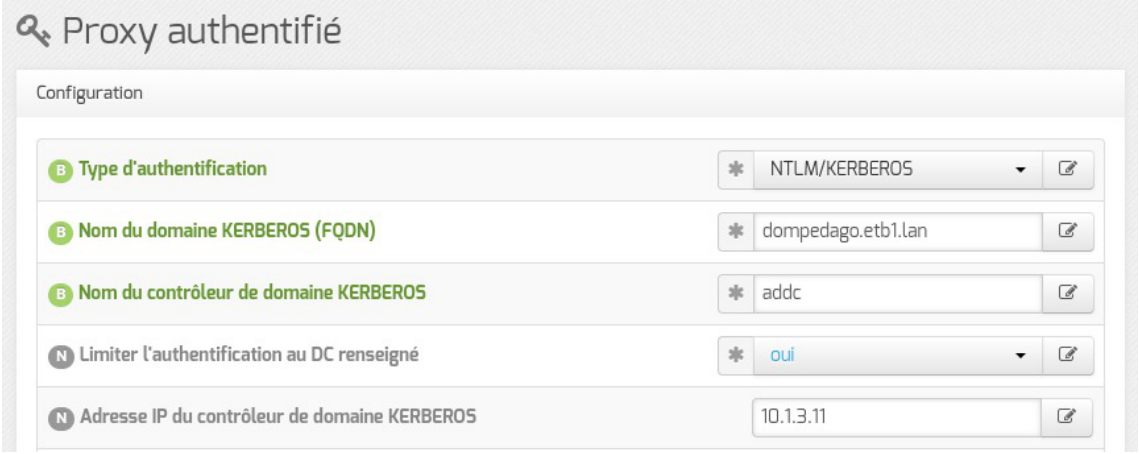
Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/KERBEROS

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory[p.702].

Cette configuration est à choisir si vous disposez d'un serveur Scribe ou Horus en mode AD ou d'un serveur Microsoft AD.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Si l'authentification `NTLM/KERBEROS` est activée sur le proxy, le `Nom de machine`, qui se paramètre dans l'onglet `Général`, ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.

À partir d'EOLE 2.8.1,

- il n'est plus obligatoire de fournir explicitement l'`Adresse IP du contrôleur de domaine KERBEROS` ;
- il est possible de désactiver la limitation de l'authentification au DC renseigné dans `Nom du contrôleur de domaine KERBEROS`.

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 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

À partir d'EOLE 2.8.1, lorsque l'authentification est configurée en mode `NTLM/KERBEROS`, les postes hors domaine peuvent utiliser directement le proxy authentifié.

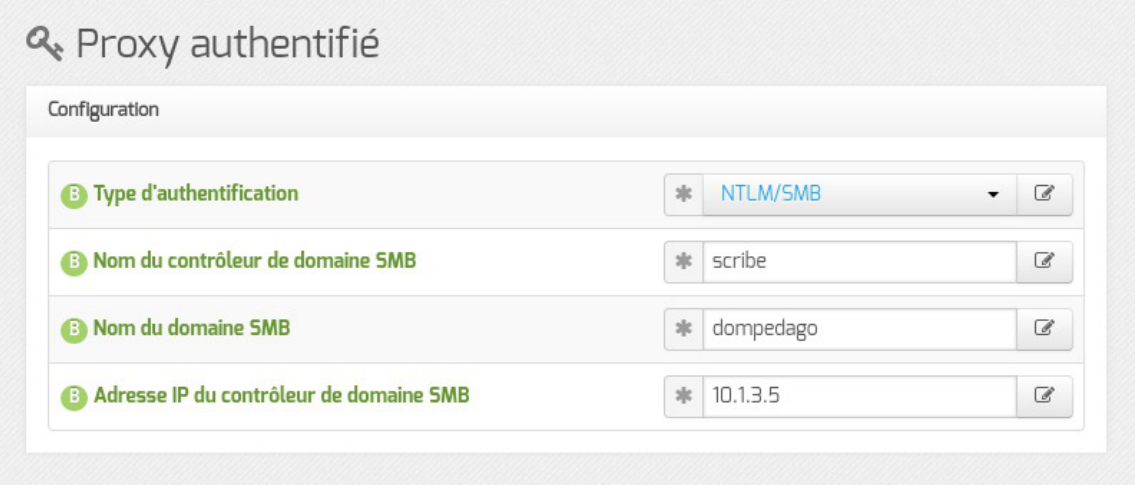
Contrairement aux versions précédentes pour lesquelles il était recommandé d'activer le proxy NTLM, les navigateurs proposent nativement une fenêtre d'authentification dans laquelle l'utilisateur saisit uniquement ses login et mot de passe Active Directory.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba[p.730] NT.

Cette configuration est à choisir si vous disposez d'une version ancienne du serveur pédagogique Scribe ou du serveur administratif Horus.



Cette méthode d'authentification nécessite l'intégration du serveur au domaine Samba.

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 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`.

L'enregistrement au domaine étant proposé lors de l'instanciation du module, de ce fait l'authentification NTLM/SMB n'est plus proposée pour une deuxième authentification.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.



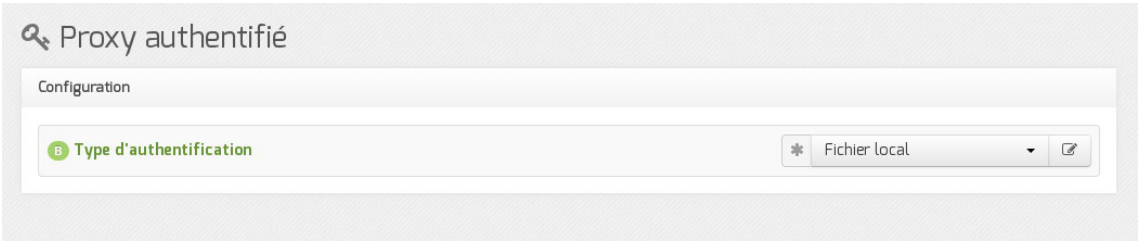
Cet annuaire est interrogé uniquement si le premier ne répond pas.
Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

Authentification LDAP (Active Directory)



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

Authentification sur Fichier local



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

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



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

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

ou

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

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors interface 0 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 de l'interface 2, 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)`.

Notes techniques

Les fichiers de logs spécifiques au premier type d'authentification sont les suivants :

- `/var/log/rsyslog/local/squid/squid1.info.log` → 1ère instance de squid
- `/var/log/rsyslog/local/e2guardian/e2guardian0.info.log` → 1ère instance de e2guardian (filtre web 1)
- `/var/log/rsyslog/local/e2guardian/e2guardian1.info.log` → 2ème instance de e2guardian (filtre web 2)

3.18. Onglets Proxy authentifié 2 : Double authentification

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

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

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

Configuration pas à pas

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



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'enregistrement au domaine est proposé lors de l'instanciation du module, de ce fait l'authentification NTLM/SMB n'est plus proposée pour une deuxième authentification.

Notes techniques

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

- `/var/log/rsyslog/local/squid/squid2.info.log` → 2ème instance de squid
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log` → 3ème instance de e2guardian (filtre web 3)

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).

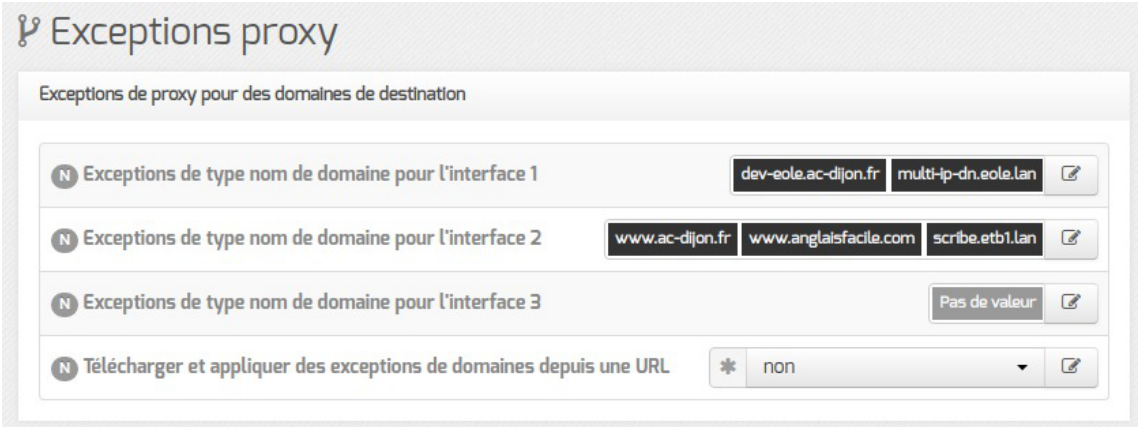
3.19. Onglet Exceptions proxy

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.

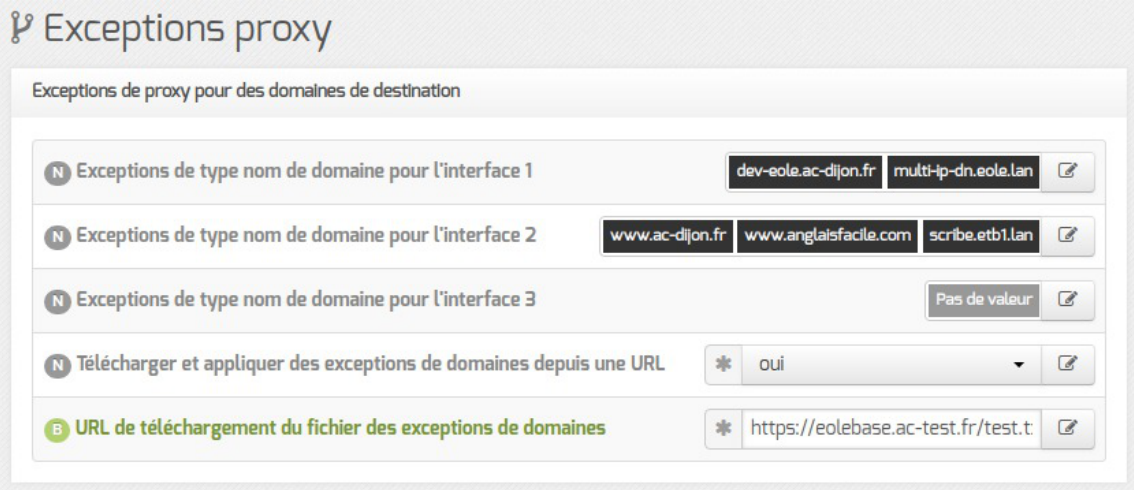
Exception de proxy pour des domaines de destination

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



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

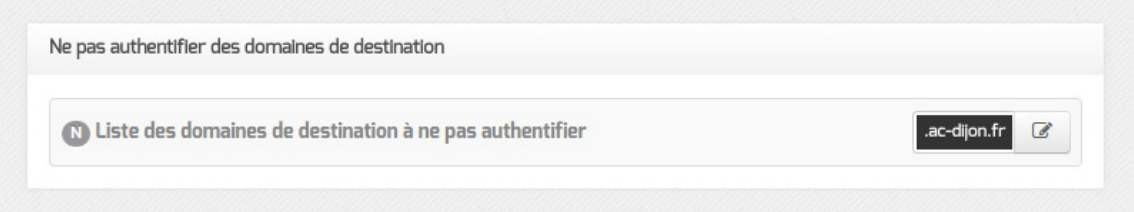


Il est également possible de fournir une liste de noms de domaine ou d'IP à inclure dans les exceptions au proxy depuis une URL, en activant la variable `Télécharger et appliquer des exceptions de domaine depuis une URL`.

Si vous utilisez une copie des modèles ERA fournis, il faudra l'adapter pour obtenir les règles supplémentaires

Exception au niveau de l'authentification des domaines de destination

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



Si WPAD est activés sur l'interface réseau, les utilisateurs utiliseront directement Squid pour accéder à ces sites.

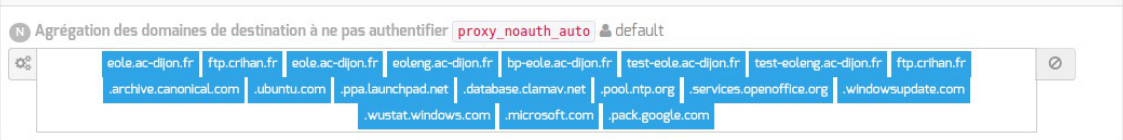
Les domaines commençants par un `.` sont gérés, le domaine lui-même et les sous-domaines ne sont pas authentifiés.

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.

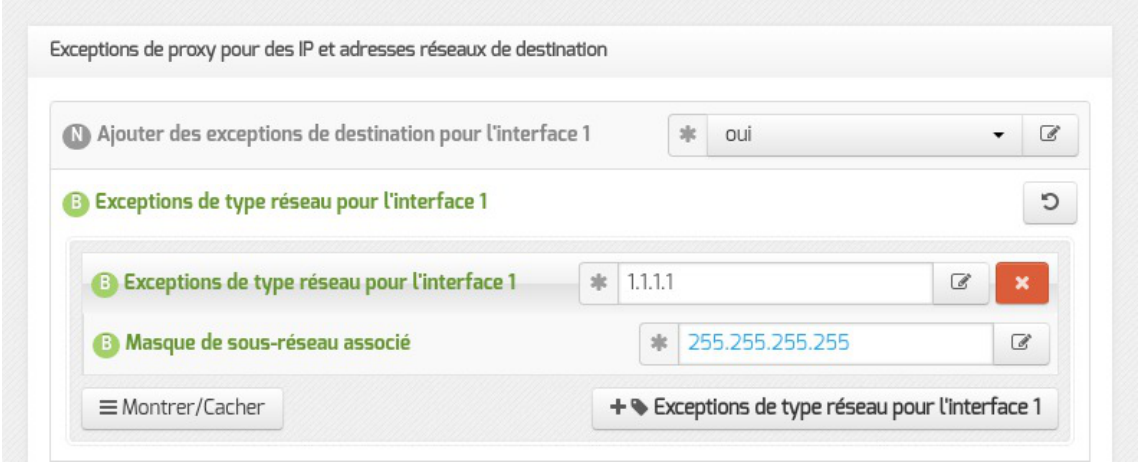
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

Exceptions de proxy pour des IP et adresses réseaux de destination

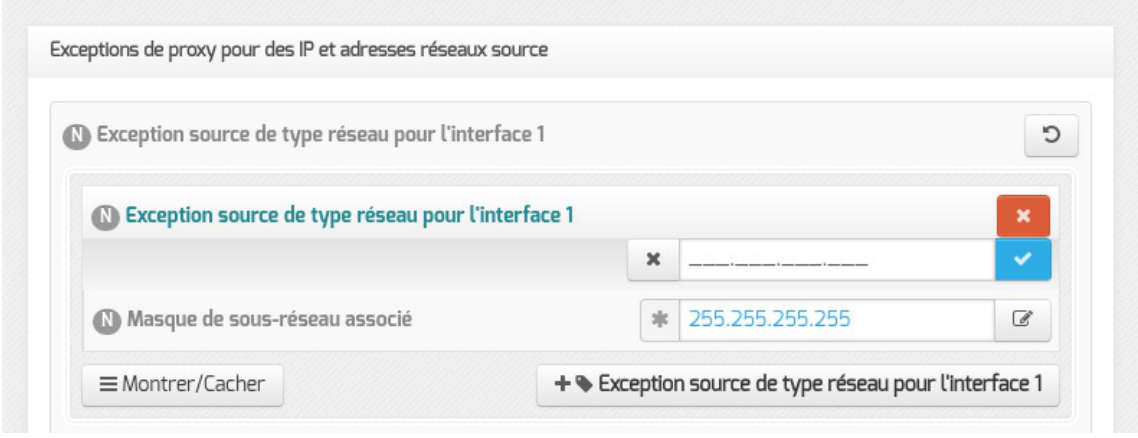
Cette exception commune à ERA et à WPAD permet de déclarer une adresse IP ou une plage d'adresses IP de **destination** pour laquelle on ne passe pas par le proxy.



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

Exceptions de proxy pour des IP et adresses réseaux source

Cette exception spécifique à ERA permet de déclarer une adresse IP ou une plage d'adresses IP **source** pour laquelle on ne passe pas par le proxy.



Le bouton `+ Exception source de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.



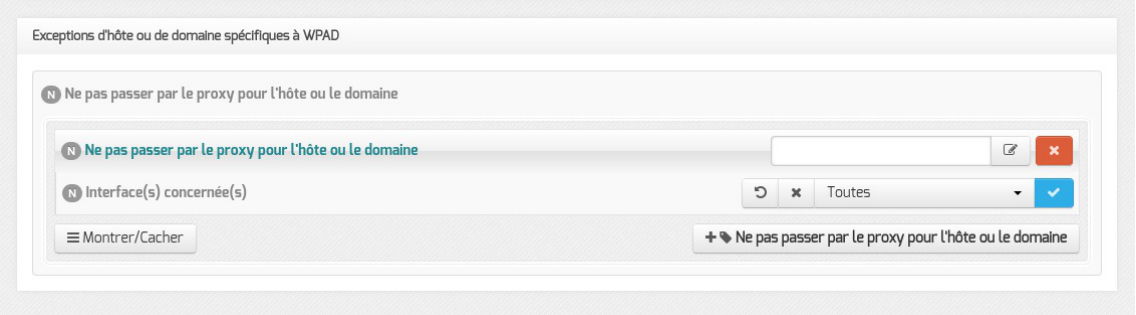
Cette fonctionnalité permet à une machine de contourner le proxy ce qui constitue un non respect des règles légales de sécurité. Elle peut servir pour effectuer des tests de proxy et

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

d'exceptions de filtrage.

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

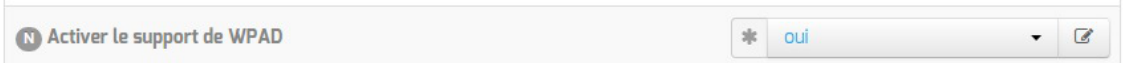
3.20. Onglet Wpad : découverte automatique du proxy

WPAD est mis à disposition sur les modules Amon et AmonEcole au travers du paquet `eole-wpad`.

Sur un module personnalisé, il n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

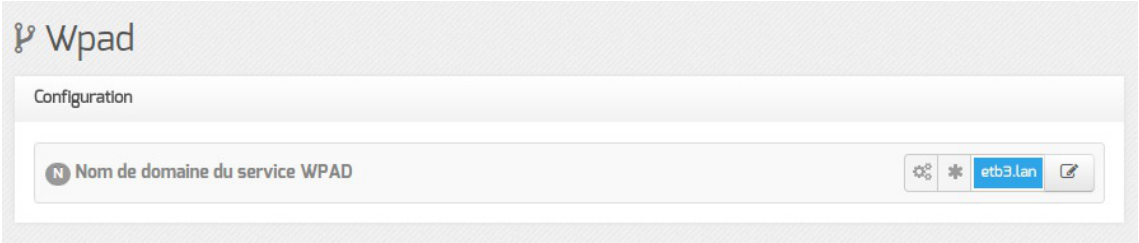
Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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...

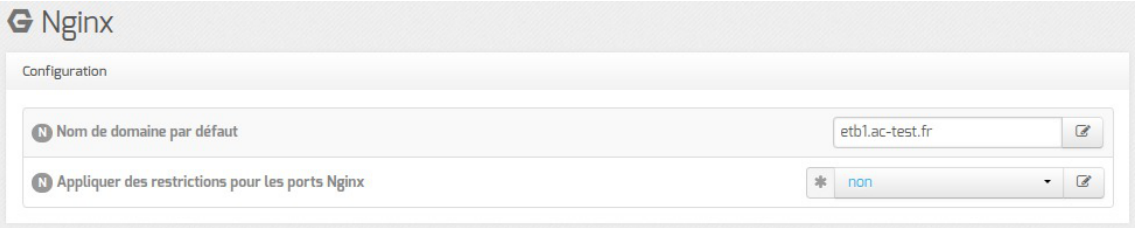
> Configurer la découverte automatique du proxy avec WPAD [p.348]

3.21. Onglet Nginx

L'onglet `Nginx` est disponible si au moins l'un des deux paramètres suivants est activé dans l'onglet `Services` :

- `Activer la publication d'applications web par Nginx` ;
- `Activer le reverse proxy Nginx`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Nom de domaine par défaut

En mode normal, cet onglet permet de saisir le `Nom de domaine par défaut` vers lequel sera redirigé un client qui accède au serveur avec un nom de domaine non déclaré.

Restriction Nginx

À partir d'EOLE 2.8.1, la variable : `Appliquer des restrictions pour les ports Nginx` permet de restreindre l'accès aux ports ouverts pour Nginx aux adresses autorisées à administrer le serveur.

> Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans le bloc `Administration à distance` de l'onglet `Interface-0`.

3.22. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.722].

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.709] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.731].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables*[p.716]*/DNAT*.

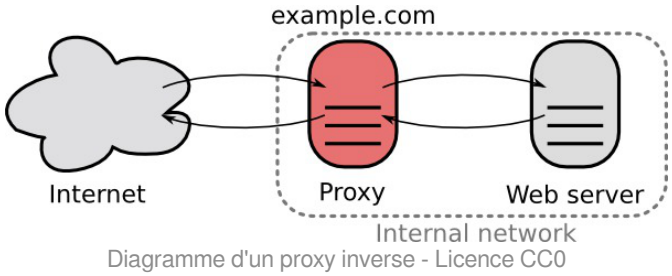
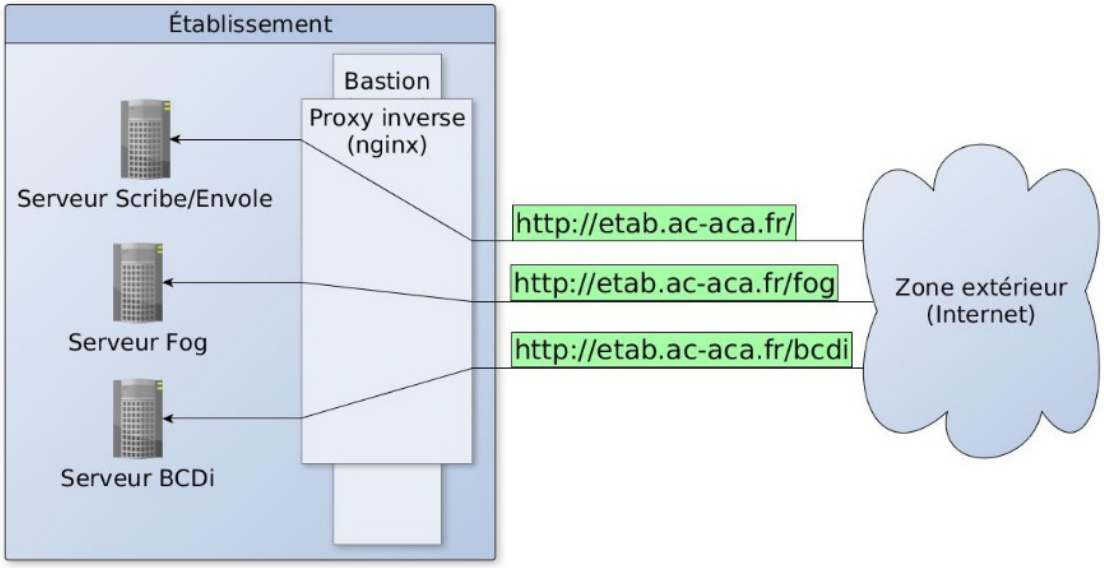


Diagramme d'un proxy inverse - Licence CC0

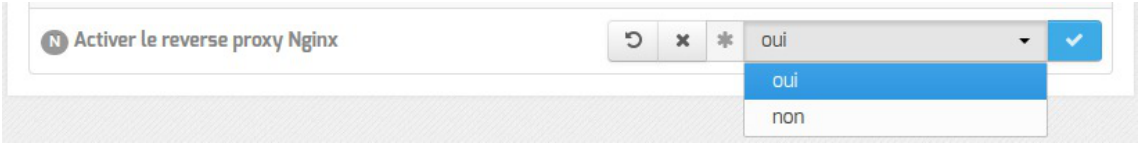
Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD[p.710] ;
- application EOP ;
- protocole HTTP[p.714] ;
- protocole HTTPS[p.714].

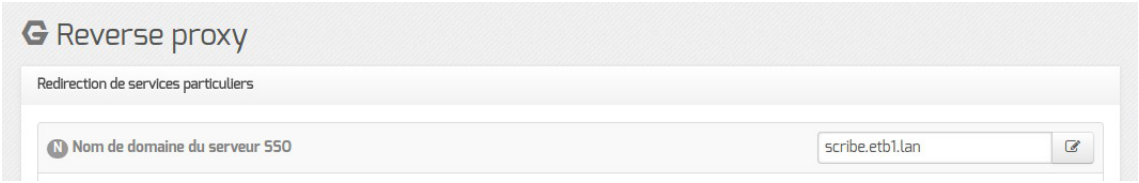
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

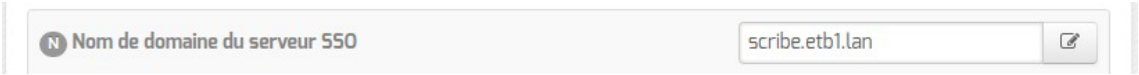


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

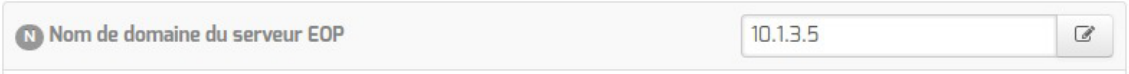
Redirection du service EoleSSO



Pour rediriger le service EoleSSO (port 8443), il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

Cette fonctionnalité n'est disponible que dans le cas ou le serveur EoleSSO n'est pas activé en local (`Utiliser un serveur EoleSSO` doit être différent de `local` dans l'onglet `Services`).

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.734]).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour rediriger l'application EOP, il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

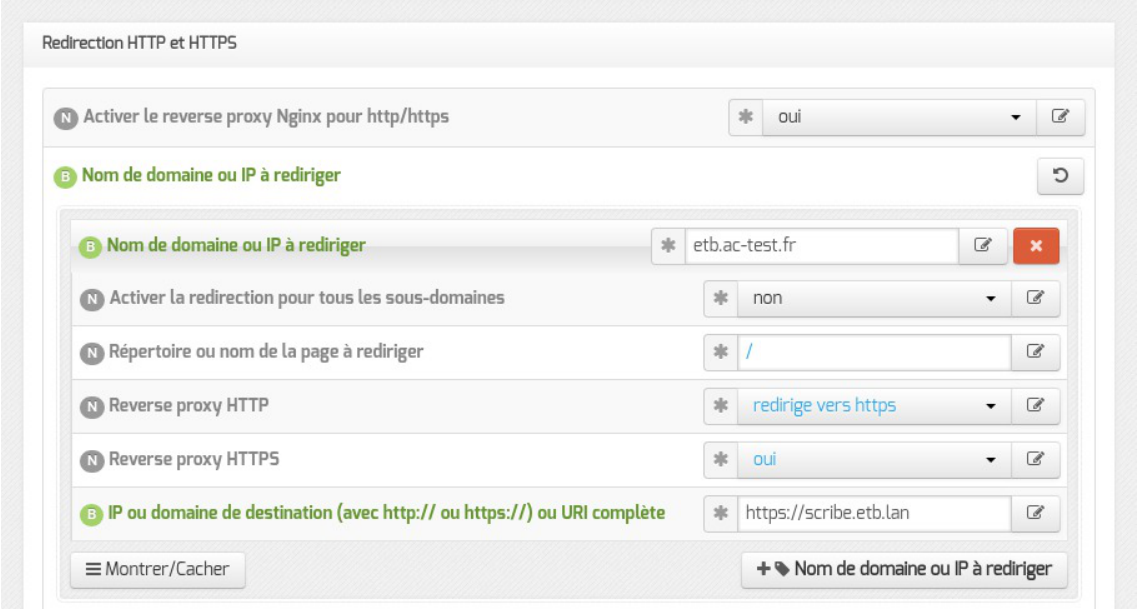
Redirection de l'interface d'administration EAD



Pour accéder de manière sécurisée à l'EAD d'un serveur depuis l'extérieur de l'établissement, il est recommandé :

- d'activer l'interface web de l'EAD du serveur interne sur un second port (4203 par défaut) dans l'onglet expert `Ead-web` de ce module ;
- d'activer la redirection sur le serveur faisant office de reverse proxy en configurant l'adresse IP ou le nom de domaine interne de la machine de destination et son port d'écoute.

Redirection HTTP et HTTPS



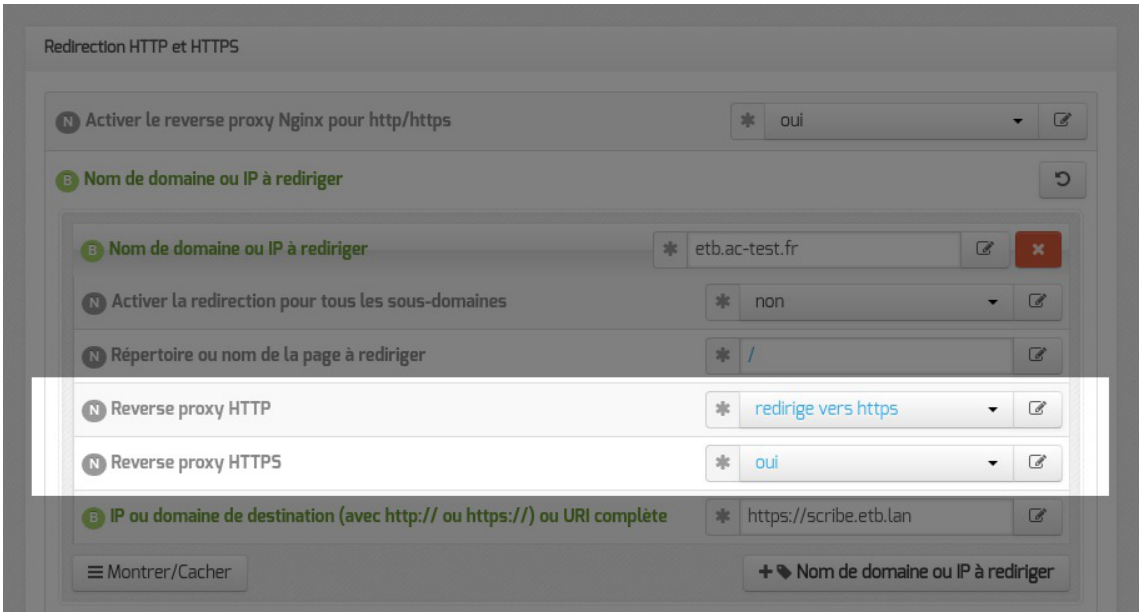
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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 ;
- `Activer la redirection pour tous les sous-domaines` : cette variable est disponible à partir de la version 2.6.2 d'EOLE, elle permet la prise en charge de tous les sous-domaines par le proxy inverse ;
- `Demander un certificat à Let's Encrypt pour ce domaine` ? : cette variable est disponible à partir de la version 2.6.2 d'EOLE si la redirection pour tous les sous-domaines n'est pas activé et que le certificat SSL est Let's Encrypt ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.734] (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.).

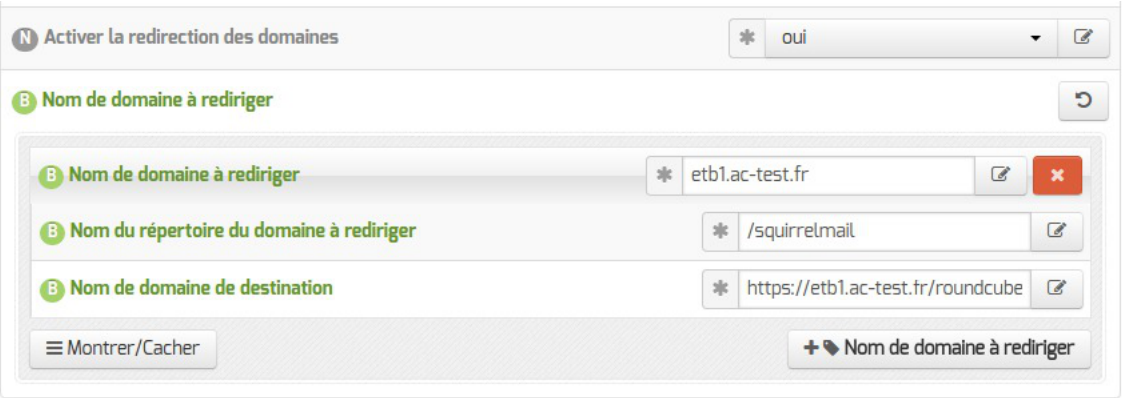
Le proxy inverse peut être utilisé pour ne rediriger que le HTTPS en passant les valeurs `Reverse proxy HTTP` à `non` et `Reverse proxy HTTPS` à `oui`.

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.727], `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).

Redirection de domaines

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



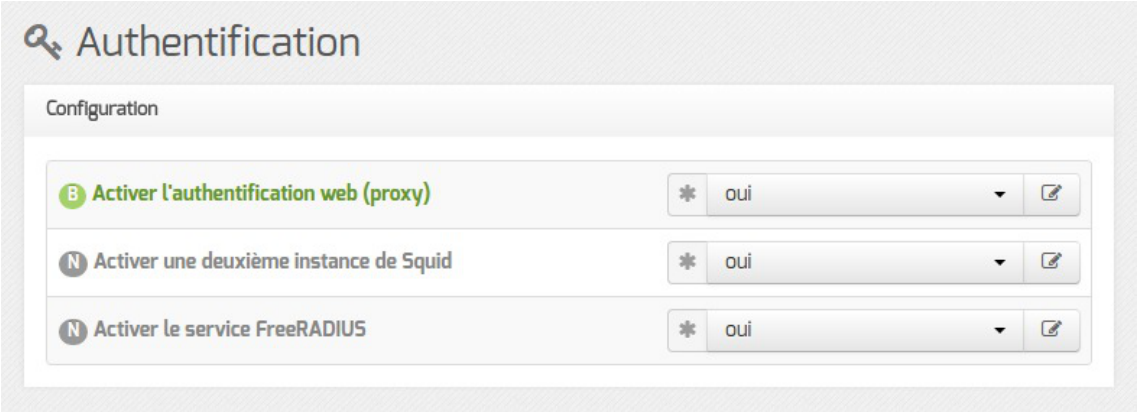
Le reverse proxy permet de rediriger automatiquement les utilisateurs voulant accéder à une page particulière vers une autre page.

L'exemple ci-dessus illustre le remplacement de SquirrelMail par Roundcube : si l'utilisateur cherche à accéder à l'adresse `http://etb1.ac-test.fr/squirrelmail/`, la page se recharge automatiquement avec l'URL de la nouvelle messagerie : `http://etb1.ac-test.fr/roundcube/`.

3.23. Onglet Freeradius : Configuration de l'authentification Radius

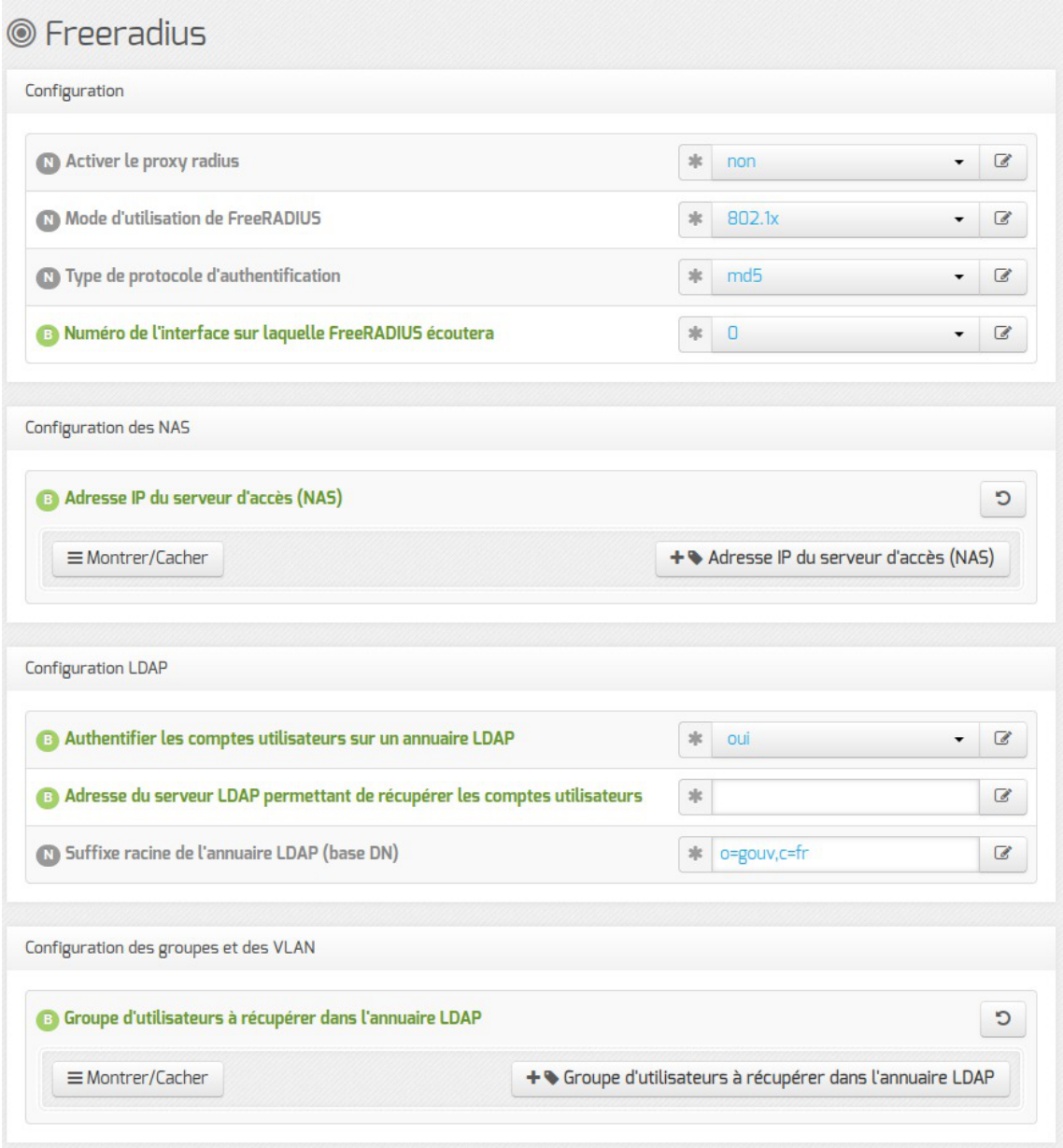
EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.728].

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`.

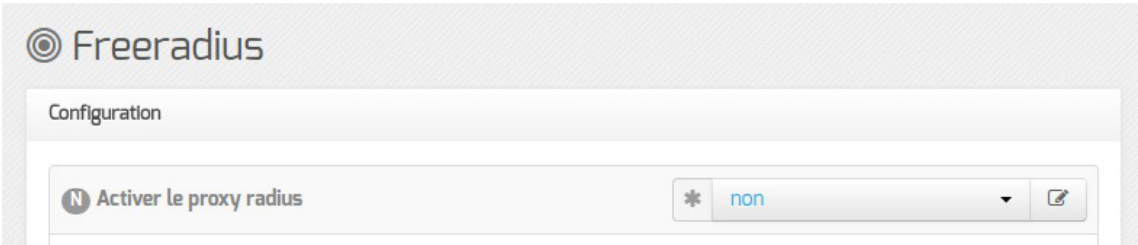
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Proxy RADIUS

L'activation du proxy RADIUS permet de relayer les requêtes d'authentification vers un autre serveur RADIUS.

Le paramétrage fin du serveur proxy RADIUS n'est pas implémenté. La configuration est celle proposée par défaut dans le logiciel.



Certains serveurs NAS[p.721] nécessitent un serveur proxy RADIUS pour le bon

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> fonctionnement de l'authentification.

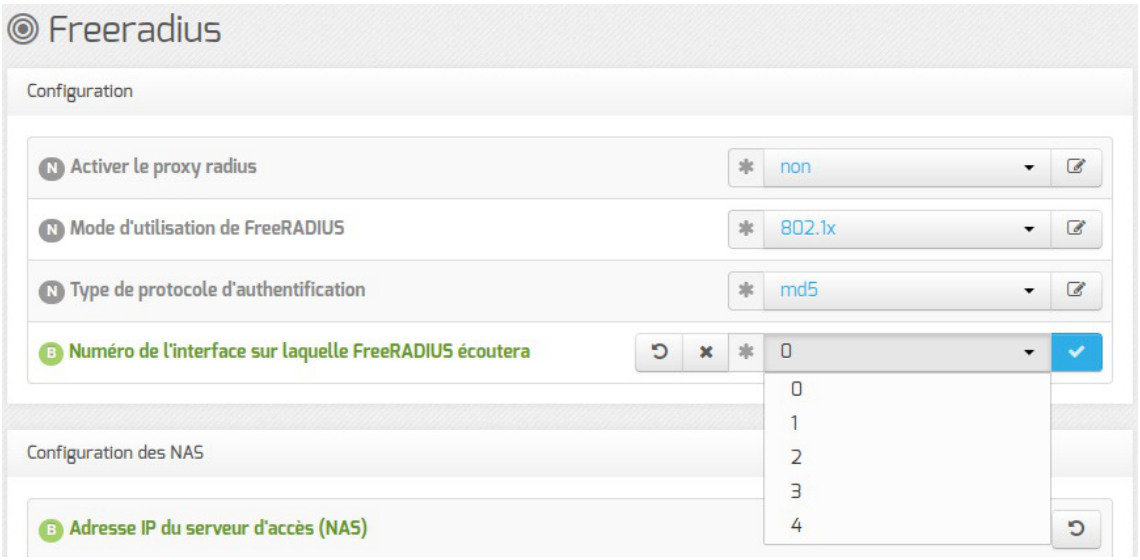
Modes de fonctionnement

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

- 802.1x ;
- accounting.

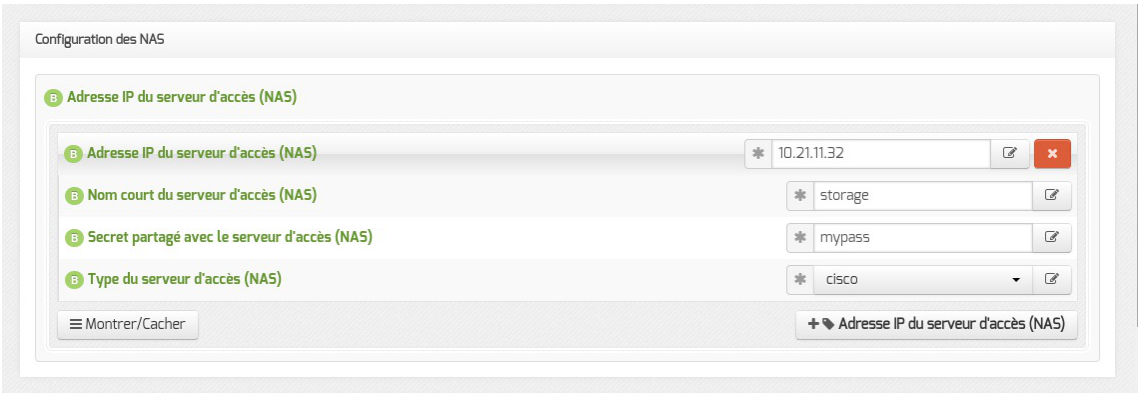
Le mode 802.1x

Le mode `802.1x` permet de marquer dynamiquement des ports d'un switch (NAS[p.722]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



`Numéro de l'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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Configuration LDAP

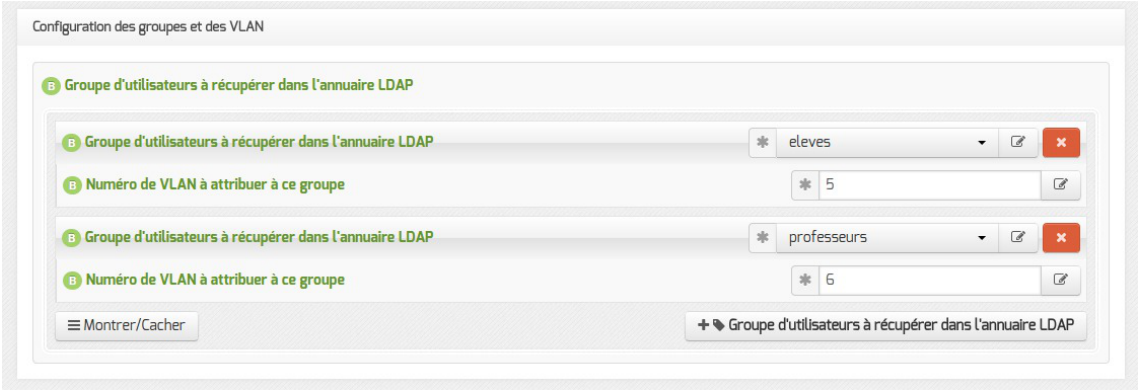


`Authentifier les comptes utilisateurs sur un annuaire LDAP` : L'authentification LDAP permet de s'assurer que l'utilisateur est autorisé à accéder aux réseaux. Mais si on gère une flotte de machine, l'authentification par clé TLS peut être jugée comme suffisante. Pour désactiver l'authentification LDAP, sélectionner `non`.

`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 marqué avec ce numéro de VLAN.

Le mode accounting

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



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.706]) 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



`Authentifier les comptes utilisateurs sur un annuaire LDAP` : L'authentification LDAP permet de s'assurer que l'utilisateur est autorisé à accéder aux réseaux. Mais si on gère une flotte de machine, l'authentification par clé TLS peut être jugée comme suffisante. Pour désactiver l'authentification LDAP, sélectionner `non`.

`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.



Pour tester la connexion à Freeradius en mode accounting il est possible d'utiliser la commande `radtest` :

```
root@amon:~# radtest -x admin <mdp admin> <Adresse IP sur laquelle
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
FreeRADIUS écoute> <port d'écoute du NAS> <Secret partagé avec le serveur d'accès>
```

ou encore

```
root@amon:~# radtest -x admin <mdp admin> $(CreoleGet "freerad_listen_addr") <port d'écoute du NAS> $(CreoleGet "freerad_nas_passwd")
```

Les journaux systèmes sont disponibles dans `/var/log/rsyslog/local/freeradius/` :

```
root@amon:/usr/share/eole/creole# tail -f /var/log/rsyslog/local/freeradius/freeradius.notice.log
2017-06-09T16:49:36.420151+02:00 amon.etb1.lan freeradius[32240]: Login OK: [admin] (from client other port 10)
2017-06-09T16:49:57.807213+02:00 amon.etb1.lan freeradius[32240]: Login OK: [admin] (from client other port 10)
```

Choix du protocole d'authentification

FreeRADIUS supporte plusieurs versions du protocole EAP (Extensible Authentication Protocol) :
https://wiki.freeradius.org/protocol/EAP

MD5

La version historique et la plus basique est la version MD5[p.720].

Le client est authentifié par le serveur qui utilise une authentification défi réponse. Une valeur aléatoire constituant le défi est envoyée au client, qui concatène à ce défi le mot de passe et en calcule, en utilisant l'algorithme MD5, le hash, une empreinte qu'il renvoie au serveur. Le serveur calcule sa propre empreinte connaissant le mot de passe, puis il compare les deux et valide ou non l'authentification.

La sécurité de cette version est faible. En cas d'écoute du trafic, il est possible de retrouver le mot de passe via force brute.

EAP-TLS

La version EAP-TLS[p.733] permet d'avoir un trafic chiffré entre le client et le serveur mais permet aussi, d'identifier le certificat présent sur le poste client.

Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement, dans un fonctionnement similaire au protocole https.

Pour activer EAP-TLS, sélectionner `tls` dans la variable `Type de protocole d'authentification`.



Version TLS

La version TLS 1.1 est désactivée au profit de la version 1.2 !

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

MD5

Ce mode n'est plus considéré comme sécurisé et ne permet pas d'identifier le poste.

3.24. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (Mode Normal)

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les serveurs EOLE.

Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur certains des modules.

Installation de LemonLDAP::NG

Installation sur Scribe, AmonEcole ou Seth Éducation

Pour activer le serveur LemonLDAP::NG[p.717] sur les modules Scribe, AmonEcole ou Seth Éducation, il faut installer le paquet **eole-lemonldap-ng-auto**.

```
apt install eole-lemonldap-ng-auto
```

Le service sera alors pré-configuré pour utiliser l'annuaire du module.

Installation sur les autres modules

Pour activer le serveur LemonLDAP::NG sur les autres modules EOLE (Eolebase par exemple), il faut installer le paquet **eole-lemonldap-ng**.

```
apt install eole-lemonldap-ng
```

Les sources d'authentification seront à saisir dans l'interface de configuration du module.

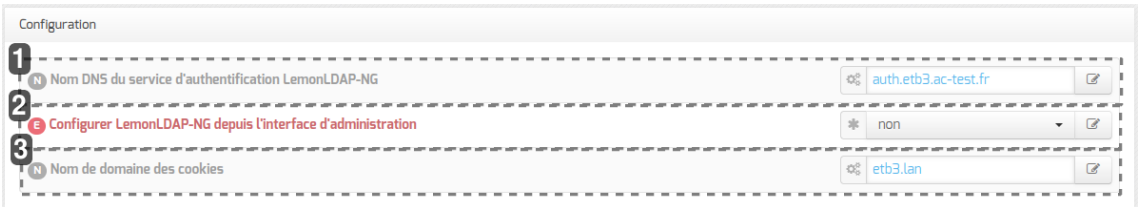
Module Seth

L'installation du paquet eole-lemonldap-ng-auto sur un module Seth transformera ce dernier en Seth Éducation !

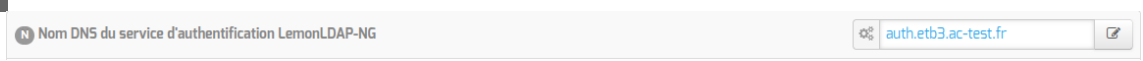
LemonLDAP vs EoleSSO

L'installation des paquets eole-lemonldap-ng et/ou eole-lemonldap-ng-auto entraîne la désinstallation du paquet **eole-sso-server** par le jeu des dépendances de paquets (dpkg[p.704]).

Partie Configuration



1



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nom DNS du service d'authentification LemonLDAP-NG

Variable calculée.

Nom interne de la variable

authWebName

2



Configurer LemonLDAP-NG depuis l'interface d'administration

Permet d'activer l'interface d'administration fournie par le projet LemonLDAP::NG.

Par défaut, cette interface est désactivée, les cas classiques de configuration étant pris en charge via les mécanismes EOLE.

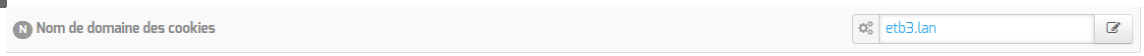
Conflit des modes de configuration

La configuration de LemonLDAP::NG depuis son interface d'administration écrase et remplace celle générée via les mécanismes EOLE.

Nom interne de la variable

ll_activer_manager

3



Nom de domaine des cookies

Cette variable est pré-remplie.

Nom interne de la variable

cookieDomain

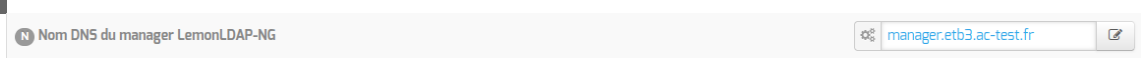
La variable `Nom DNS du service d'authentification LemonLDAP-NG` doit être renseignée avec le nom DNS du serveur précédé du nom du service.

La variable `Configurer LemonLDAP-NG depuis l'interface d'administration` permet d'activer l'interface d'administration de LemonLDAP::NG.

Si la variable est à oui une nouvelle variable apparaît en mode Normal et deux en mode Expert.



1



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nom DNS du manager LemonLDAP-NG

Indique le nom de domaine avec lequel le manager de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

managerWebName

2



Nom DNS du service Reload LemonLDAP-NG

Indique le nom de domaine avec lequel le service de rechargement de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

reloadWebName

Si vous activez l'interface d'administration de LemonLDAP::NG vous perdrez la possibilité d'utiliser les outils EOLE pour interagir avec LemonLDAP::NG.

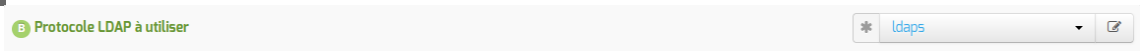
À ne choisir que si vous savez ce que vous faites !

Partie Configuration LDAP

Dans cette partie vous avez accès aux paramètres propres à LemonLDAP::NG.



1



Protocole LDAP à utiliser

Il est possible d'adapter le protocole à utiliser selon les capacités du serveur LDAP associé. Le choix se fait entre **ldaps** et **ldap**.

Nom interne de la variable

ldapScheme

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2



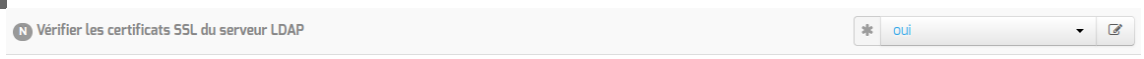
Port d'écoute du LDAP utilisé par LemonLDAP::NG

Port utilisé pour contacter l'annuaire.

Nom interne de la variable

ldapServerPort

3



Vérifier les certificats SSL du serveur LDAP

Active ou désactive la vérification du certificat SSL fourni par l'annuaire dans le cas du protocole LDAPS

Nom interne de la variable

lmldapverify

4



Nombre de processus dédié à Lemon (équivalent au nombre de processeurs)

Permet de limiter les ressources allouées

★

Il est conseillé de ne pas allouer la totalité des files de traitement pour éviter de bloquer le système complètement en cas de charge excessive.

Nom interne de la variable

lemonproc

La variable `Protocole LDAP à utiliser` permet de choisir entre `LDAP` et `LDAPS`.

Le serveur LemonLDAP::NG prend en charge LDAP over SSL (LDAPS). La fonction Strict SSL est définie par défaut. La fonction Strict SSL nécessite une certification de serveur.

Pour des interactions en LDAP avec Active Directory, prendre en compte que certaines actions nécessitent l'utilisation de LDAPS (LDAP sur SSL) entre le client et Active Directory

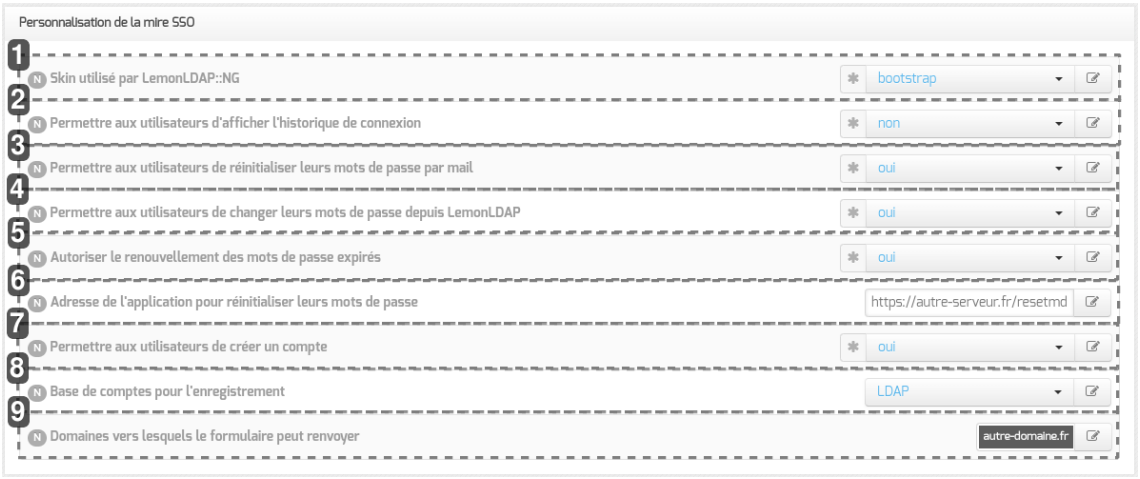
La variable `Port d'écoute du LDAP utilisé par LemonLDAP::NG` permet de changer le port associé au LDAP. Par défaut il s'agit du port `636`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

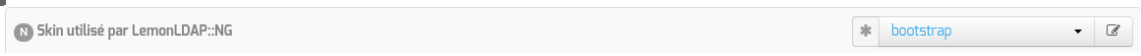
La variable `Vérifier les certificats SSL du serveur LDAP` permet de valider les certificats SSL pour l'authentification du serveur LemonLDAP::NG.

La variable `Nombre de processus dédié à Lemon (équivalent au nombre de processeurs)` indique le nombre de processus utilisé par LemonLDAP::NG. Par défaut cette variable est à 4, néanmoins il est préférable d'avoir ce nombre légèrement inférieur au nombre de processeurs.

Partie Personnalisation de la mire SSO



1



Skin utilisé par LemonLDAP::NG

Sélectionne l'aspect visuel de la mire d'authentification parmi les thèmes proposés par l'application LemonLDAP::NG :

- bootstrap
- dark
- impact
- pastel

Nom interne de la variable

llSkin

2



Permettre aux utilisateurs d'afficher l'historique de connexion

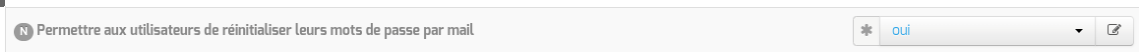
Active l'affichage de son historique de connexion pour chaque utilisateur.

Nom interne de la variable

llCheckLogins

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

3



Permettre aux utilisateurs de réinitialiser leurs mots de passe par mail

Active la fonctionnalité de réinitialisation autonome de mot de passe en cas de perte.

Nom interne de la variable

llResetPassword

4



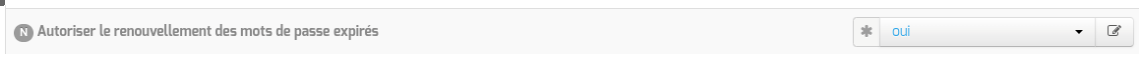
Permettre aux utilisateurs de changer leurs mots de passe depuis LemonLDAP

Active le formulaire de changement de mot de passe.

Nom interne de la variable

llChangePassword

5



Autoriser le renouvellement des mots de passe expirés

Permet le renouvellement du mot de passe depuis la mire dans le cas d'une expiration.

Nom interne de la variable

llResetExpiredPassword

6



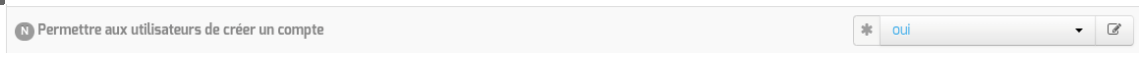
Adresse de l'application pour réinitialiser leurs mots de passe

Adresse du formulaire à présenter aux utilisateurs pour leur permettre de réinitialiser leur mot de passe

Nom interne de la variable

llResetUrl

7



Permettre aux utilisateurs de créer un compte

Donne le droit aux utilisateurs de créer un compte.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nom interne de la variable

> llRegisterAccount

8



Base de comptes pour l'enregistrement

Type de base pour l'enregistrement des comptes créés parmi les choix suivants :

- LDAP
- AD
- Demo
- Custom

Nom interne de la variable

> llRegisterDB

9



Domaines vers lesquels le formulaire peut renvoyer

Liste des domaines autorisés depuis le formulaire.

Nom interne de la variable

> llCSPTargets

La variable `Skin utilisé par LemonLDAP:`:NG permet de choisir le skin utilisé par LemonLDAP::NG.

La variable `Permettre aux utilisateurs d'afficher l'historique de connexion` permet aux utilisateurs lorsqu'elle est à `oui`, d'afficher leur historique de connexion.

La variable `Permettre aux utilisateurs de réinitialiser leurs mots de passe par mail` met en place la possibilité pour les utilisateurs de modifier leurs mots de passe depuis la fenêtre de connexion. La méthode consiste à demander la confirmation de l'adresse mail de l'utilisateur, si celle-ci correspond il recevra un mail avec un lien pour changer son mot de passe.

La variable `Permettre aux utilisateurs de changer leurs mots de passe depuis LemonLDAP` permet aux utilisateurs de changer librement leur mot de passe depuis la page de gestion LemonLDAP::NG correspondant par défaut à la variable `Nom DNS du service d'authentification LemonLDAP-NG` ou variable Creole `authWebName`

La variable `Autoriser le renouvellement des mots de passe expirés` autorise le

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

renouvellement par l'utilisateur.

Dans ce cas il est possible avec la variable `Adresse de l'application pour réinitialiser leurs mots de passe` d'indiquer une application ou un service spécifique (compatible LDAP, LDAPS, et LemonLDAP::NG) pour cette opération.

La variable `Permettre aux utilisateurs de créer un compte` autorise les utilisateurs à créer des comptes supplémentaires en lieu et place de l'administrateur, depuis l'interface LemonLDAP::NG.

La Variable `Base de comptes pour l'enregistrement` vous permet de choisir le type de base que vous voulez parmi 4 possibilités :

- Une base LDAP
- Une base AD
- Une base de démonstration
- Une base personnalisable.

Si vous choisissez une base personnalisable une nouvelle variable apparaîtra. `Adresse de l'application de création de compte` qu'il faut remplir en indiquant le service ou l'application qui va remplir la base.



Indiquer l'adresse de l'application de création de compte alternative. (https://.....)

Nom interne de la variable

llRegisterURL

La variable `Domaines vers lesquels le formulaire peut renvoyer`, concerne tous services ou applications externes au domaine du serveur LemonLDAP::NG vers lesquels il doit cependant pouvoir, soit donner accès, soit interagir.

Documentation annexe

Site officiel : LemonLDAP::NG [https://lemonldap-ng.org/]

Documentation officielle (en anglais) : Documentation [https://lemonldap-ng.org/documentation/latest/]

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

- `Général` ;
- `Services` ;
- `Firewall` ;
- `Système` ;
- `Sshd` ;
- `Ntp` ;
- `Logs` * ;
- `Interface-0` (configuration de l'interface réseau) ;
- `Interface-1` (configuration de l'interface réseau) ;
- `Réseau avancé` ;
- `Certificat ssl` ;
- `Dépôt tiers` ;
- `Schedule` ;
- `Agrégation` * ;
- `Clamav` * ;
- `Relai dhcp` * ;
- `Onduleur` * ;
- `Ead3` * ;
- `Saltstack` * ;
- `Rvp` * ;
- `Eole sso` * ;
- `Zone-dns` ;
- `Ead-web` ;
- `Mode restreint` ;
- `Messagerie` ;
- `Authentification` ;
- `Filtrage web` ;
- `Squid` ;
- `Squid2` *;
- `Proxy authentifié` ;
- `Proxy authentifié 2` *;
- `Exceptions proxy` ;
- `Proxy parent` ;
- `Wpad` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- Nginx ;
- Applications web nginx *;
- Reverse proxy * ;
- Freeradius *;
- Eoleflask.
- Lemonldap.

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

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.

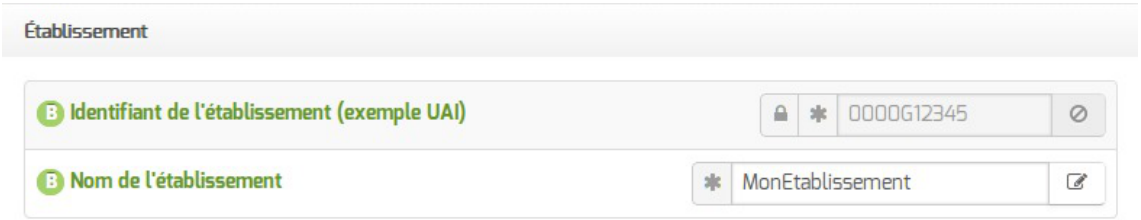
Le nombre d'interfaces doit, bien évidemment, être choisi en fonction du nombre de cartes réseau physiques du serveur mais plus encore en fonction du nombre de sous-réseaux souhaités.

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



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, ...

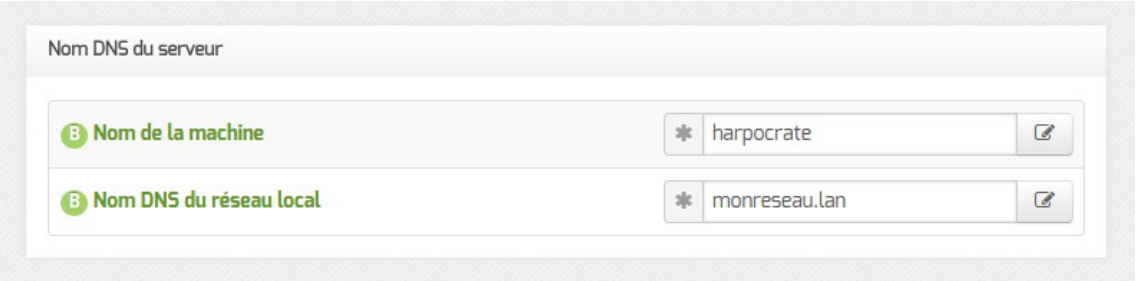
Sur les modules fournissant un annuaire LDAP[p.717] local, ces variables sont utilisées pour créer l'arborescence.



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

Nom DNS du serveur

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



En premier lieu, il convient de configurer le nom DNS du serveur.

Cette information est découpée en 2 champs :

- le nom de la machine dans l'établissement ;
- le nom DNS du réseau local.

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

Si l'authentification NTLM/KERBEROS est activée sur le proxy, le `Nom de machine` ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.

Le `Nom DNS du serveur` utilise fréquemment des domaines de premier niveau du type `.lan` .

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.

Rappel : les outils mDNS (Avahi, Bonjour, ...) utilise la racine '.local'. Pour éviter les problèmes de DNS, nous vous déconseillons d'utiliser cette racine.

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

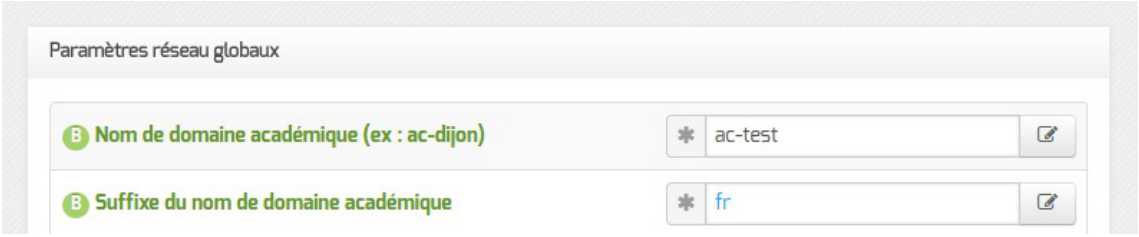
Sur un réseau local les noms de domaine sont privés et on peut tout à fait utiliser des domaines de premier niveau, et leur donner la sémantique que l'on veut.

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.

Paramètres réseau globaux

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

Cette information est découpée en plusieurs champs :

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

Nombre d'interfaces

Un module Amon ou AmonEcole 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.



La déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module qui serait protégé par un module Amon.

Déchiffrement et interception du protocole HTTPS

Par rapport au protocole HTTP[p.714], le protocole HTTPS permet de chiffrer la communication entre le navigateur du poste client et le serveur du site distant.

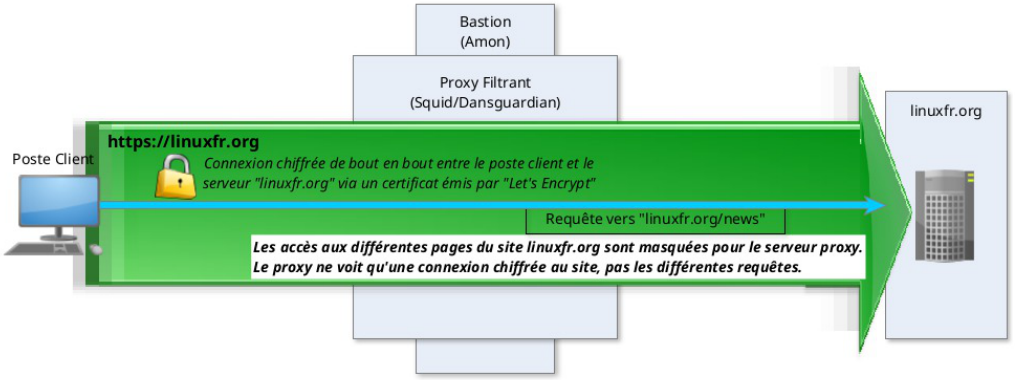
Dans ce cas, le serveur proxy ne journalise qu'une seule connexion vers le site distant (exemple : https://pcll.ac-dijon.fr) mais pas les différentes requêtes d'accès aux pages ou aux fichiers se trouvant

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

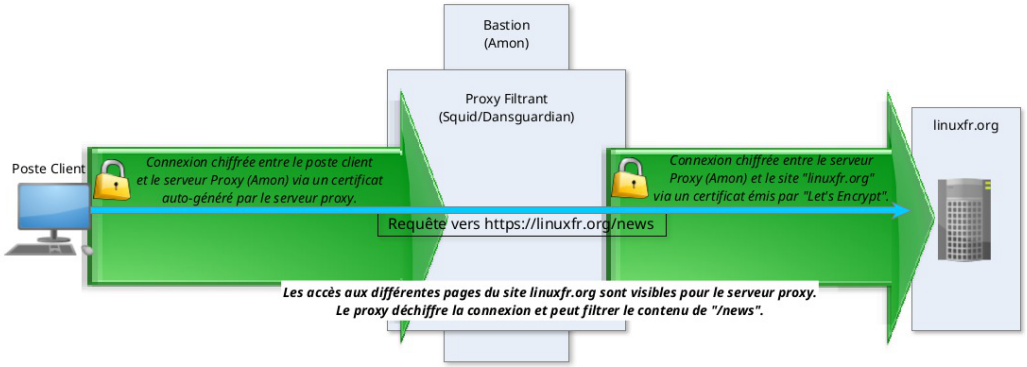
sur ce serveur (exemple : https://pcll.ac-dijon.fr/eole/).

En HTTPS, le serveur Proxy ne peut pas filtrer le contenu des pages consultées ni scanner les fichiers téléchargés avec un antivirus.

Le déchiffrement HTTPS sur le serveur Proxy permet d'intercepter l'ensemble des requêtes et de les journaliser, de filtrer le contenu des pages visitées et de scanner les fichiers téléchargés.



Fonctionnement HTTPS normal



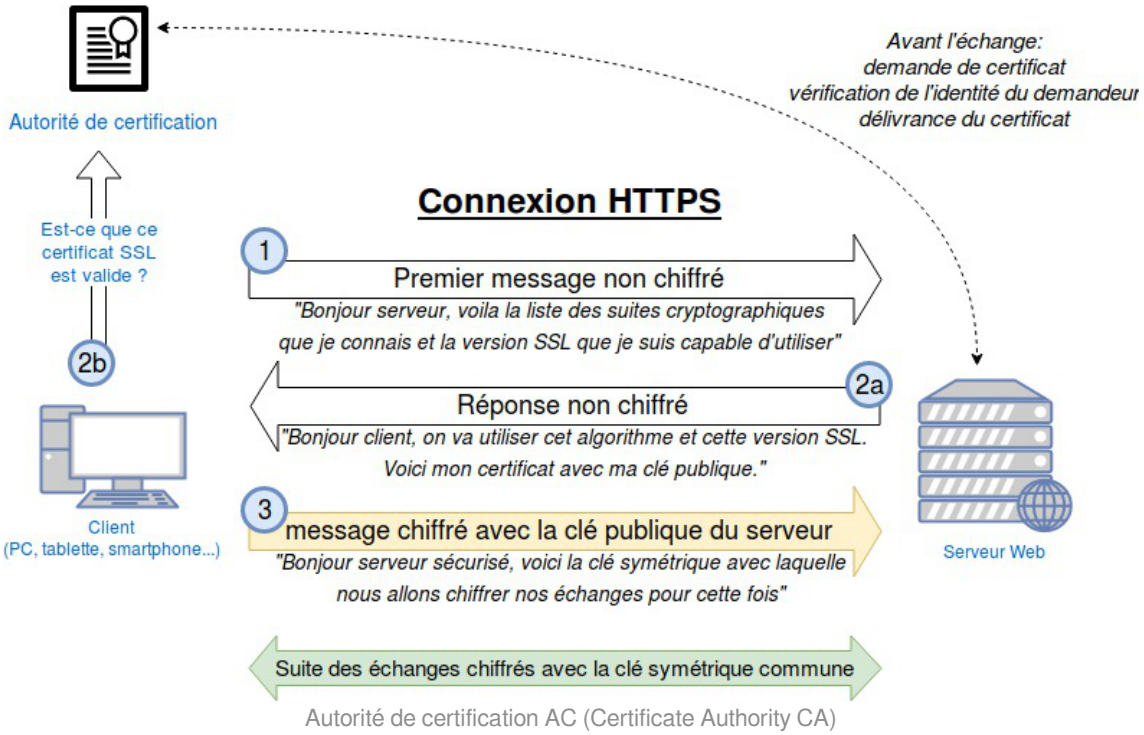
Fonctionnement HTTPS déchiffré par le Proxy

Certificat Racine de l'autorité de certification

Un certificat HTTPS est émis par une autorité de certification[p.704].

Let's Encrypt[p.717], par exemple, est une autorité de certification publique et connue des navigateurs ; son certificat racine est pré-installé dans les navigateurs et les systèmes d'exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



À partir de la version 2.8.1, le module Amon est équipé d'une fonctionnalité d'interception du trafic HTTPS. Il est possible de déclarer son certificat racine servant à sur-signer les ressources servies par le protocole HTTPS et transitant par le proxy filtrant. Cette déclaration permet d'en automatiser l'intégration dans le magasin de certificats local.

Si la variable `Utiliser un serveur mandataire (proxy) pour accéder à Internet` est passée à `oui`, la variable `Le serveur mandataire intercepte les communications HTTPS` est proposée et permet elle-même de faire apparaître deux variables permettant d'identifier le certificat racine employé par le proxy filtrant.



En passant la variable `Le serveur mandataire intercepte les communications HTTPS` à `oui`, il est possible de renseigner les variables suivantes en utilisant les données affichées par la commande `diagnose` sur le module Amon :

- `Type d'empreinte du certificat racine du proxy` : SHA256 (par défaut sur Amon 2.8.1)
- `Empreinte du certificat racine du proxy` : information donnée par le diagnose du serveur Amon dans le cas où celui-ci fait office de proxy filtrant

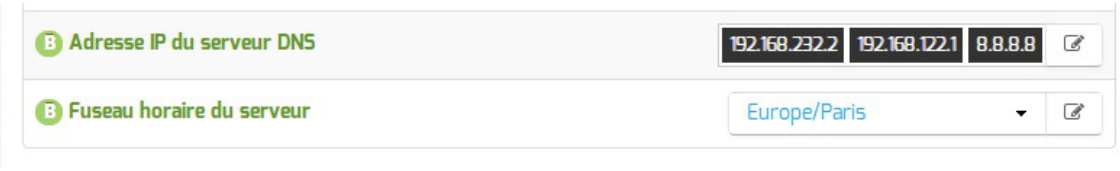
Cette configuration est nécessaire uniquement lorsque le module Amon est configuré pour l'interception des communications HTTPS.

Sur un module Amon configuré pour l'interception des communications HTTPS, la commande `diagnose` permet de connaître le chemin et l'empreinte du certificat :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
*** Validité du certificat racine du proxy (/etc/eole/squid_CA.crt)
.                signingCA.crt => Ok
.                    Empreinte => SHA256 Fingerprint=62
:1B:BF:25:28:44:31:02:7E:09:31:A6:EA:FD:A5:A8:7C:D4:EB:B6:3D:83:88:62:0F:98:85:

```

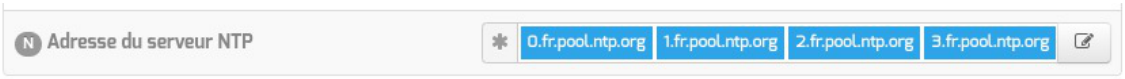
DNS et fuseau horaire



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.709].

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

NTP



Une liste de serveurs de temps (NTP[p.723]) à utiliser est proposée par défaut.

Il est possible de modifier ces valeurs afin d'utiliser un serveur de temps personnalisé.

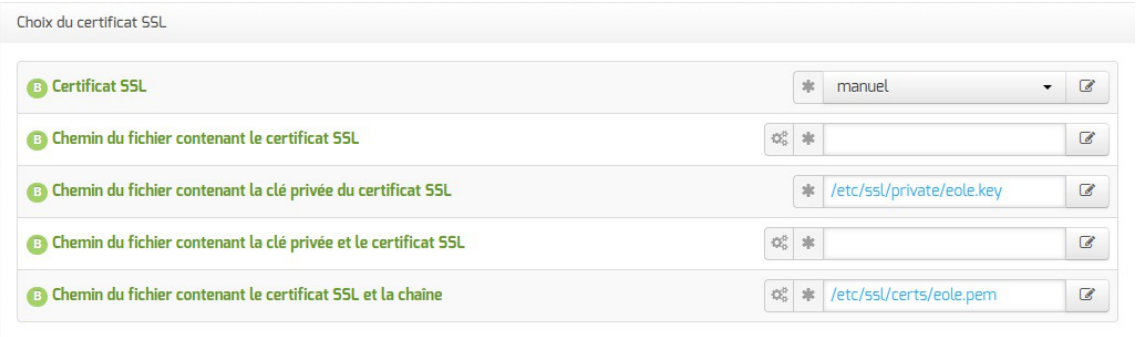
Ports utilisés par ntpdate

Le service `ntp` utilisant et bloquant le port 123, `ntpdate` utilise un port source aléatoire dans la plage des ports non privilégiés.

Les éventuelles règles de pare-feu ne peuvent donc pas présumer que le port source est le port 123.

Par contre, le port de destination reste inchangé (port : 123).

Choix du certificat SSL



Trois types de certificats peuvent être utilisés pour sécuriser les connexions avec TLS[p.733] :

- `autosigné` : le certificat est généré localement et signé par une CA[p.704] locale ;
- `letsencrypt` : le certificat est généré et signé par l'autorité Let's Encrypt[p.717] ;
- `manuel` : le certificat est mis en place manuellement par l'administrateur. Pour ce faire, il faut

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

disposer au préalable des certificats fournis par l'autorité de certification, si ce n'est pas encore le cas, le choix `autosigné` permet d'utiliser le serveur de façon non optimale. Le répertoire `/etc/ssl/certs/` est recommandé pour placer les certificats.

Le système de certificat utilisé repose sur une clé privée et une clé publique (le certificat) contre-signée par une autorité de certification.

Selon le contexte d'utilisation, les différents éléments de la chaîne de certification (clé privée, certificats du service ou de l'autorité de certification) doivent être combinés selon différents modes.

En mode `letsencrypt` et `autosigné`, le détail de ces combinaisons est automatique et caché.

En mode `manuel`, les variables suivantes permettent d'identifier l'emplacement des fichiers contenant les différentes combinaisons de fichiers utiles :

- `Chemin du fichier contenant le certificat SSL` : emplacement du fichier contenant uniquement le certificat ;
- `Chemin du fichier contenant la clé privée du certificat SSL` : emplacement du fichier contenant uniquement la clé privée ;
- `Chemin du fichier contentant la clé privée et le certificat SSL` : emplacement du fichier contenant la concaténation du certificat SSL puis de la clé privée ;
- `Chemin du fichier contenant le certificat SSL et la chaîne` : emplacement du fichier contenant la concaténation du certificat SSL et des certificats intermédiaires formant la chaîne de certification à l'exclusion du certificat racine.

Par défaut, le type de certificat par défaut est `autosigné` et aucun paramétrage n'est nécessaire.

Cette configuration est déconseillée car elle nécessite l'installation de l'autorité de certification locale sur tous les postes clients.

Pour plus d'informations, consulter la partie consacrée à l'`onglet expert` `Certificats ssl` (cf. Onglet Certificats ssl : gestion des certificats SSL) [p.233].

Mise à jour

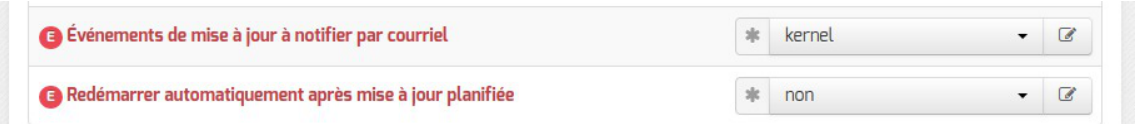


Il est possible de définir d'autres adresses pour le serveur de mise à jour EOLE que celles fournies par défaut, dans le cas où vous auriez, par exemple, un miroir des dépôts.



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

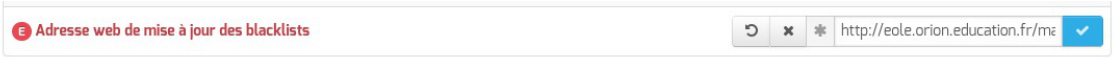
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



La variable `Événements de mise à jour à notifier par courriel` permet d'activer les notifications par courriel pour certains événements liés à la mise à jour :

- `aucun` : aucune notification ;
- `queryauto` : notification en cas de mise à jour disponible (nécessite l'activation de la tâche schedule *`queryauto`* dans l'onglet `Schedule`) ;
- `kernel` : notification en cas de redémarrage nécessaire suite à l'installation d'un nouveau noyau[p.718] ;
- `tous` : notification en cas de mise à jour disponible ou de redémarrage nécessaire.

La variable `Redémarrer automatiquement après mise à jour planifiée` permet de désactiver le redémarrage automatique du serveur qui intervient après sa reconfiguration lorsque la mise à jour planifiée a installé un nouveau noyau[p.718].



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.718]).

Voir aussi...

Onglet Interface-n [p.95]

Les différents types de mises à jour [p.449]

Sites : Bases de filtres optionnels [p.504]

4.2. Onglet Services

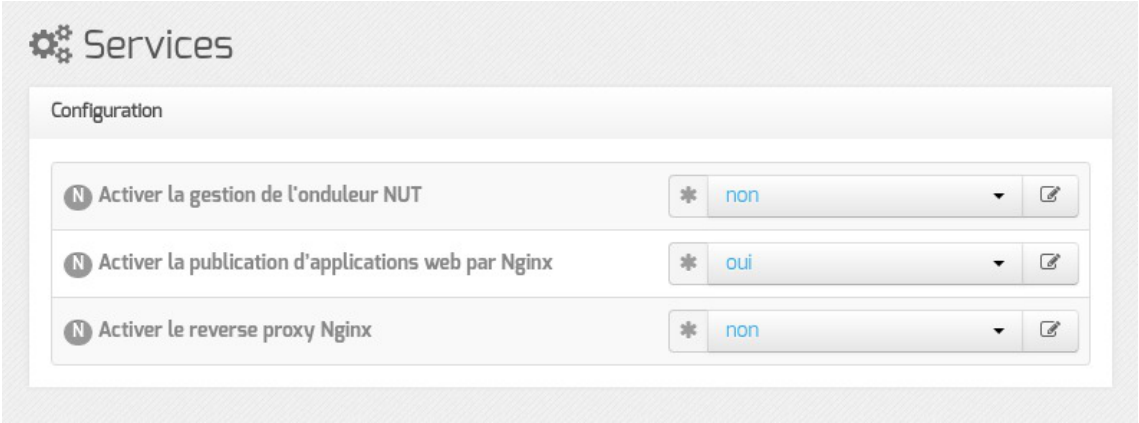
L'onglet `Services` permet d'activer et de désactiver une partie des services proposés par le module.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.723].

L'activation d'applications web par Nginx[p.722] et du proxy inverse sont également disponibles sur ce module.

Les autres services propres au module Amon en mode normal sont les suivants :

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

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

- la gestion des logs centralisés ;
- l'activation de l'interface web de l'EAD[p.710] ;
- l'activation de l'interface d'administration du module EAD3[p.710] ;
- l'activation de l'accès web à l'interface de configuration du module (`GenConfig`) sur le port 443.

Une fois le module instancié, l'accès web à l'interface de configuration du module est activé par défaut sur le port 443.

L'interface reste également accessible en https sur le port historique 7000.

Le seul service propre au module Amon en mode expert est le filtrage sur le proxy qui est activé par défaut.



Sa désactivation entraîne celle du logiciel e2guardian[p.710] et rend indisponibles de nombreuses fonctionnalités.

Voir aussi...

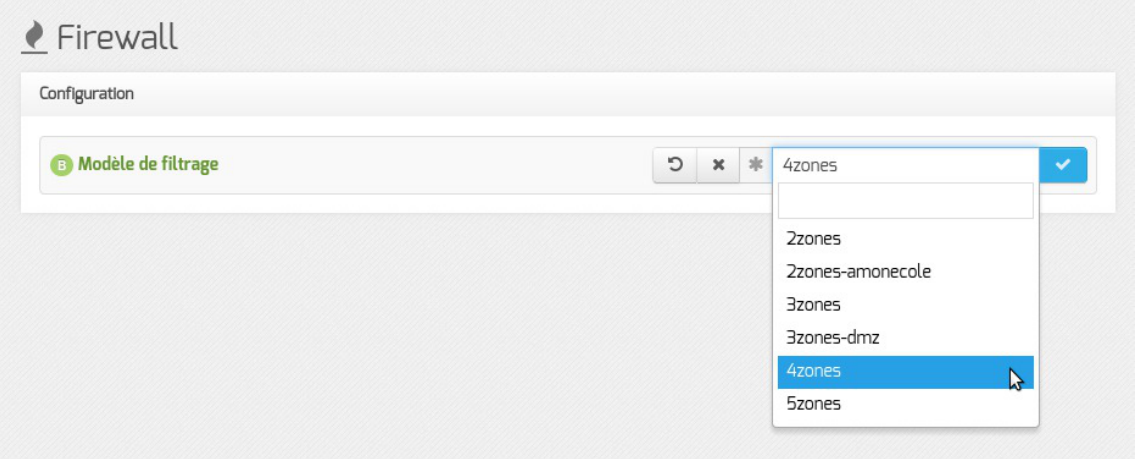
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Onglet Logs : Gestion des logs [p.205]

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 l'interface 1 ;
- **2zones-amonecole** : modèle spécifique au module AmonEcole (pedago sur l'interface 1) ;
- **3zones** : gestion d'une zone admin sur l'interface 1 et d'une zone pedago sur l'interface 2 ;
- **3zones-dmz** : gestion d'une zone pedago sur l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.

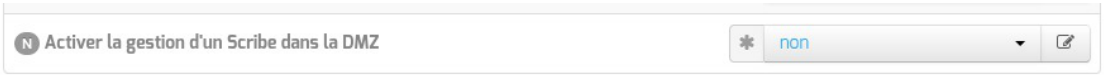
Chaque modèle de zone proposé correspond à un modèle de filtrage ERA. Les modèles de filtrage ERA sont la description de pare-feu enregistrés dans des fichiers XML situés par défaut dans le répertoire `/usr/share/era/modeles/`.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Déclaration d'un module Scribe en DMZ

La variable `Activer la gestion d'un Scribe dans la DMZ` permet la prise en charge par bastion[p.704] des règles propres à la DMZ[p.709].



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

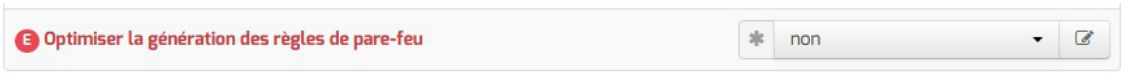
- un réseau administratif ;
- un réseau pédagogique ;
- une DMZ contenant un serveur Scribe hébergeant des services web à ouvrir depuis l'extérieur.

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).

Optimisation de la génération des règles

En mode expert, il est possible de désactiver la génération accélérée des règles de pare-feu en passant la variable `Optimiser la génération des règles de pare-feu` à `non`.



La génération des règles de pare-feu accélérée utilise le format `iptables-restore` en lieu et place d'une succession de commandes *`iptables`*.

Interdire des accès réseaux



Par défaut, l'accès à des réseaux extérieurs pour des réseaux autres que l'interface 1 (l'interface 1 étant généralement *admin*) n'est pas interdit.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Si on passe l'option `Interdire les interfaces autres que 1 à accéder à des réseaux extérieurs` à `oui`, il est possible d'interdire l'accès

pour la ou les adresse(s) réseau et le ou les masque(s) souhaités.

Pour les réseaux RVP, il est habituel de ne pas conserver les données téléchargées par les utilisateurs dans le cache du proxy. C'est pour cela que l'option `Désactiver le cache du proxy pour les accès à ce réseau` est à `oui` par défaut. Cela signifie qu'en cas de téléchargement de page web, d'image, ... ces informations seront automatiquement re-téléchargées depuis le site source plutôt que conservées dans le cache du proxy.

Enfin, l'option `En plus de l'interdiction proxy, interdire tous les protocole`s permet de bloquer, via des règles iptables tout accès à ces réseaux.

Voir aussi...

> Configuration du module Amon avec le module Scribe en DMZ [p.337]

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.

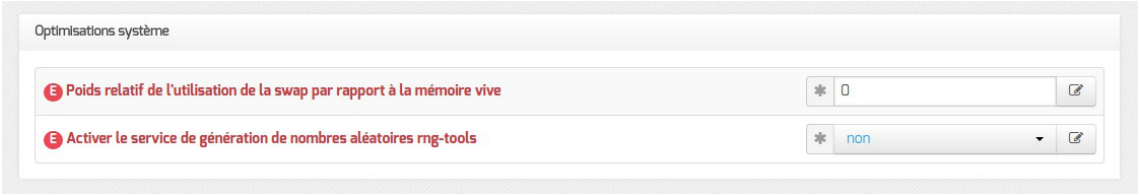
Paramétrage de la console



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `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.
- `Nuance du fond d'écran dans VIM` : l'éditeur VIM peut utiliser différents thèmes pour la coloration syntaxique et adapter ceux-ci en fonction de la valeur de la couleur d'arrière-plan pour en améliorer la lisibilité. La variable prend une valeur parmi dark et light, permettant d'adapter la coloration syntaxique à un arrière-plan sombre et clair respectivement.

Optimisations système



- `Poids relatif de l'utilisation de la swap par rapport à la mémoire vive` : Le swappiness est un paramètre du noyau Linux permettant de définir avec quelle sensibilité il va écrire dans la swap si la quantité de RAM à utiliser devient trop importante. Le système accepte des valeurs comprises entre 0 et 100. La valeur `0` empêchera au maximum le système d'utiliser la partition d'échange.



La commande suivante permet de connaître les réglages de swappiness appliqués :
`cat /proc/sys/vm/swappiness`

- `Activer le service de génération de nombres aléatoires rng-tools` : Le démon `rngd` agit comme une passerelle entre un vrai générateur de nombres aléatoires, matériel (TRNG), tel que ceux que l'on peut trouver dans les puces Intel/AMD/VIA et le pseudo-générateur de nombres aléatoires du noyau (PRNG).



Sur les serveurs virtualisés, le service `rngd` ne sera généralement pas fonctionnel et affichera, au démarrage, un message du type :
`erreur Starting Hardware RNG entropy gatherer daemon: (failed)`

Validation des mots de passe

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Un paramétrage par défaut est proposé mais il est possible d'adapter.

La complexité des mots de passe peut être réglée 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`.

La valeur 0 permet de désactiver une classe de caractères.

Pour obliger l'utilisation de 2 classes de caractères minimum et d'un minimum de 7 caractères :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 0
- `Taille minimum du mot de passe utilisant deux classes de caractères` : 7
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7
- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7

Pour obliger l'utilisation de 3 classes de caractères minimum et d'un minimum de 7 caractères :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 0
- `Taille minimum du mot de passe utilisant deux classes de caractères` : 0
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7



Il est impossible d'obliger l'utilisation de 3 classes minimum sans obliger l'utilisation de 2 classes minimum, exemple de valeur impossible :

- `Taille minimum du mot de passe utilisant une seule classe de caractères` : 7
- `Taille minimum du mot de passe utilisant deux classes de caractères` : 0
- `Taille minimum du mot de passe utilisant trois classes de caractères` : 7
- `Taille minimum du mot de passe utilisant quatre classes de caractères` : 7

Les valeurs doivent être respectivement : 0, 0, 7 et 7.



Deux librairie sont utilisées pour vérifier la validité des mots de passe : `pam passwdqc.so` et `pam unix.so`.

Les réglages de la première librairie s'effectuent via les variables proposées. Si les règles établies par la première librairie ne sont pas suffisamment sécurisées, d'autres règles seront imposées par la seconde :

- le mot de passe ne peut être basé sur l'identifiant du compte ;
- le mot de passe ne peut être basé sur l'ancien mot de passe ;
- le mot de passe ne peut pas comporter des mots du dictionnaire ;
- le mot de passe ne peut être basé sur une séquence connue (suite de lettre sur le clavier par exemple) ;
- le mot de passe doit contenir suffisamment de caractères différents ;
- les lettres majuscules au début du mot de passe et les chiffres à la fin du mot de passe ne comptent pas comme l'utilisation d'une classe de caractère.



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



Il est possible de désactiver la validation des mots de passe en passant `Vérifier la complexité des mots de passe` à `non`.

Il ne faut bien évidement pas désactiver cette fonctionnalité dans un contexte de production.

Cette fonctionnalité est intéressante pour faciliter la mise en place d'une infrastructure de test.



Ce paramétrage concerne uniquement les comptes système du serveur. Les utilisateurs

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> LDAP ne sont pas soumis aux mêmes restrictions.

Ajustement du partitionnement



> L'ajustement du partitionnement est disponible dans l'interface de configuration du module en mode expert et ce uniquement :
>
> - avant l'instance
> - si le partitionnement à l'installation depuis l'ISO n'a pas été modifié

Pour maîtriser correctement ce qui va être fait il faut consulter l'état du partitionnement avant de saisir les paramètres souhaités à l'aide de la commande `df -h /` et des commandes `vgdisplay` et `lvdisplay`.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     2,1G  6,5G  25% /
tmpfs                          1000M      28K 1000M   1% /dev/shm
tmpfs                           5,0M       0  5,0M   0% /run/lock
tmpfs                          1000M       0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M     107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G     2,9M  1,7G   1% /tmp
tmpfs                           200M       0  200M   0% /run/user/0
root@eolebase:~#
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  8
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       5550 / 21,68 GiB
  Free  PE / Size       4510 / 17,62 GiB
  VG UUID               ctPVcP-76Se-EpMp-FLO3-13aR-Ghg9-PdIdUW

root@scribe:~#
```

```
root@scribe:~# lvdisplay

  --- Logical volume ---
  LV Path                /dev/scribe-vg/root
  LV Name                root
  VG Name                scribe-vg
  LV UUID                uN8emF-hD9j-eNwv-zdaC-mEeK-9XGe-uBu2OU
  LV Write Access        read/write
  LV Creation host, time scribe, 2017-10-05 18:37:11 +0200
```

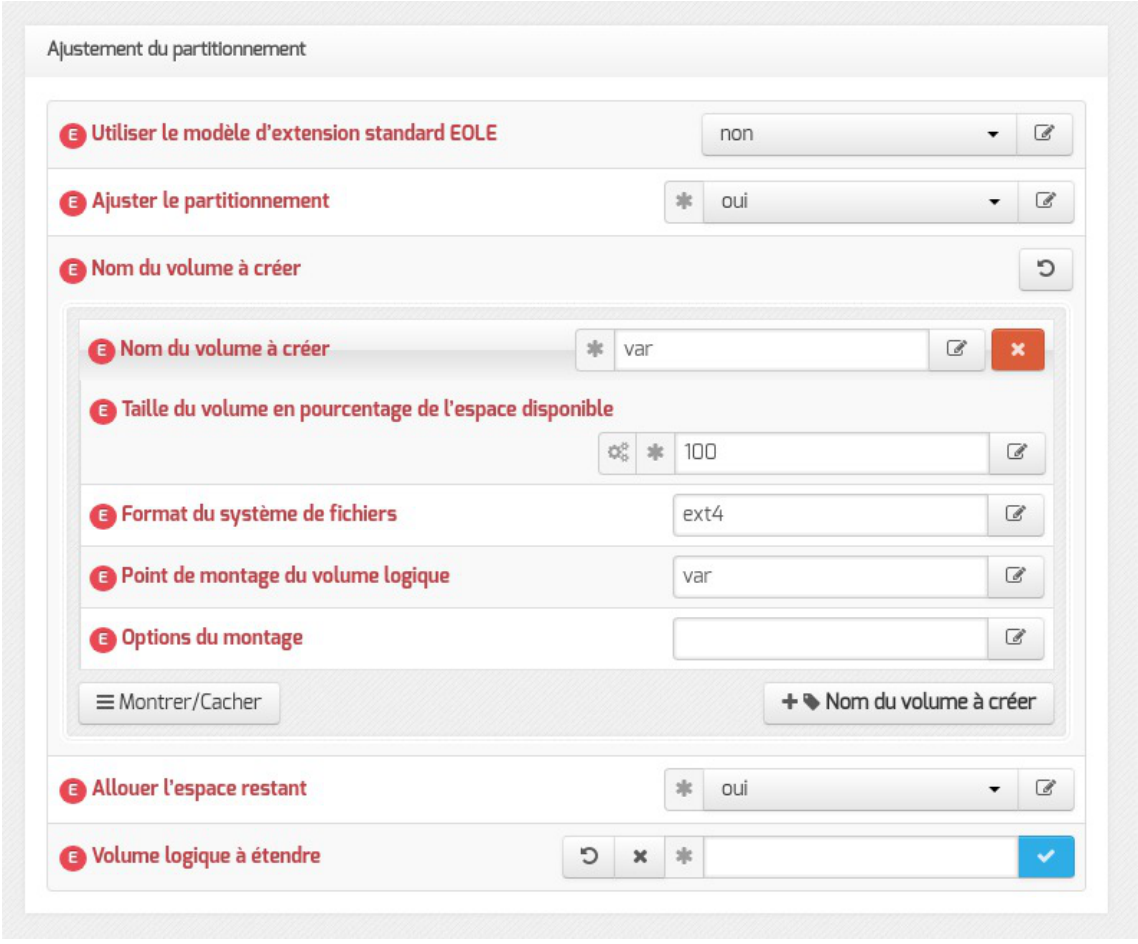

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
  LV Status              available
  # open                 1
  LV Size                8,94 GiB
  Current LE             2288
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:0

[...]
```

Ajuster le partitionnement

Ajuster le partitionnement permet d'ajouter un ou plusieurs volumes logiques et d'ajouter de l'espace à des partitions existantes.

Pour ajuster le partitionnement à partir de la version 2.6.2 d'EOLE, ouvrir l'interface de configuration du module, passer en mode Expert et se rendre dans l'onglet `Système`. Puis il faut passer `Utiliser le modèle d'extension standard EOLE` à `non` pour ajuster le partitionnement.



Ajustement du partitionnement à partir d'EOLE 2.6.2

Après avoir passer `Ajuster le partitionnement` à `oui`, les partitions existantes sont affichées et un certain nombre de paramètres s'affichent.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- nom du volume ;
- pourcentage de l'espace disponible à utiliser ;
- format du système de fichier à utiliser : sans précision le système de fichier est `ext4` ;
- point de montage ;
- les options du montage (indispensable pour la gestion des quotas par exemple).

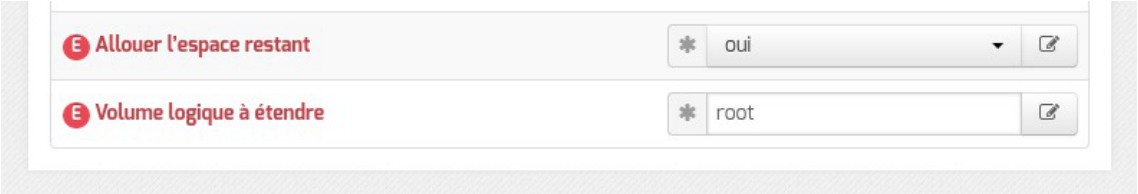
Pour ajouter un nouveau volume logique, cliquer sur le bouton `+ Nom du volume à créer`.



Les nouveaux volumes ne sont pas montés automatiquement, il faut renseigner le fichier `/etc/fstab`.

Allouer l'espace restant

Positionner la variable `Allouer l'espace restant` à `oui` permet de choisir un volume existant auquel ajouter la totalité de l'espace libre restant.



La valeur à saisir est la partie du nom du volume qui permet d'identifier le point de montage, par exemple pour le volume `/dev/mapper/eolebase--vg-root` il faut saisir `root` dans le nom du `Volume logique à étendre`. S'il ne reste pas d'espace, ce jeu de paramètres est sans effet.

Résultat après instance

Le paramétrage est effectif après l'instanciation du module.

```
root@eolebase:~# df -h
Sys. de fichiers              Taille Utilisé Dispo Uti% Monté sur
udev                            980M       0  980M   0% /dev
tmpfs                           200M     3,2M  197M   2% /run
/dev/mapper/eolebase--vg-root   9,1G     1,9G  6,7G  22% /
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
tmpfs                          1000M        0 1000M   0% /dev/shm
tmpfs                           5,0M        0  5,0M   0% /run/lock
tmpfs                          1000M        0 1000M   0% /sys/fs/cgroup
/dev/sda1                       687M    107M  531M  17% /boot
/dev/mapper/eolebase--vg-tmp    1,8G    3,6M  1,7G   1% /tmp
tmpfs                           200M        0  200M   0% /run/user/0
/dev/mapper/eolebase--vg-var     27G    311M   25G   2% /var
root@eolebase:~#
```

Le nouveau volume logique est présent et la partition `/root` s'est vu augmentée du reste de l'espace libre.

Voir aussi...

Les mots de passe [p.361]

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).

Autoriser les connexions SSH pour l'utilisateur root

Permet d'interdire les connexions SSH avec le compte utilisateur `root` (paramètre `PermitRootLogin`).

Autoriser les connexions SSH par mot de passe (si non clef RSA obligatoire)

Permet d'interdire les connexions SSH par mot de passe. Dans ce cas, seules les connexions par clef RSA seront autorisées (paramètre `PasswordAuthentication`).

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)`.

Autoriser les connexions SSH pour les groupes

Permet de déclarer des groupes Unix supplémentaires autorisés à se connecter en SSH au serveur (paramètre `AllowGroups`).

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Critères à appliquer pour le blocage des tentatives de connexions par force brute

La première valeur est le nombre de tentatives de connexions échouées tolérées. La dernière valeur est le nombre de connexions échouées maximales. La deuxième valeur fixe le pourcentage de refus aléatoire une fois le nombre de connexions tolérées atteint. Ce pourcentage de refus augmente à chaque échec supplémentaire jusqu'à ce que le nombre de connexions maximales soit atteint (paramètre `MaxStartups`).

4.6. Onglet NTP : Options supplémentaires pour la synchronisation de l'horloge système



Le paramètre disponible dans cet onglet du mode expert permet de désactiver l'utilisation d'un pool de serveurs de secours pour la synchronisation de l'horloge.

Recourir aux serveurs de ce pool permet de pallier une défaillance du ou des serveurs NTP renseignés dans l'onglet Général (variable `serveur_ntp`).

Par défaut, l'utilisation du pool est activée.

Sa désactivation est parfois requise pour limiter la bande passante utilisée par le service de synchronisation du temps, celui-ci cherchant à contacter un grand nombre de sources de temps pour déterminer l'heure du serveur.

4.7. Onglet Logs : Gestion des logs

La journalisation des événements des applications est un élément important de la maintenance et de l'analyse du fonctionnement d'un module.

Les modules disposent de deux dispositifs de journalisation en partie complémentaire pour la conservation des événements localement. En outre, ils proposent la configuration avancée de Rsyslog pour la centralisation des journaux de plusieurs modules.

Conservation locale des journaux

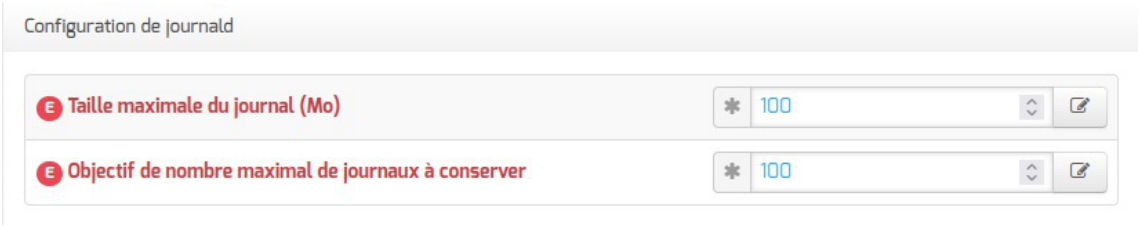
En plus d'être envoyés a Rsyslog[p.729], la plupart des événements des applications sont également stockés dans des fichiers binaires par journald[p.716].

Sur les modules EOLE, les journaux de référence sont ceux gérés via Rsyslog.

journald offre néanmoins d'autres modalités de recherche, utiles notamment pour l'analyse des incidents. Aussi, les modules mettent en place une configuration permettant de conserver une quantité restreinte de journaux binaires afin de limiter la place occupée mais néanmoins permettre de profiter de capacités d'interrogation étendues sur les journaux récents.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

L'espace occupé par les journaux gérés par journald[p.716] est configuré via deux variables disponibles en mode expert dans l'onglet `Logs`.



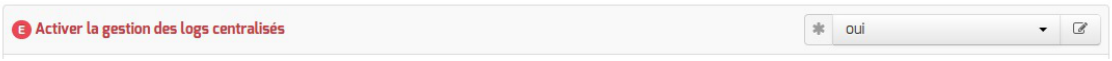
- `Taille maximale du journal (Mo)` : définit une limite de taille du journal en Mo.
- `Objectif de nombre maximal de journaux à conserver` : définit la cible du nombre de journaux à conserver, étant donné que seuls les journaux archivés peuvent être supprimés pour atteindre cet objectif.

> Une configuration équivalente des fichiers gérés par Rsyslog et logrotate n'est pas disponible pour l'administrateur et répond, notamment, aux exigences légales.

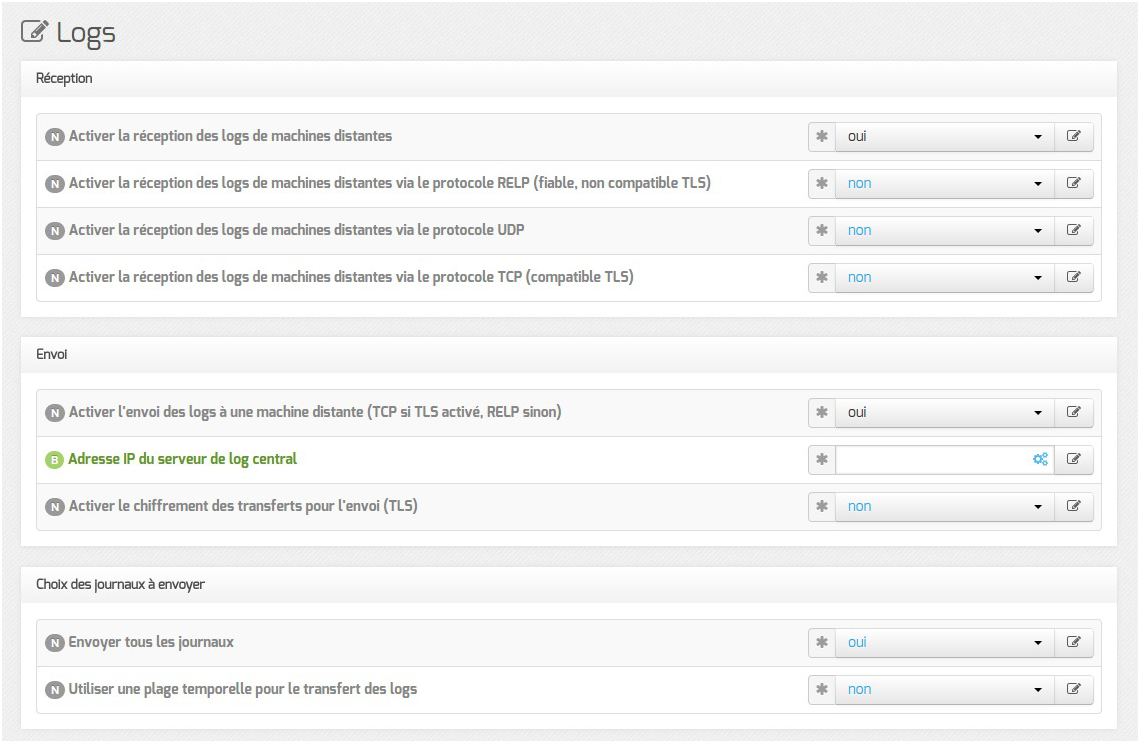
Centralisation des journaux

La possibilité de centraliser des logs a été dissociée de la mise en place d'un serveur ZéphirLog[p.735]. Cela rend possible un transfert croisé des journaux ou une centralisation.

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



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



Vue de l'onglet Logs

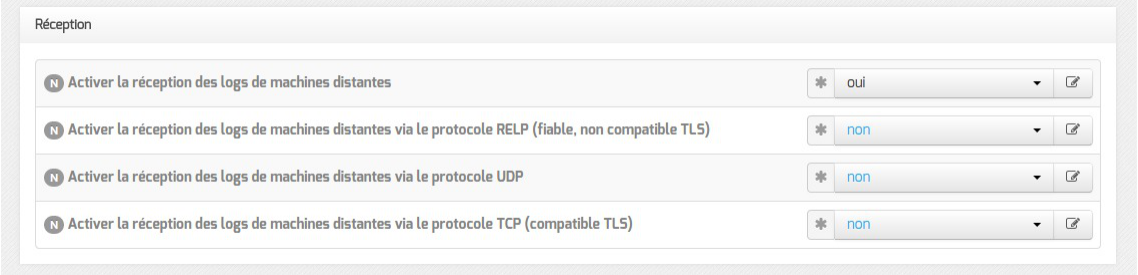
Les options de cet onglet sont réparties en plusieurs sections :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.732] ou RELP[p.728]) utilisé est contraint par l'activation ou non du chiffrement (TLS[p.733]) ;
- 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.703].

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.703].

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Certificats

Si le protocole utilisé pour la réception ou l'envoi des journaux nécessite un chiffrement (TLS), il est possible de spécifier les chemins associés aux certificats utilisés par rsyslog.



Par défaut, les certificats du module sont utilisés et leur validité n'est pas vérifiée.

Choix des journaux à envoyer

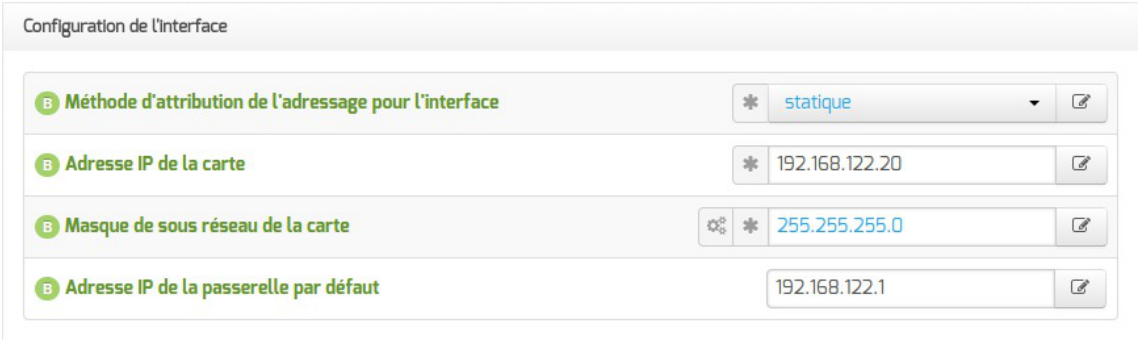
Si l'envoi des journaux est activé, il est possible d'envoyer tous les journaux ou de choisir les journaux à envoyer.



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.

4.8. Onglet Interface-0

Configuration de l'interface



Avant toute chose, il faut décider comment la carte réseau est configurée.

Pour cela, il existe trois possibilités : statique[p.702], DHCP[p.708] ou `non géré`.

Méthode d'attribution statique

Dans le cas de la configuration statique, il faut renseigner l'adresse IP, le masque et la passerelle.



EOLE est pleinement fonctionnel avec une connexion en IP fixe. Si vous ne disposez pas d'IP

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

fixe, certaines fonctionnalités ne seront plus disponibles.

Méthode d'attribution DHCP

La configuration DHCP ne nécessite aucun paramétrage particulier.

Lors du passage d'une configuration statique à une configuration DHCP, il faut procéder à deux reconfigure successifs.

Méthode d'attribution "non géré"

L'utilisation de la nouvelle valeur `non gérée` permet de déléguer la configuration réseau à cloud-init[p.714] ou à un autre outil de contextualisation.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

Afin de respecter la convention Consistent Network Device Naming[p.706], le nom de l'interface réseau proposé dans l'interface de configuration du module correspond à son emplacement physique.

L'ordre de chargement des cartes réseau n'est donc plus susceptible d'être modifié en cas de changement matériel, contrairement aux versions précédentes qui utilisaient les adresses MAC[p.702] des cartes pour les identifier.

De ce fait, l'ancien fichier de configuration `/etc/udev/rules.d/70-persistent-net.rules` n'existe plus.

Ajouter des interfaces physiques supplémentaires à la variable `Nom de l'interface réseau` permet d'activer l'agrégation de liens Ethernet[p.702].

Les noms réels des interfaces sont visibles dans le répertoire `/sys/class/net/` :

```
# ls -d /sys/class/net/*
/sys/class/net/ens4 /sys/class/net/lo
```

Les interfaces gérées par EOLE sont enregistrées dans le fichier spécial : `/var/lib/eole/config/persistent-net.cfg`.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface logique associée à l'interface physique pour cette zone.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Activation du mode promiscuous pour l'interface

Par défaut, le mode promiscuous[p.721] est désactivé sur les interfaces réseau du module.

Toutefois, il peut être activé, par interface, pour permettre le fonctionnement du module dans certains types d'infrastructure.

Par exemple, le mode promiscuous doit être activé si le module utilise des conteneurs LXC[p.719] (AmonEcole et Scribe notamment) et est virtualisé grâce à `VirtualBox`.

Pour le désactiver, le passage de la variable à non et le reconfigure ne sont pas suffisants. Il faut, en plus, redémarrer le serveur.

Auto-négociation de la connexion pour l'interface

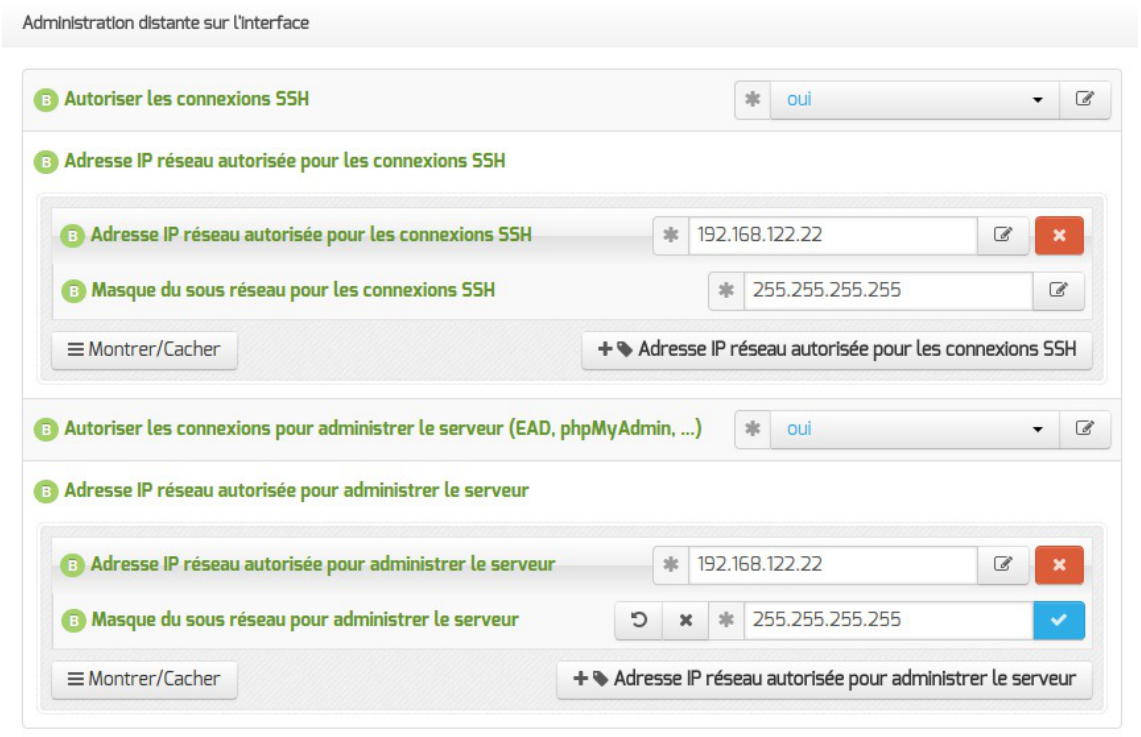
Par défaut, toutes les interfaces sont en mode *auto-négociation*.

Ce paramètre ne devrait être modifié 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.

En passant cette variable à `non`, il devient possible de spécifier la vitesse et le duplex de la connexion.

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

Administration à distance



Configuration de l'administration à distance sur une interface

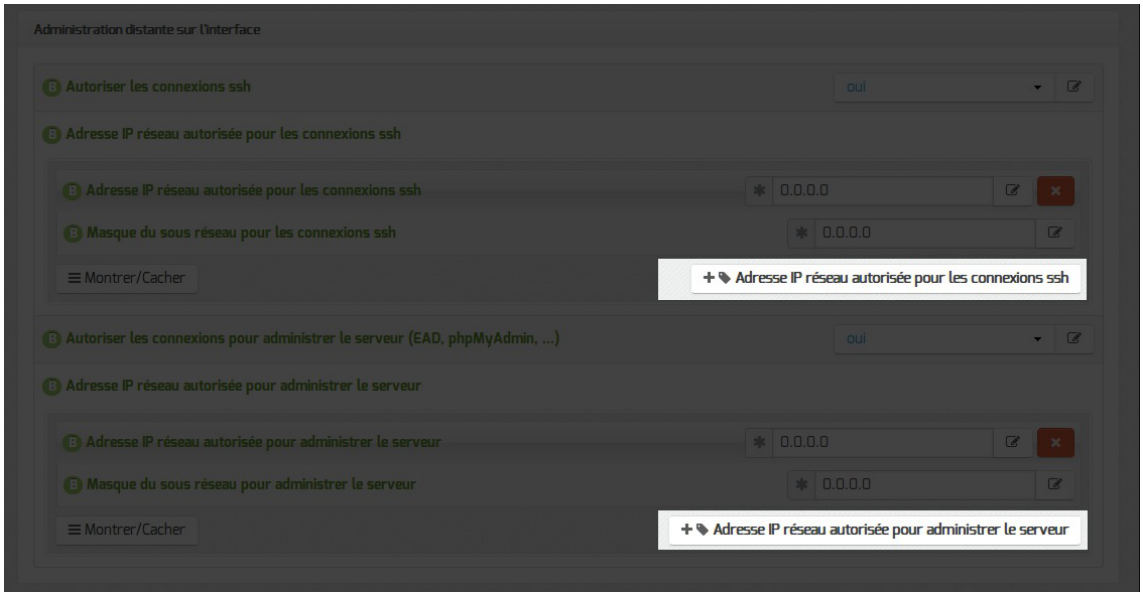
Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

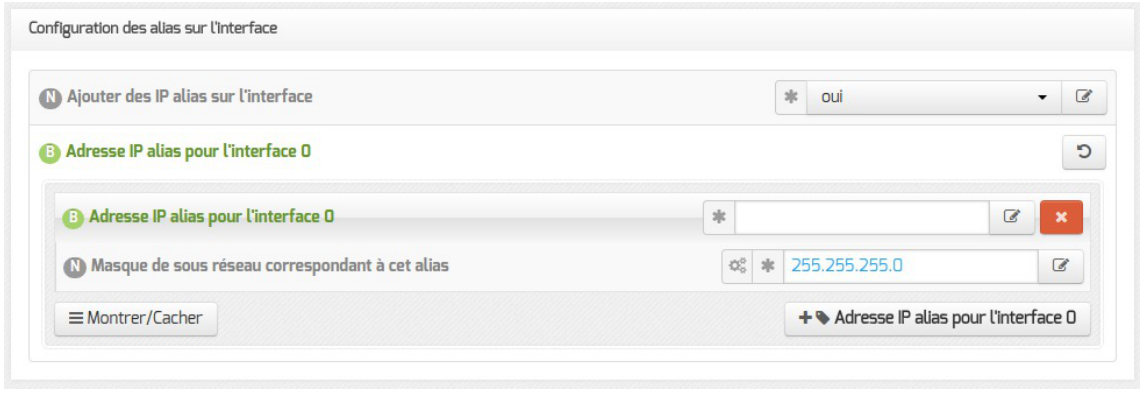
Dans le cadre de test sur un module l'utilisation de la valeur `0.0.0.0` dans les champs `Adresse IP réseau autorisée pour les connexions SSH` et `Masque du sous réseau pour les connexions SSH` autorise les connexions SSH depuis n'importe quelle adresse IP.

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

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

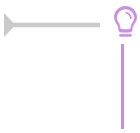
Configuration des alias sur l'interface

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



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

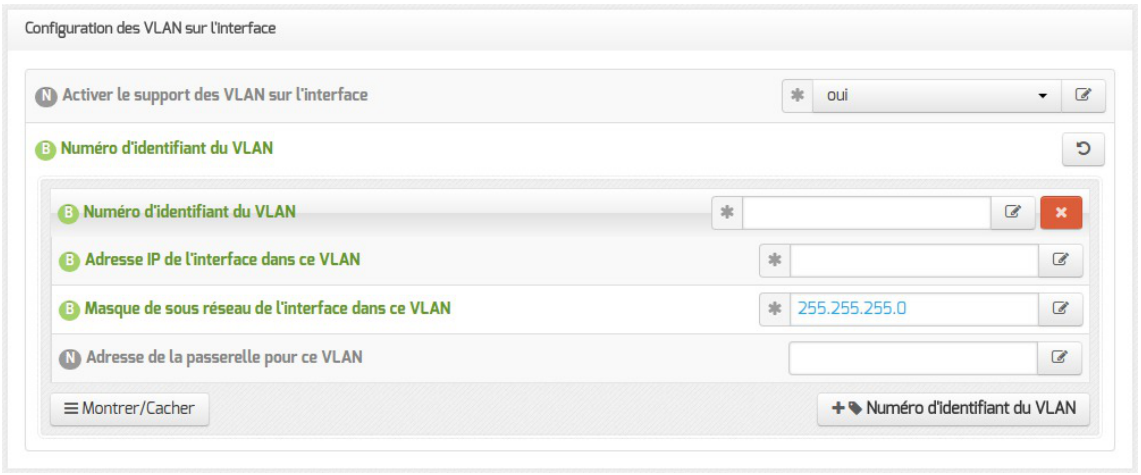
Pour cela, il faut activer le support des alias (`Ajouter des IP alias sur l'interface` à `oui`) et configurer l'adresse IP et le masque de sous-réseau.



Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

Configuration des VLAN sur l'interface

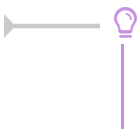
Il est possible de configurer des VLAN[p.734] (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous-réseau de l'interface dans ce VLAN.

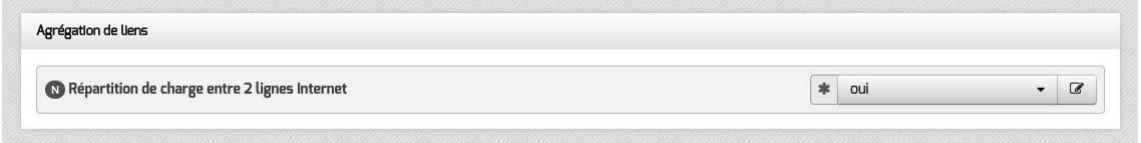
Il est possible de configurer une passerelle particulière pour un VLAN de l'interface 0.



Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

Agrégation de routes IP

L'activation d'un alias IP, fait apparaître un nouveau paramètre : `Répartition de charge entre 2 lignes Internet`.



Pour activer l'agrégation de routes IP[p.702] (niveau 3), il faut passer ce nouveau paramètre à `oui`.

Un nouvel onglet : `Agrégation` est alors disponible.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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



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`.

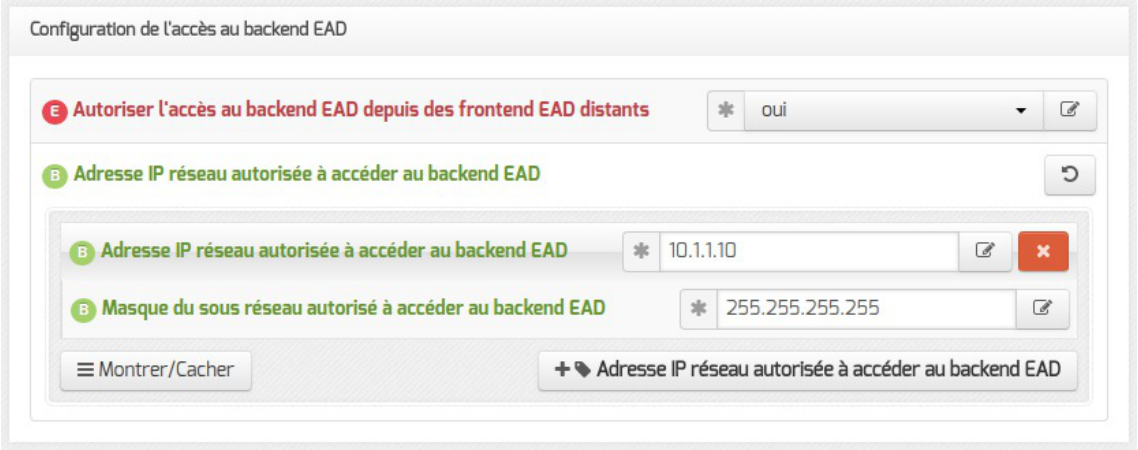


Sur les modules Amon et AmonEcole cette question est également présente dans l'onglet `Interface-0`.

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.

Accès au backend EAD



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour permettre à un frontend EAD[p.710] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Par défaut, l'accès au backend est bloqué pour chaque interface.

Si le pare-feu est désactivé (mode expert dans l'onglet `Réseau avancé`), ces autorisations ne sont plus visibles et l'accès est autorisé à tous les frontend depuis toutes les interfaces.

Voir aussi...

Onglet Agrégation : Mise en place d'une répartition de charge ou d'une haute disponibilité [p.128]

Mise en place de l'agrégation de liens Ethernet (bonding) [p.358]

4.9. Onglet Interface-1

Nombre d'interfaces

Un module Amon ou AmonEcole 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



En mode expert, il est possible de configurer l'interface en mode DHCP[p.708].



Si l'interface est configurée avec un adressage statique[p.702], il faut renseigner l'adresse IP et le masque de sous-réseau.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

Afin de respecter la convention Consistent Network Device Naming[p.706], le nom de l'interface réseau proposé dans l'interface de configuration du module correspond à son emplacement physique.

L'ordre de chargement des cartes réseau n'est donc plus susceptible d'être modifié en cas de changement matériel, contrairement aux versions précédentes qui utilisaient les adresses MAC[p.702] des cartes pour les identifier.

De ce fait, l'ancien fichier de configuration `/etc/udev/rules.d/70-persistent-net.rules` n'existe plus.

Ajouter des interfaces physiques supplémentaires à la variable `Nom de l'interface réseau` permet d'activer l'agrégation de liens Ethernet[p.702].

Les noms réels des interfaces sont visibles dans le répertoire `/sys/class/net/` :

```
# ls -d /sys/class/net/*
/sys/class/net/ens4 /sys/class/net/lo
```

Les interfaces gérées par EOLE sont enregistrées dans le fichier spécial : `/var/lib/eole/config/persistent-net.cfg`.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface logique associée à l'interface physique pour cette zone.

Activation du mode promiscuous pour l'interface

Par défaut, le mode promiscuous[p.721] est désactivé sur les interfaces réseau du module.

Toutefois, il peut être activé, par interface, pour permettre le fonctionnement du module dans certains types d'infrastructure.

Par exemple, le mode promiscuous doit être activé si le module utilise des conteneurs LXC[p.719] (AmonEcole et Scribe notamment) et est virtualisé grâce à `VirtualBox`.

Pour le désactiver, le passage de la variable à non et le reconfigure ne sont pas suffisants. Il faut, en plus, redémarrer le serveur.

Auto-négociation de la connexion pour l'interface

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

Ce paramètre ne devrait être modifié que s'il y a un problème de négociation entre un élément actif et une

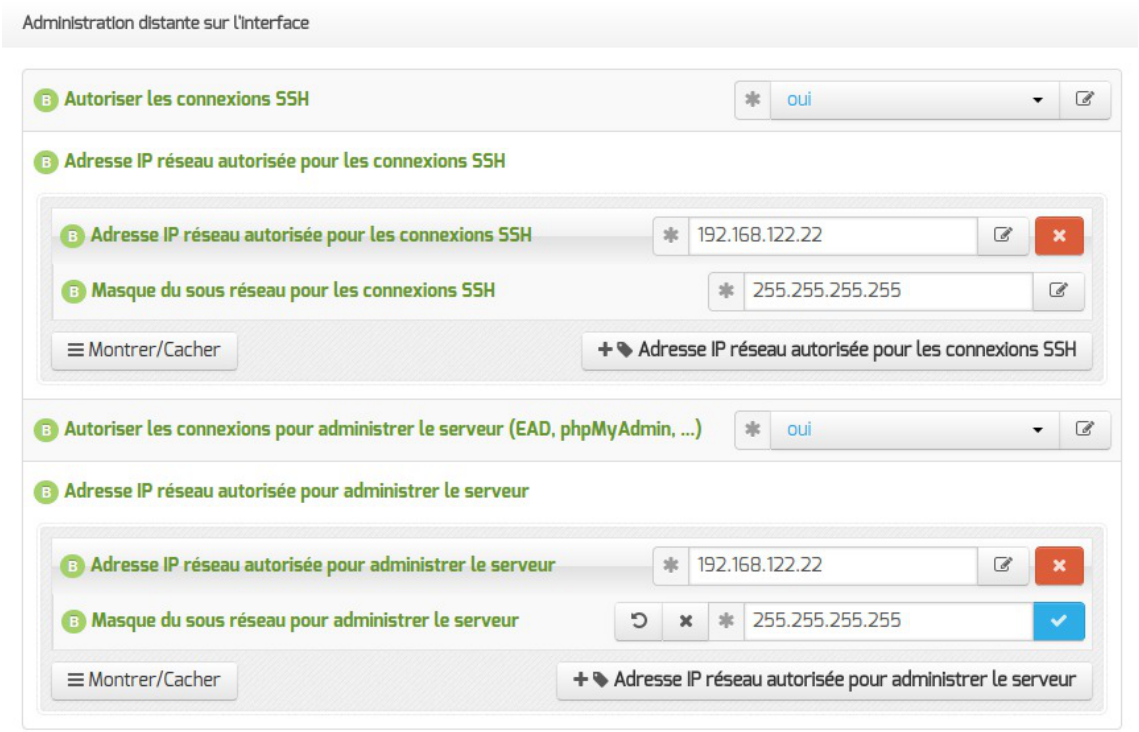
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

des cartes réseau, tous les équipements modernes gérant normalement l'auto-négociation.

En passant cette variable à `non`, il devient possible de spécifier la vitesse et le duplex de la connexion.

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

Administration à distance



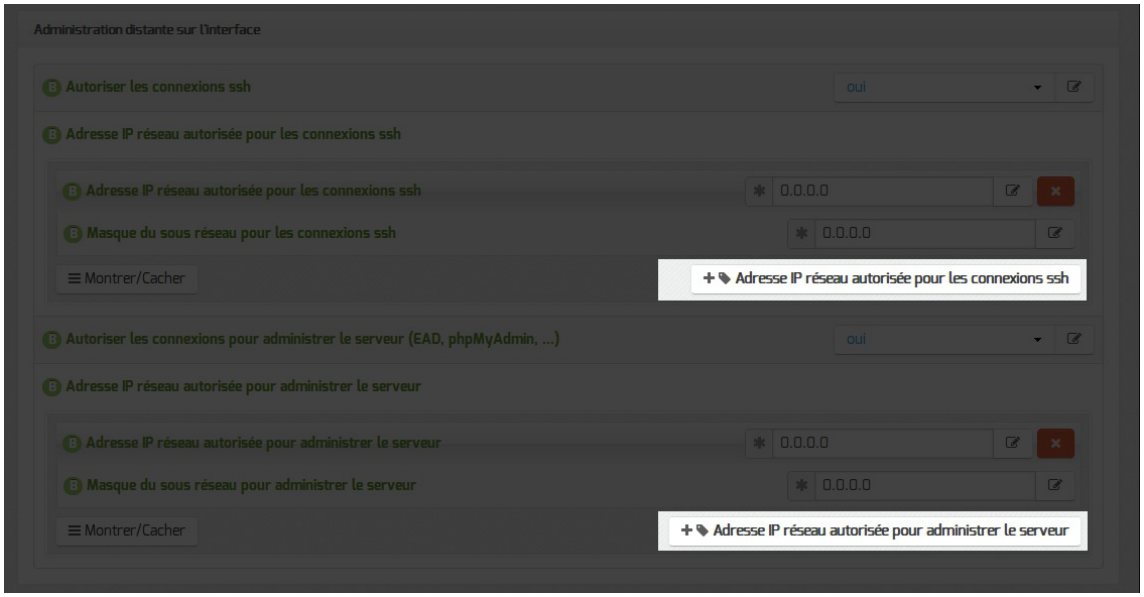
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

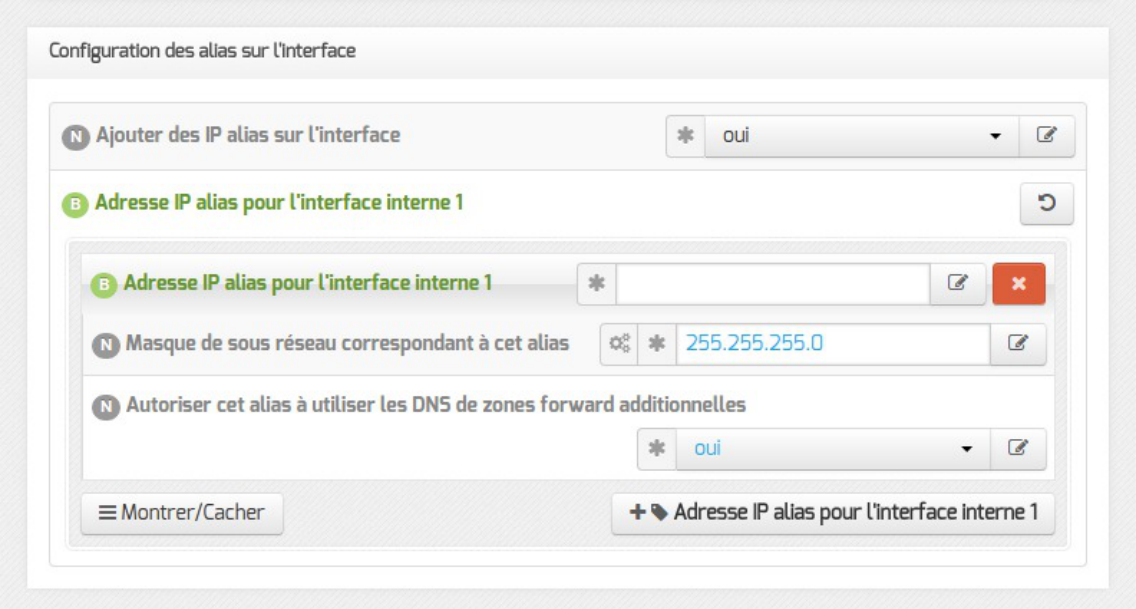
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -ni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

Configuration des alias sur l'interface

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

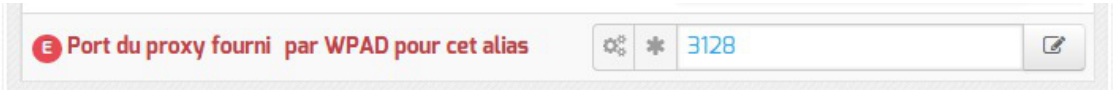
La variable `Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

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.

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

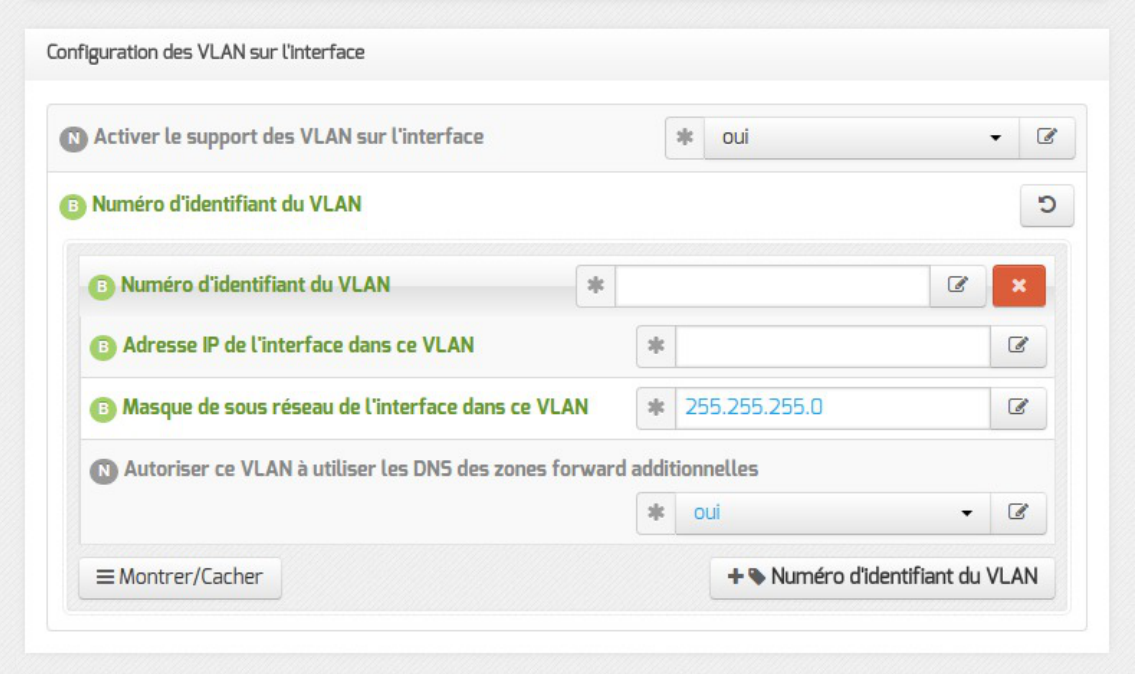


Par défaut, le port du proxy est défini à 3128.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.734] (réseau local virtuel) sur une interface déterminée du module.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

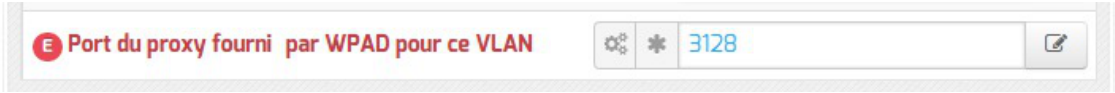
La variable `Autoriser ce VLAN à utiliser les DNS des zones forward additionnelles` permet d'autoriser le réseau de ce VLAN à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

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.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Configuration DNS sur l'interface

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

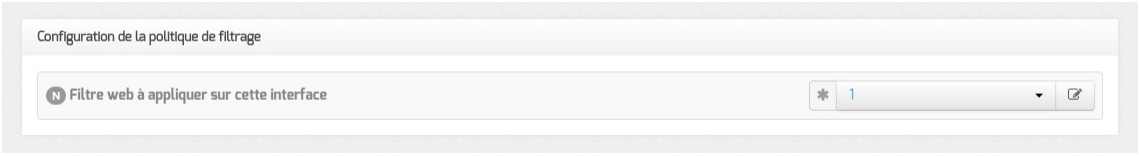


- `Nom de la zone (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface. Le nom (par défaut admin pour l'interface 1) doit être différent pour chacune des interfaces.

Configuration des zones de filtrage

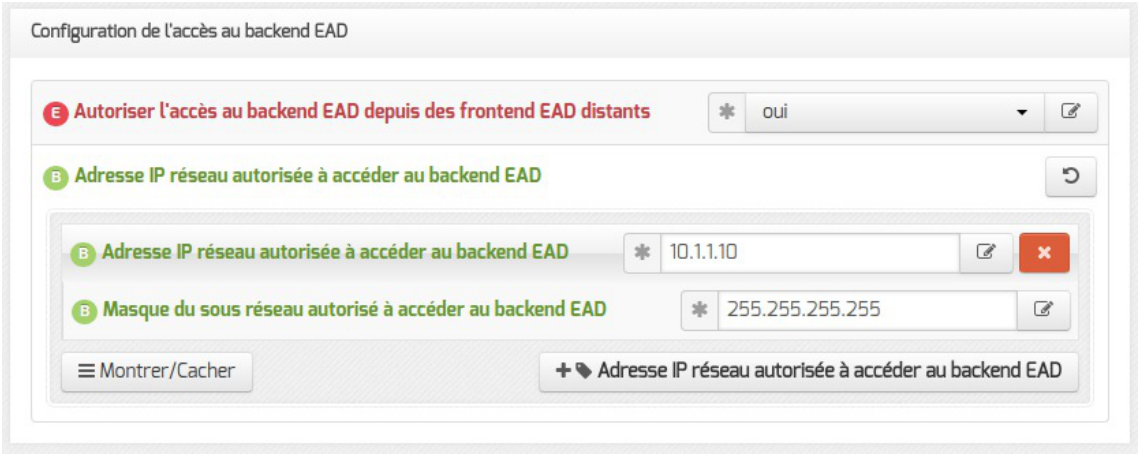
La solution de filtrage permet de différencier 2 zones, ce qui permet de dissocier 2 politiques de filtrage majeures et distinctes comme par exemple une zone réseau administratif et une zone réseau pédagogique.

Il faut choisir à quelle zone appartient une interface. Cela s'effectue dans la configuration de chaque interface réseau en sélectionnant le numéro de la zone souhaité dans le champ `Filtre Web à appliquer à cette interface`.



> Les zones `Filtre web 1` et `Filtre web 2` correspondent chacun à une instance du logiciel de filtrage. La configuration de chacune des instances s'effectue dans l'onglet `Filtrage web`.

Accès au backend EAD



Pour permettre à un frontend EAD[p.710] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Par défaut, l'accès au backend est bloqué pour chaque interface.

> Si le pare-feu est désactivé (mode expert dans l'onglet `Réseau avancé`), ces autorisations ne sont plus visibles et l'accès est autorisé à tous les frontend depuis toutes les interfaces.

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.

Voir aussi...

Onglet Filtrage web : Configuration du filtrage web [p.285]

Mise en place de l'agrégation de liens Ethernet (bonding) [p.358]

4.10. Onglet Interface-n

Nombre d'interfaces

Un module Amon ou AmonEcole 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.



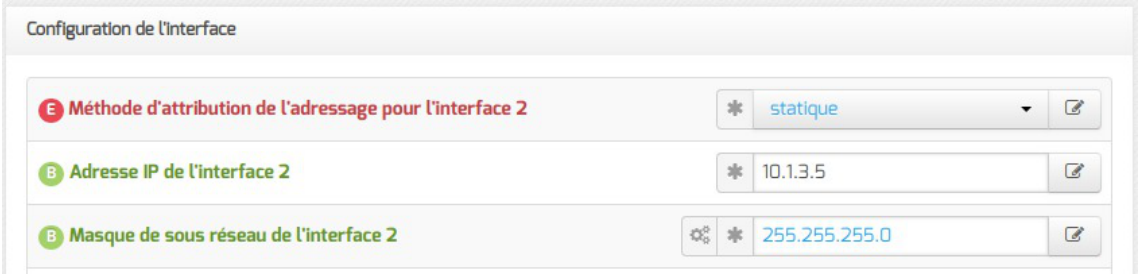
Cela ajoute autant d'onglets `Interface-n` que le nombre d'interfaces à activer choisi.

Configuration de l'interface



En mode expert, il est possible de configurer l'interface en mode DHCP[p.708].

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Si l'interface est configurée avec un adressage statique[p.702], il faut renseigner l'adresse IP et le masque de sous-réseau.

En mode expert quelques variables supplémentaires sont disponibles.



Nom de l'interface réseau

Afin de respecter la convention Consistent Network Device Naming[p.706], le nom de l'interface réseau proposé dans l'interface de configuration du module correspond à son emplacement physique.

L'ordre de chargement des cartes réseau n'est donc plus susceptible d'être modifié en cas de changement matériel, contrairement aux versions précédentes qui utilisaient les adresses MAC[p.702] des cartes pour les identifier.

De ce fait, l'ancien fichier de configuration `/etc/udev/rules.d/70-persistent-net.rules` n'existe plus.

Ajouter des interfaces physiques supplémentaires à la variable `Nom de l'interface réseau` permet d'activer l'agrégation de liens Ethernet[p.702].

Les noms réels des interfaces sont visibles dans le répertoire `/sys/class/net/` :

```
# ls -d /sys/class/net/*
/sys/class/net/ens4 /sys/class/net/lo
```

Les interfaces gérées par EOLE sont enregistrées dans le fichier spécial : `/var/lib/eole/config/persistent-net.cfg`.

Nom de l'interface réseau de la zone

Ce champ permet de personnaliser le nom de l'interface logique associée à l'interface physique pour cette zone.

Activation du mode promiscuous pour l'interface

Par défaut, le mode promiscuous[p.721] est désactivé sur les interfaces réseau du module.

Toutefois, il peut être activé, par interface, pour permettre le fonctionnement du module dans certains types d'infrastructure.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Par exemple, le mode promiscuous doit être activé si le module utilise des conteneurs LXC[p.719] (AmonEcole et Scribe notamment) et est virtualisé grâce à `VirtualBox`.

Pour le désactiver, le passage de la variable à non et le reconfigure ne sont pas suffisants. Il faut, en plus, redémarrer le serveur.

Auto-négociation de la connexion pour l'interface

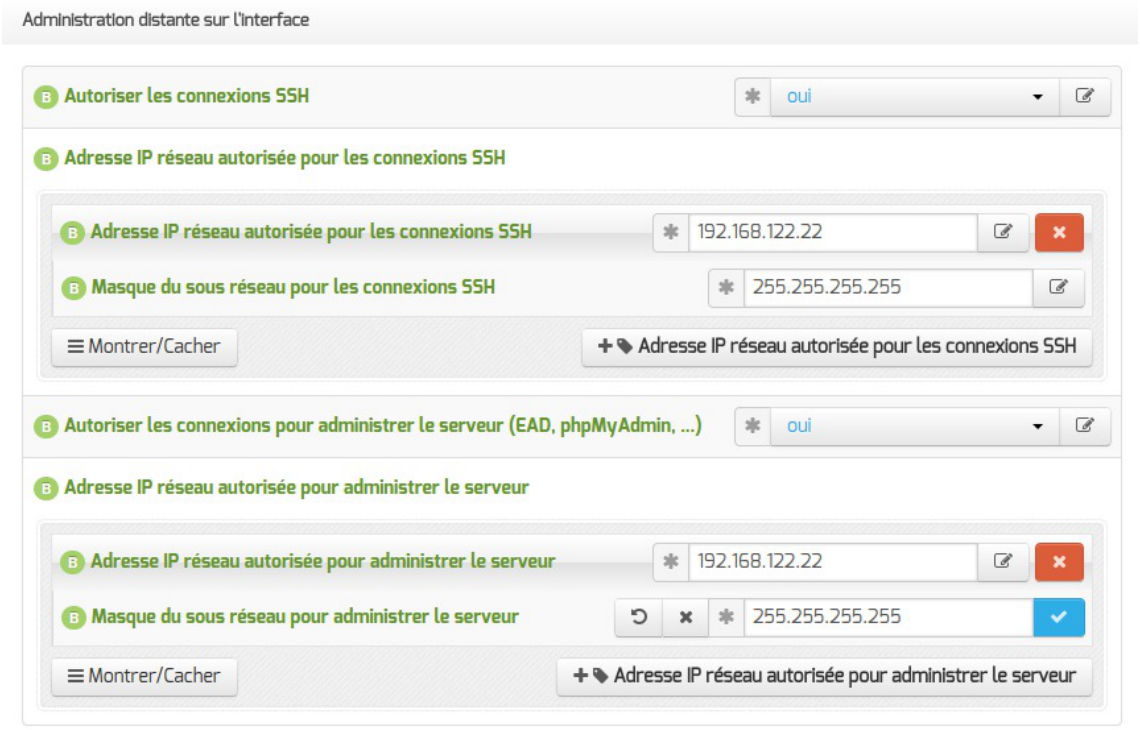
Par défaut, toutes les interfaces sont en mode *auto-négociation*.

Ce paramètre ne devrait être modifié 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.

En passant cette variable à `non`, il devient possible de spécifier la vitesse et le duplex de la connexion.

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

Administration à distance



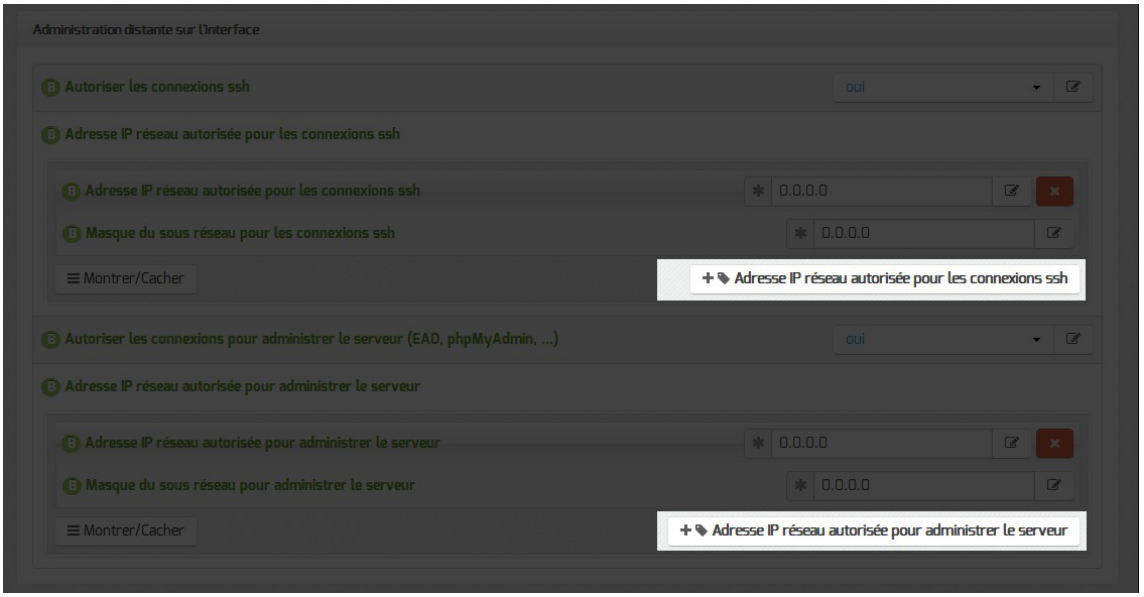
Configuration de l'administration à distance sur une interface

Par défaut les accès SSH[p.731] et aux différentes interfaces d'administration (EAD, Adminer, CUPS, ARV... selon le module) sont bloqués.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

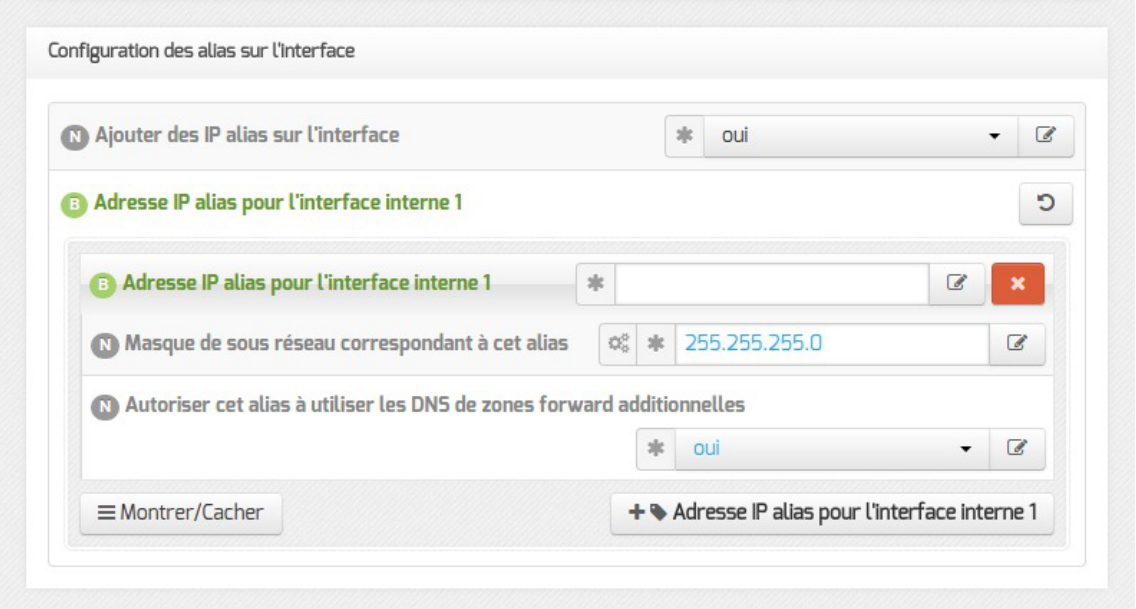
La commande suivante permet d'observer les connexions SSH arrivant sur un serveur EOLE : `tcpdump -ni $(CreoleGet nom_carte_eth0) port 22`

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans l'onglet `Onglet Interface-0` partie `Administration à distance`

Configuration des alias sur l'interface

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

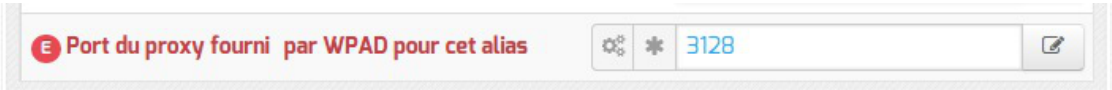
La variable `Autoriser cet alias à utiliser les DNS de zones forward additionnelles` permet d'autoriser le réseau de cet alias à résoudre les noms d'hôte des domaines déclarés dans la section Forward de zone DNS de l'onglet `Zones-dns`.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

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.

En mode expert, si WPAD est activé, il est possible de modifier le port du proxy diffusé pour un alias donné.

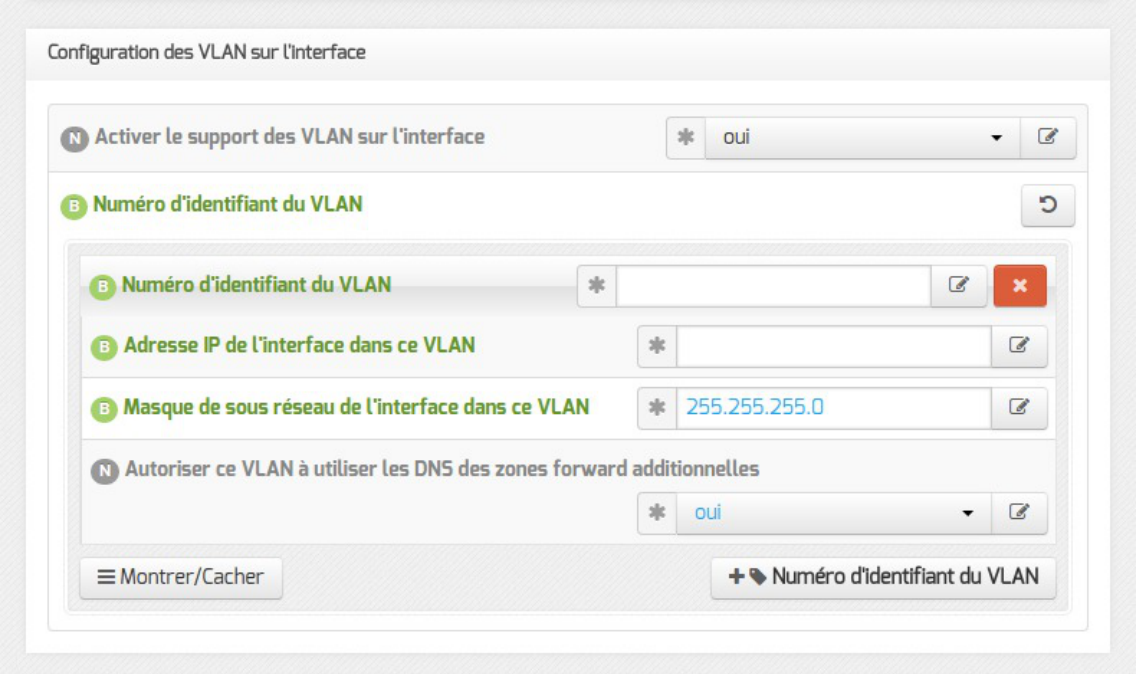


Par défaut, le port du proxy est défini à 3128.

Configuration des VLAN sur l'interface

Il est possible de configurer des VLAN[p.734] (réseau local virtuel) sur une interface déterminée du module.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

La variable `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`.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

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.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Configuration DNS sur l'interface

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

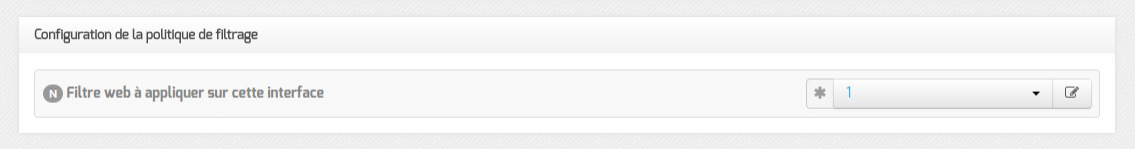


- `Nom de la zone (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface. Le nom (par défaut admin pour l'interface 1) doit être différent pour chacune des interfaces.

Configuration des zones de filtrage

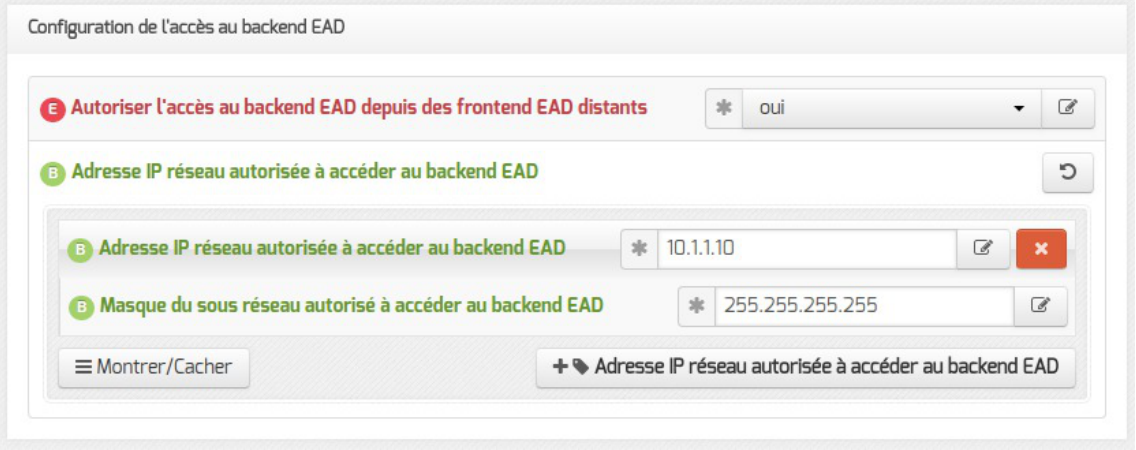
La solution de filtrage permet de différencier 2 zones, ce qui permet de dissocier 2 politiques de filtrage majeures et distinctes comme par exemple une zone réseau administratif et une zone réseau pédagogique.

Il faut choisir à quelle zone appartient une interface. Cela s'effectue dans la configuration de chaque interface réseau en sélectionnant le numéro de la zone souhaité dans le champ `Filtre Web à appliquer à cette interface`.



> Les zones `Filtre web 1` et `Filtre web 2` correspondent chacun à une instance du logiciel de filtrage. La configuration de chacune des instances s'effectue dans l'onglet `Filtrage web`.

Accès au backend EAD



Pour permettre à un frontend EAD[p.710] distant de se connecter au serveur de commandes de l'EAD local, il faut l'autoriser explicitement pour chaque interface.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Par défaut, l'accès au backend est bloqué pour chaque interface.

Si le pare-feu est désactivé (mode expert dans l'onglet `Réseau avancé`), ces autorisations ne sont plus visibles et l'accès est autorisé à tous les frontend depuis toutes les interfaces.

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.

Voir aussi...

- Onglet Filtrage web : Configuration du filtrage web [p.285]
- Onglet Proxy authentifié : 4 méthodes d'authentification [p.300]
- Mise en place de l'agrégation de liens Ethernet (bonding) [p.358]

4.11. Onglet Réseau avancé

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

Configuration IP



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`)

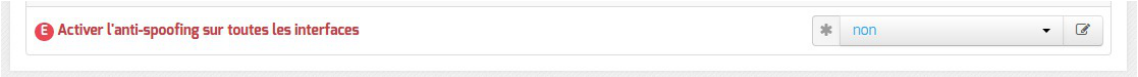
Sécurité



Si la variable `Journaliser les "martian sources"` est à `oui`, tous les passages de paquets

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

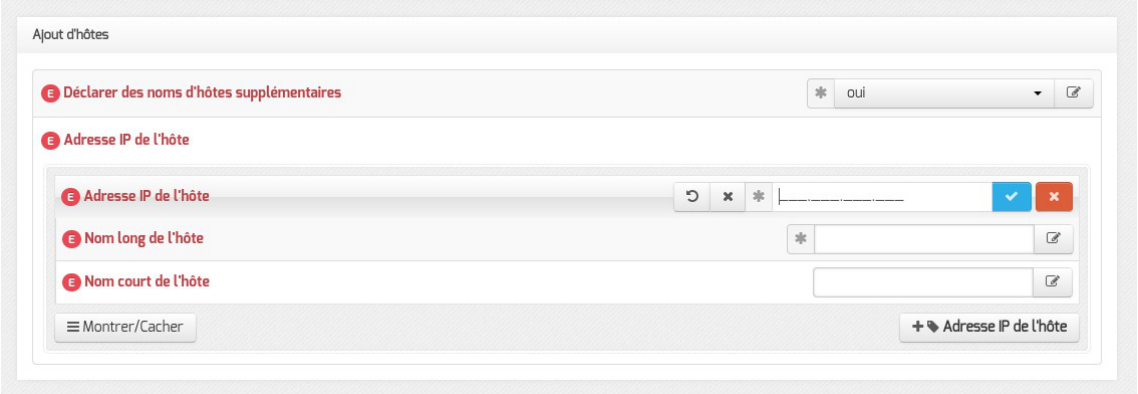
utilisant des adresses IP réservées à un usage particulier (http://tools.ietf.org/html/rfc5735) seront enregistrées dans les journaux.



Par défaut, l'anti-spoofing[p.703] est activé sur l'interface-0 des modules EOLE.

Sur les serveurs ayant 2 interfaces réseau ou plus d'activées (cas par défaut sur les modules Amon, Sphynx et Hâpy), il est possible de demander l'activation de l'anti-spoofing sur les autres interfaces en passant la variable `Activer l'anti-spoofing sur toutes les interfaces` à `oui`.

Ajout d'hôtes



Passer la variable `Déclarer des noms d'hôtes supplémentaires` à `oui`, permet de déclarer des noms d'hôtes qui seront ajoutés au fichier `/etc/hosts`.

Il est possible d'ajouter plusieurs hôtes supplémentaires en cliquant sur le bouton `+Adresse IP de l'hôte` .

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

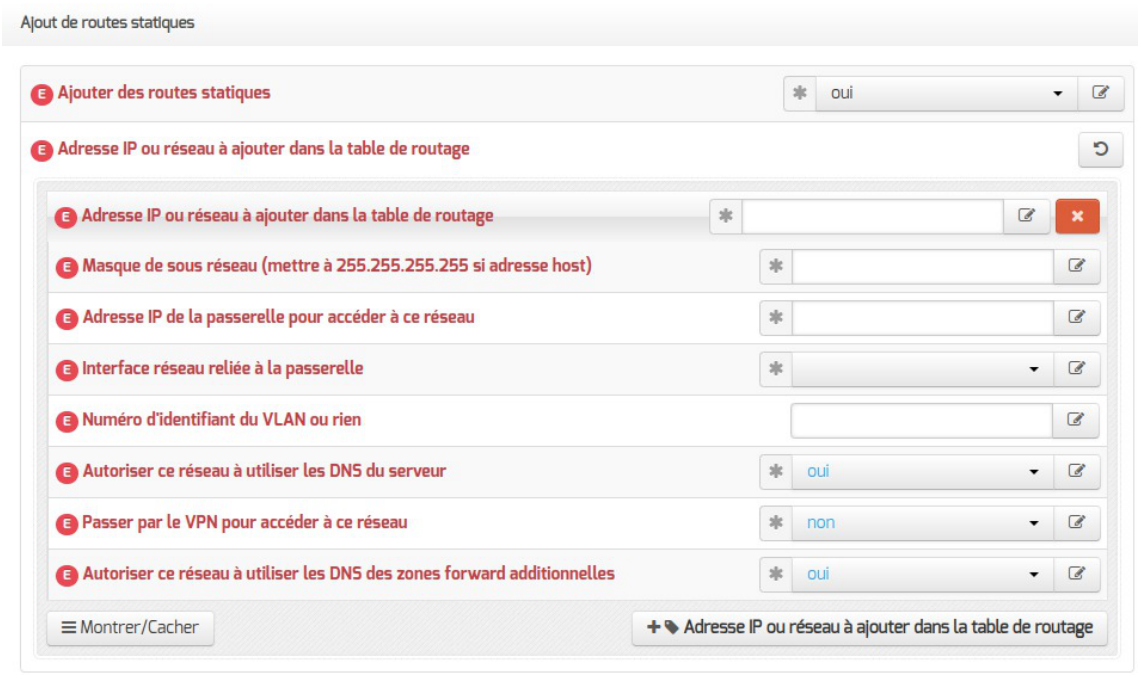


Sur les serveurs EOLE faisant office de serveur DNS, comme les modules Amon et AmonEcole, pour que le logiciel BIND[p.705] puisse résoudre un nom, il faut que le suffixe DNS de ce nom long corresponde au `Nom de domaine privé du réseau local` saisi dans l'onglet `Général`.

Si ce n'est pas le cas, il faut déclarer un `Nom de domaine local supplémentaire` dans l'onglet `Zones-dns` pour permettre au serveur de résoudre ce nom d'hôte.

Ajout de routes statiques

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 configurer 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 ;
- `Numéro d'identifiant du VLAN ou rien` : permet d'associer une route à un VLAN ;

Les deux paramètres suivants apparaissent uniquement si le service `eole-dns` est installé sur le module :

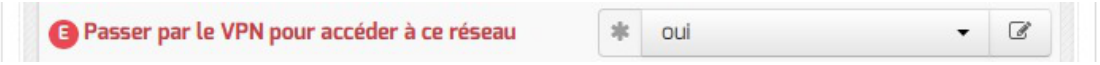
- `Autoriser ce réseau à utiliser les DNS du serveur` : les postes du réseau cible peuvent interroger le service DNS du serveur ;
- `Autoriser ce réseau à utiliser les DNS des zones forward additionnelles` : les postes du réseau cible sont autorisés à interroger les DNS des zones de forward.

Le paramètre suivant apparaît uniquement si le réseau virtuel privé RVP est activé :

- `Passer par le VPN pour accéder à ce réseau` : ce réseau n'est pas un réseau local. C'est un réseau distant accessible par le VPN.

Si le support du RVP est activé, des options supplémentaires sont disponibles :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- `Passer par le VPN pour accéder à ce réseau` : Il est possible d'indiquer si l'accès à ce réseau doit passer ou non par le VPN.



- `Autoriser ce réseau à utiliser les DNS de Forward RVP/AGRIATES` : Si 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[p.702].

Configuration du MTU



La variable `Configurer manuellement le MTU` permet d'activer ou non le path MTU discovery[p.721] (paramètre : `/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.

Cette valeur peut poser problème, notamment avec le réseau virtuel privé (VPN), lorsque les paquets ICMP[p.715] 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 que l'accès à certains sites (ou certaines pages d'un site) n'aboutit pas (la page reste blanche) ou que les courriels n'arrivent pas dans le client 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.721] pour chacune des interfaces activées dans l'interface de configuration du module.

Si le champ n'est pas renseigné, la valeur par défaut est utilisée (1500 octets pour un réseau de type Ethernet).

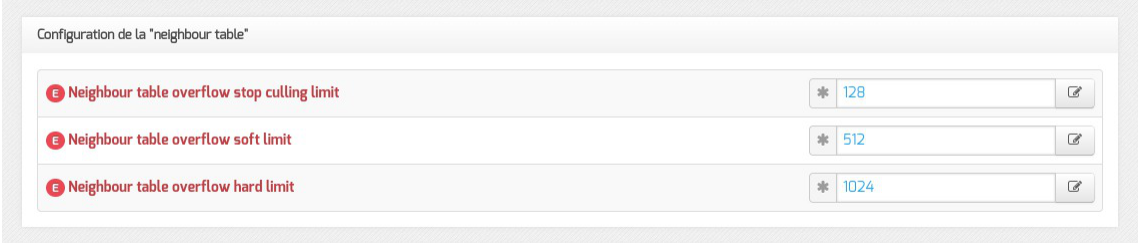


À partir de la version 2.7.0 du module Amon, le support du protocole PPPoE[p.727] comme méthode de connexion de l'interface externe est supprimé.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les commandes `ping`, `ip route` et `tracepath` sont utilisées pour ajuster les valeurs.

Configuration de la "neighbour table"



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

- **gc_thresh1** : seuil en-deçà duquel aucun recyclage des entrées de la table qui ne sont plus utilisées n'est effectué ;
- **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.

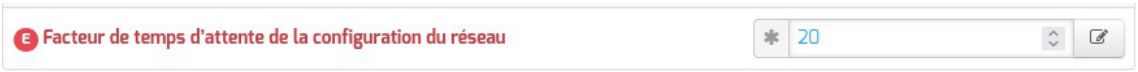
Test de l'accès distant



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.



La variable `Facteur de temps d'attente de la configuration du réseau` définit le nombre de cycles maximum dans la procédure de test de l'état des interfaces à partir du moment où l'état n'évolue plus.

Cette variable a été ajoutée suite à des remontées d'erreur concernant le service `netplan-wait-online` au `reconfigure` : https://dev-eole.ac-dijon.fr/issues/36181

Voir aussi...

Onglet Zones-dns : Configuration du DNS [p.273]

Résoudre des dysfonctionnements liés au MTU [p.550]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

4.12. Onglet Certificats ssl : gestion des certificats SSL

Afin de faciliter la mise en œuvre des certificats, leur gestion a été standardisée.

Le choix du type de certificat à mettre en place sur le serveur s'effectue dans l'onglet Général.

Certificat de type Let's Encrypt

L'autorité de certification[p.704] Let's Encrypt[p.717] permet de mettre en place, gratuitement, des certificats dont la distribution et le renouvellement sont automatisés.

Vous pouvez à présent gérer des certificats Let's Encrypt pour des serveurs accessibles depuis Internet ou au travers d'un proxy inverse.

Nom DNS supplémentaires



Il est possible de faire des requêtes supplémentaires pour d'autres noms DNS connus d'Internet que celui du serveur en renseignant la variable `Nom de domaines supplémentaires`.

> Il y aura autant de certificats supplémentaires que de noms DNS déclarés dans la variable `Nom de domaines supplémentaires`.

Paramètres du client Let's Encrypt

L'utilisation de certificats Let's Encrypt requiert l'utilisation de noms DNS connus d'Internet.

Le certificat sera créé avec le nom DNS résultant de la concaténation du nom de la machine et du nom de DNS du réseau local saisis dans l'onglet Général.

Seule la variable `Mode de fonctionnement du client Let's Encrypt` nécessite un paramétrage en fonction de l'accessibilité du serveur :

- accessible depuis Internet → utiliser la valeur `standalone` ;
- accessible au travers d'un proxy inverse → utiliser la valeur `webroot`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



1



le_config_dir

Chemin du répertoire du client Let's Encrypt

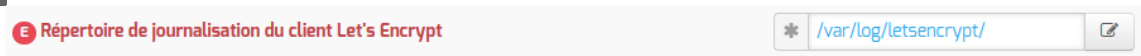
2



le_log_dir

Chemin du répertoire de travail du client Let's Encrypt

3



le_logs_dir

Chemin du répertoire de journalisation du client Let's Encrypt

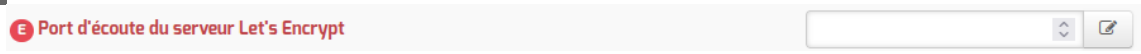
4



le_server_addr

Adresse du serveur Let's Encrypt

5



le_server_port

Port d'écoute du serveur Let's Encrypt

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

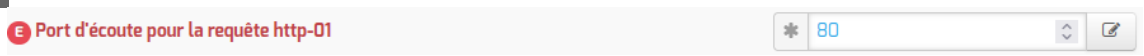
6



le_client_mode

Mode de fonctionnement du client Let's Encrypt

7



le_http_01_port

Port d'écoute pour http-01

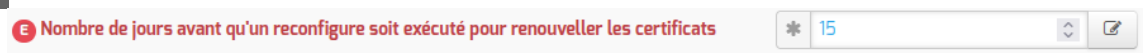
8



le_tls_sni_port

Port d'écoute pour TLS

9



le_expire_delay

Nombre de jours avant le déclenchement du renouvellement des certificats

Détail

- Les trois premiers points concernent l'emplacement des fichiers/données gérés par le client Let's Encrypt qui peuvent êtres modifiés.
- Les point 4 et 5 sont utiles dans le cas où vous souhaitez spécifier un serveur Let's Encrypt spécifique.
- Les points 7 et 8 permettent de modifier les ports associés aux défis `http-01` et `TLS-SNI`.
- Le point 9 permet de déclencher le renouvellement des certificats avant la fin de validité des certificats Let's Encrypt déjà acquis.

Mode Let's Encrypt

Le point 6 permet de spécifier le mode de fonctionnement de Let's Encrypt, soit :

- webroot
- standalone

Le choix du mode de vérification n'est pas anodin, et peut engendrer des effets de bord.

`webroot` : Obtenir un certificat en écrivant dans la racine d'un serveur web fonctionnel.

`standalone` : Obtenir un certificat en lançant un serveur web autonome (le port 80 doit être disponible)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour plus d'information consulter la documentation Let's Encrypt

Certificat de type manuel

Le type `manuel` vous permet d'utiliser le certificat de votre choix (en général, un certificat signé par une autorité tierce).

Pour que les services d'un module EOLE l'utilisent, il faut placer vos fichiers aux endroits définis au préalable dans la section `Choix du certificat SSL` de l'onglet `Général`.

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

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

Le répertoire `/etc/ssl/local_ca/` accueille uniquement des certificats CA.

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

Emplacement et contenu des fichiers

Chemin du fichier contenant le certificat SSL

Le certificat SSL est contenu dans un fichier au format PEM.

Ce fichier débute par la chaîne :

```
-----BEGIN CERTIFICATE-----
```

et se termine par :

```
-----END CERTIFICATE-----
```

Le chemin doit pointer vers le fichier contenant le certificat ainsi que les éventuels certificats intermédiaires.

Si la chaîne de certification du serveur contient une ou plusieurs autorités intermédiaires, vous devez concaténer le certificat du serveur avec les certificats des autorités intermédiaires en respectant l'ordre depuis la chaîne de certification vers l'autorité racine.

Construction du fichier avec plusieurs autorités intermédiaires

Soit la chaîne de certification suivante :

1. `CA-ROOT`
2. `CA-SUB1` signée par `CA-ROOT`
3. `CA-SUB2` signée par `CA-SUB1`
4. `mon-serveur` signé par `CA-SUB1`

Si le chemin du fichier contenant le certificat SSL est `/etc/ssl/cert/mon-serveur.crt`, les

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

différents certificats devront être concaténés dans l'ordre suivant :

```
cat mon-serveur.crt ca-sub2.crt ca-sub1.crt > /etc/ssl/cert/mon-serveur.crt
```

Chemin du fichier contenant la clé privée du certificat SSL

</etc/ssl/private/ca.key>

La clé privée débute par la chaîne :

`-----BEGIN RSA PRIVATE KEY-----`

et se termine par :

`-----END RSA PRIVATE KEY----`

Chemin du fichier contenant la chaîne de certification

Ce fichier est la concaténation du fichier du certificat (sans les intermédiaires) et de la clé privée.

Cette dernière est au format PEM et est généralement fournie dans un fichier avec l'extension `.pem`.

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.

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

Certificat de type autosigné

En mode `autosigné` le certificat est généré localement et signé par une autorité de certification[p.704] locale.

Paramètres SSL

Les variables de la section `Paramètres SSL` permettent de personnaliser la configuration OpenSSL[p.724] à utiliser pour générer les certificats auto-signés.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Taille de la clé

Cette variable permet de définir le paramètre `default_bits` de la section *`[req]`* du fichier de configuration d'OpenSSL.

Par défaut la taille de la clé est de 2048 bits.

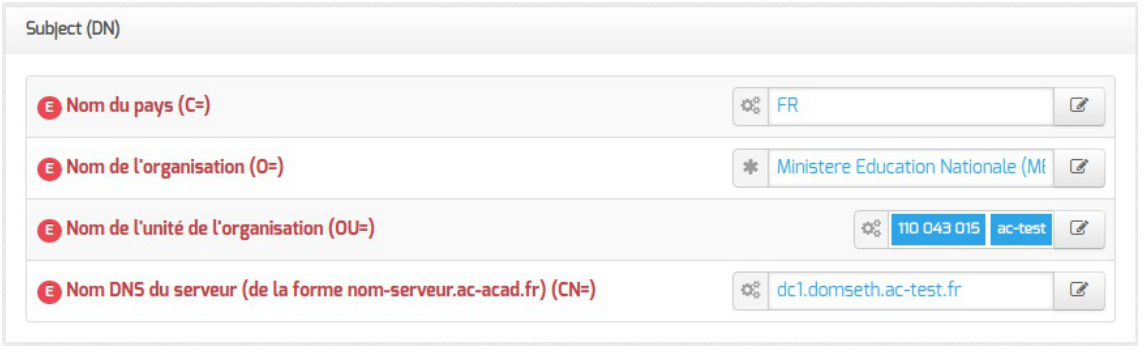
Durée de validité du certificat

Cette variable permet de définir le paramètre `default_days` des sections *`[ CA_default ]`* et *`[req]`* du fichier de configuration d'OpenSSL.

Par défaut la CA et les certificats générés expirent au bout de 3 ans (1096 jours).

Sujet du certificat

Les variables de la section `Subject (DN)` permettent de configurer le nom complet du serveur (distinguished name[p.709]) à utiliser pour générer les certificats auto-signés.



Nom du pays (C=)

Cette variable permet de définir le paramètre `countryName` de la section *`[req_distinguished_name]`* du fichier de configuration d'OpenSSL.

Il s'agit du code du nom de pays sur deux lettres, par défaut `FR` pour la France.

Nom de l'organisation (O=)

Cette variable permet de définir le paramètre `organizationName` de la section *`[req_distinguished_name]`* du fichier de configuration d'OpenSSL.

Il s'agit du nom de la structure, par défaut `Ministere Education Nationale (MENESR)` dans le cadre de l'Éducation Nationale.

Nom de l'unité de l'organisation (OU=)

Cette variable est utilisée pour ajouter des unités organisationnelles[p.734] dans le paramètre `organizationalUnitName` de la section *`[req_distinguished_name]`* du fichier de configuration d'OpenSSL.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La valeur par défaut `110 043 015` représente le numéro SIREN du Ministère de l'Éducation Nationale.

Nom DNS du serveur (CN=)

Cette variable permet de définir le paramètre `commonName` de la section `[req_distinguished_name]` du fichier de configuration d'OpenSSL.

Le CN[p.706] du serveur est pré-renseigné à l'aide des informations fournies dans l'onglet `Général`.



La commande suivante permet d'afficher les DN de l'émetteur et du sujet du certificat généré :

```
root@dc1:~# openssl x509 -in /etc/ssl/certs/eole.crt -noout -issuer
-subject
issuer=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043
015, OU = ac-test, CN = CA-dc1.domseth.ac-test.fr
subject=C = FR, O = Ministere Education Nationale (MENESR), OU = 110 043
015, OU = ac-test, CN = dc1.domseth.ac-test.fr
```

Nom DNS alternatif

La section `Nom Alternatif` de la machine permet de renseigner tous les noms DNS associés au serveur.



Nom DNS alternatif du serveur

Cette variable permet d'ajouter tous les noms DNS nécessaires dans la section `[ ALIASES ]` du fichier de configuration d'OpenSSL.

Elle doit notamment contenir les noms de domaine utilisés pour accéder aux applications web (l'EAD[p.710] par exemple).



Pour que les modifications soient prises en compte, il faut reconfigurer le serveur puis re-générer les certificats.

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
```

Re-génération des certificats

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Si les certificats auto-signés sont expirés ou si ils ne sont plus adaptés à la configuration du serveur, il est possible de les re-générer à l'aide de la commande suivante :

```
/usr/share/creole/gen_certif.py -f
```

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 signé par la CA locale, il est utilisé par les applications (apache, ead2, eole-sso, ...) ;
- `/etc/ssl/private/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`.



Les certificats émis par l'IGC/A[p.715] suivants sont déployés par défaut sur les modules EOLE :

- `menesr/igca.crt` pour le Ministère de l'Éducation nationale ;
- `medde/antsv3racine.crt` pour le Ministère de l'Ecologie, de l'Energie, du Développement durable et de la Mer.

Pour plus d'informations sur ces certificats, consulter le site de l'ANSSI[p.703] : https://www.ssi.gouv.fr/administration/services-securises/igca/certificats-emis-par-ligca-rsa-2(
.

Voir aussi...

Intégration d'un certificat et d'une chaîne d'authentification

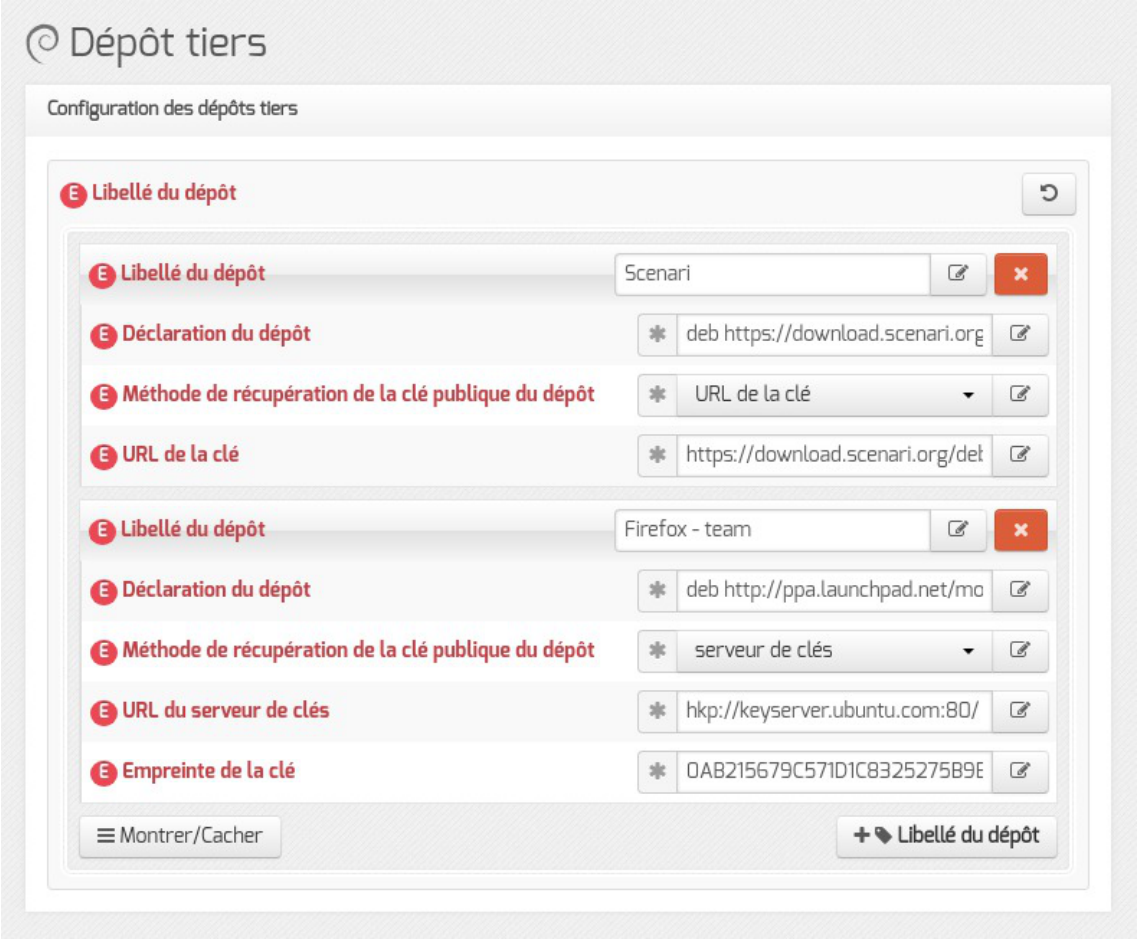
4.13. Onglet Dépôt tiers

L'utilisation de dépôts tiers permet d'ajouter de nouveaux paquets absents des dépôts officiels, ou de proposer des versions plus récentes.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> L'introduction de paquets tiers n'est pas sans risque et peut présenter des dangers pour votre système.

Cette onglet permet la prise en charge de dépôts de paquet de type `.deb`.



Un dépôt nouvellement configuré s'ajoute dans le fichier `/etc/apt/sources.list.d/additional.list`.

```
root@scribe:~# cat /etc/apt/sources.list.d/additional.list
#template genere par Maj-Auto
#
# dépôt Scenari
deb https://download.scenari.org/deb xenial main
# dépôt Firefox - team
deb http://ppa.launchpad.net/mozillateam/firefox-next/ubuntu xenial main
root@scribe:~#
```

L'ajout du dépôt est effectif après l'exécution de `Query-Auto` ou de `Maj-Auto`. L'installation d'un paquet supplémentaire s'effectue en ligne de commande.

Il est possible d'ajouter plusieurs dépôts en cliquant sur le bouton `+ Libellé du dépôt`.

La clé de signature d'un paquet permet de vérifier l'émetteur et l'intégrité du paquet, 2 méthodes sont disponibles pour récupérer la clé publique :

- serveur de clés ;
- URL de la clé.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Méthode de téléchargement de la clé publique : URL de la clé

Libellé du dépôt : `Scenari`

Déclaration du dépôt : `deb https://download.scenari.org/deb xenial main`

Méthode de récupération de la clé publique du dépôt : `URL`

URL de la clé : `https://download.scenari.org/deb/scenari.asc`

Méthode de téléchargement de la clé publique : serveur de clés

Libellé du dépôt : `Firefox - team`

Déclaration du dépôt : `deb http://ppa.launchpad.net/mozillateam/firefox-next/ubuntu xenial main`

Méthode de récupération de la clé publique du dépôt : `serveur de clés`

URL du serveur de clés : `hkp://keyserver.ubuntu.com:80/`

Empreinte de la clé : `0AB215679C571D1C8325275B9BDB3D89CE49EC21`

Si le serveur fonctionne conjointement avec le module Amon et que le proxy est activé, il faut paramétrer une exception pour le domaine du dépôt dans le champ `Liste des domaines de destination à ne pas authentifier` de l'onglet `Exceptions proxy`.

Prise en charge du nouveau dépôt

```
root@scribe:~# Query-Auto
Mise à jour le jeudi 13 avril 2017 11:01:17
*** scribe 2.6.1 (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
Configuration du dépôt Envole avec la source test-eole.ac-dijon.fr
Configuration du dépôt Scenari avec la source download.scenari.org
Configuration du dépôt Firefox - team avec la source ppa.launchpad.net
Action update pour root
Action list-upgrade pour root
Mise à jour OK
Aucun paquet à installer.
root@scribe:~#
```

Utiliser un fichier meta-release-lts alternatif

Le fichier `meta-release-lts` contient les adresses de tous les dépôts Ubuntu.

Dans un environnement sans accès direct à internet, on peut définir, via ce fichier, l'emplacement interne des dépôts à utiliser par `Upgrade-Auto`.

Dans l'interface de configuration du module, en mode expert, aller dans l'onglet `Dépôt tiers`.

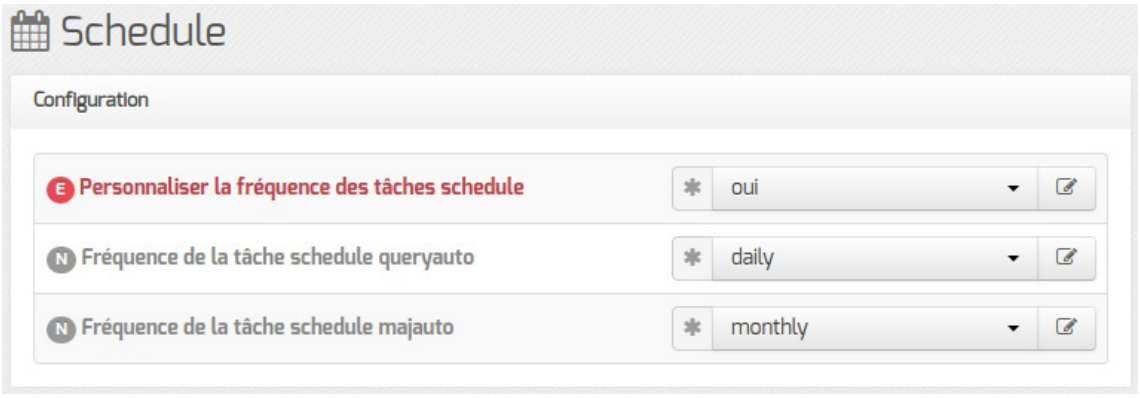


La variable `upgrade auto meta release repo` permet de définir où est téléchargé le fichier `meta-release-lts`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

4.14. Onglet Schedule

L'onglet `Schedule` permet de personnaliser la fréquence ou de désactiver les tâches eole-schedule[p.711] liées à la mise à jour.



La tâche schedule `queryauto` sert à vérifier la disponibilité des mises à jour. Il est possible de lui associer une notification par courriel dans l'onglet `Général`.

La tâche schedule `majauto` installe les mises à jour, reconfigure et redémarre le serveur si nécessaire. Une variable permet de désactiver le redémarrage automatique du serveur dans l'onglet `Général`.



Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

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

Présentation et mise en place de l'agrégation de routes IP

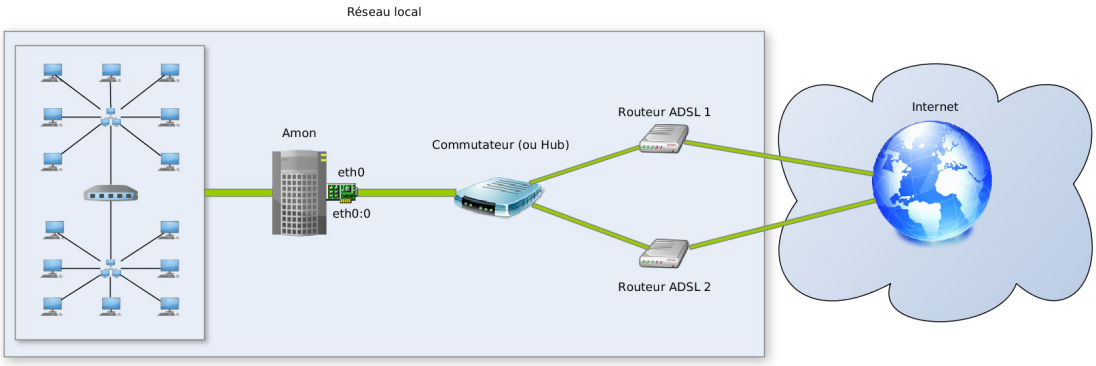
L'agrégation de routes IP (niveau 3) permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.

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

Dans ce cas :

- pas besoin d'utiliser les protocoles d'annonce de routes RIP[p.728] et OSPF[p.724] ;
- il faut un service qui surveille l'état de chacun des liens.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



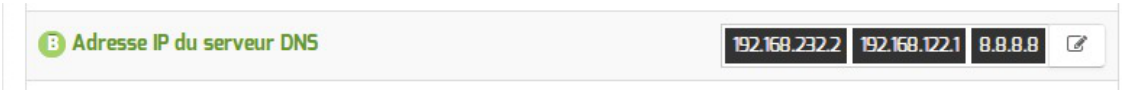
Il est nécessaire d'activer un alias sur l'interface réseau connectée sur l'extérieur pour utiliser ce service.

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

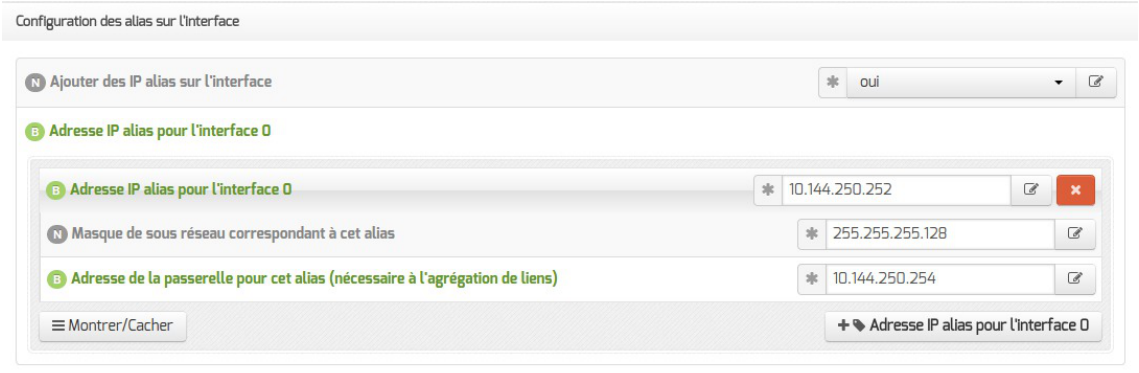
Dans la section `Adresse IP du serveur DNS` de l'onglet Général, ajouter les adresses des serveurs DNS de chacun des fournisseurs, en plaçant, de préférence, le DNS du premier lien en première position.



Onglet Interface-0

Il faut, en premier lieu, déclarer un alias sur l'interface 0 dans la section `Configuration des alias sur l'interface`.

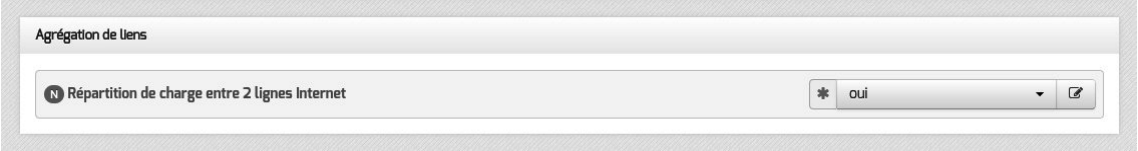
Les paramètres réseaux (IP, masque et passerelle) doivent être ceux attribués par le fournisseur d'accès du second lien.



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

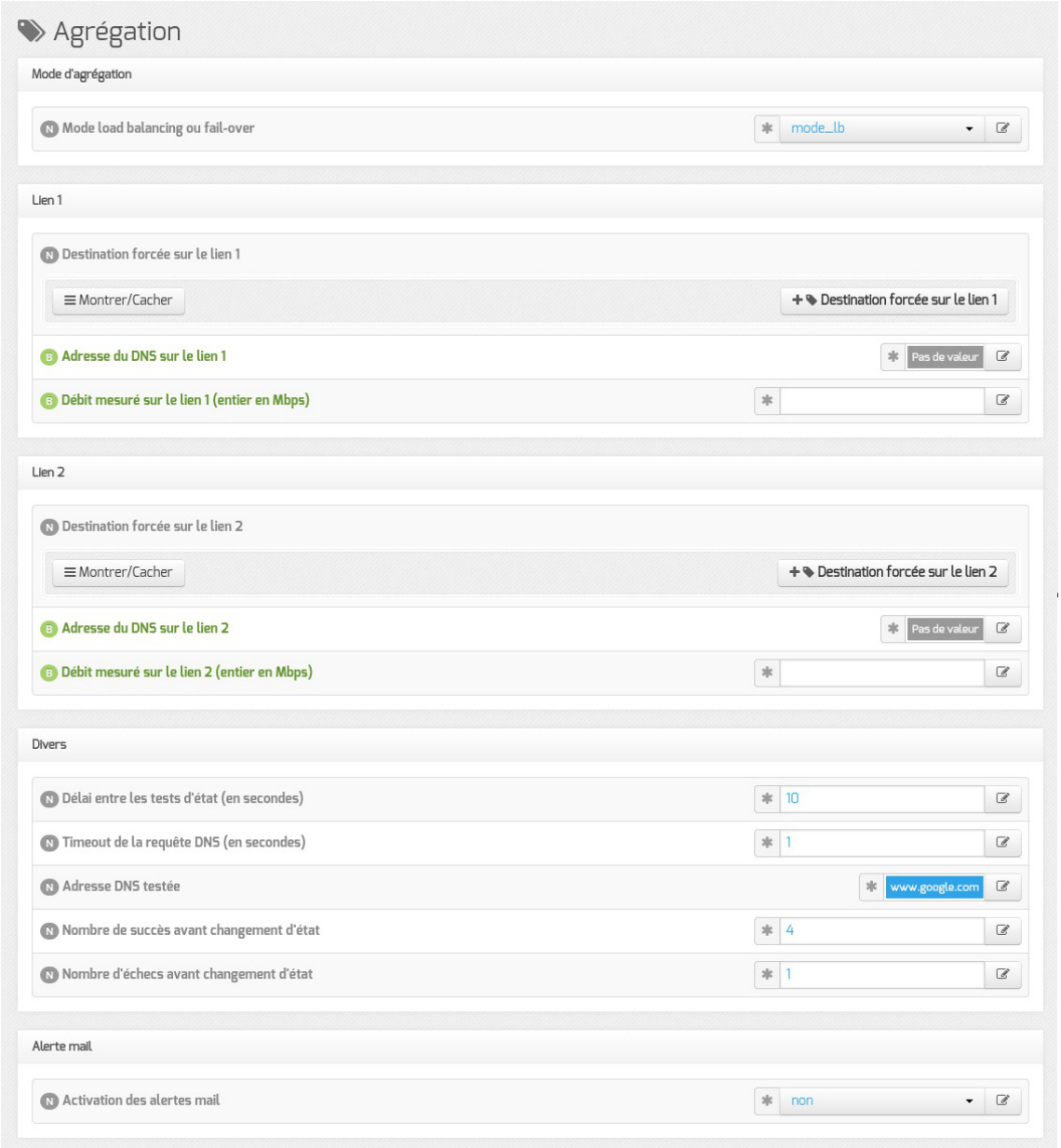
L'activation d'un alias IP, fait apparaître un nouveau paramètre, `Répartition de charge entre 2 lignes Internet`, qu'il faut passer à `oui`.



Un nouvel onglet, `Agrégation`, est disponible.

Onglet Agrégation : Configuration de l'agrégation de routes IP

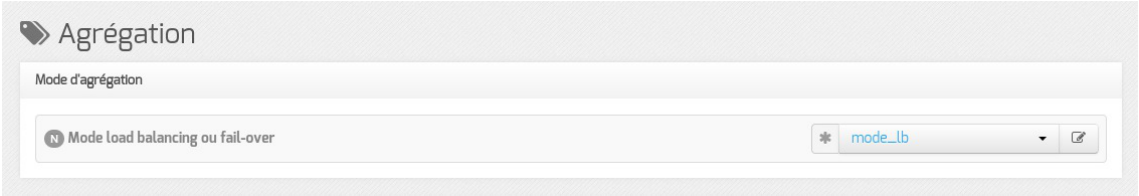
Pour avoir accès à l'onglet concernant l'agrégation, il faut avoir activé la `Répartition de charge entre 2 lignes Internet` dans l'onglet `Interface-0` comme expliqué précédemment.



Paramétrage de l'agrégation de liens

Modes d'agrégation

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Il existe deux modes d'agrégation :

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

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

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



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

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

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

Adresse des DNS

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



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

Adresse DNS testée

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



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

Alerte mail

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

Commandes

L'agrégation peut être suspendue et/ou relancée à l'aide du script `agregation` :

```
root@amon:~# agregation status
le service Agregation n'est pas démarré
root@amon:~#
```

L'option -h affiche l'aide de la commande :

```
root@amon:~# agregation -h
Usage: /usr/share/eole/sbin/agregation {start|stop|status|restart}
root@amon:~#
```

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

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

http://www.clamav.net

Activation de l'anti-virus

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

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

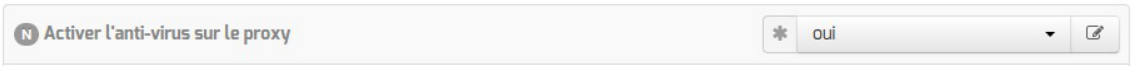


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

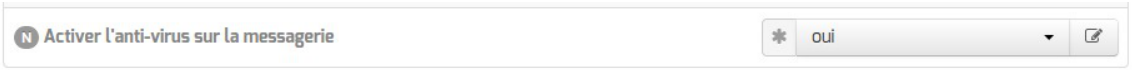


L'anti-virus sur le proxy permet d'analyser le trafic HTTP mais ne saurait en aucun cas remplacer la présence d'un anti-virus sur les postes clients.

L'anti-virus activé sur le proxy utilise beaucoup de ressources CPU[p.708]. Il peut donc affecter les performances du pare-feu et considérablement ralentir la navigation.

Activation de l'anti-virus sur la messagerie

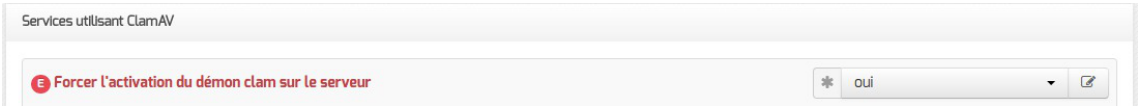
Pour activer l'anti-virus sur la messagerie il faut passer la variable `Activer l'antivirus sur la messagerie` à `oui` dans l'onglet `Clamav`.



Forcer l'activation du service clamd

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

Il est possible de forcer l'activation du service anti-virus (clamd) en passant la variable du mode expert `Forcer l'activation du démon clam sur le serveur` à `oui` dans l'onglet `Clamav`.



Configuration avancée du service anti-virus

En mode expert, l'onglet `Clamav` comporte de nombreuses variables qui permettent d'affiner la configuration du service anti-virus ClamAV.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- `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` ;
- `Profondeur maximale pour le scan des répertoires` ;
- `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.710] ;
- `Scan du contenu des fichiers PDF` ;
- `Scan des fichiers courriels` ;
- `Détection des fichiers exécutables corrompus` (déprécié par clamav et supprimé sur EOLE ≥ 2.9.0).

Configuration avancée du service de mise à jour de l'anti-virus

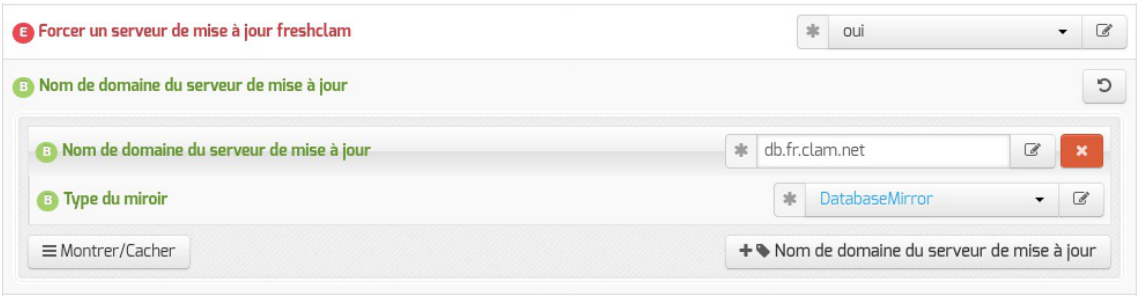
En mode expert, l'onglet `Clamav` comporte des variables qui permettent d'affiner la configuration de Freshclam, le service de mise à jour de la base de signatures.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- `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` permet de sélectionner le miroir le plus proche en se saisissant un code pays dans le cas où on n'ajoute pas manuellement de miroirs ;
- `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.

Passer `Forcer un serveur de mise à jour freshclam` à **oui** donne accès à un groupe de deux variables supplémentaires permettant de renseigner le nom de domaine d'un miroir et son type.



Lorsqu'un miroir est ajouté manuellement, il est nécessaire d'indiquer quel est son type : **DatabaseMirror** ou **PrivateMirror**. La distinction porte sur le protocole utilisé pour établir la connexion avec le miroir. **DatabaseMirror** implique l'utilisation du protocole **https** alors que **PrivateMirror** implique l'utilisation du protocole **http**.



L'établissement d'une connexion avec le protocole **https**, impliqué par le type **DatabaseMirror**, suppose que le certificat identifiant le miroir soit valide.

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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.728] comme étant des faux positifs.

4.17. Onglet Relai DHCP

Pour des raisons de sécurité, le service DHCP[p.708] n'a pas, à priori, à être installé sur le module Amon.

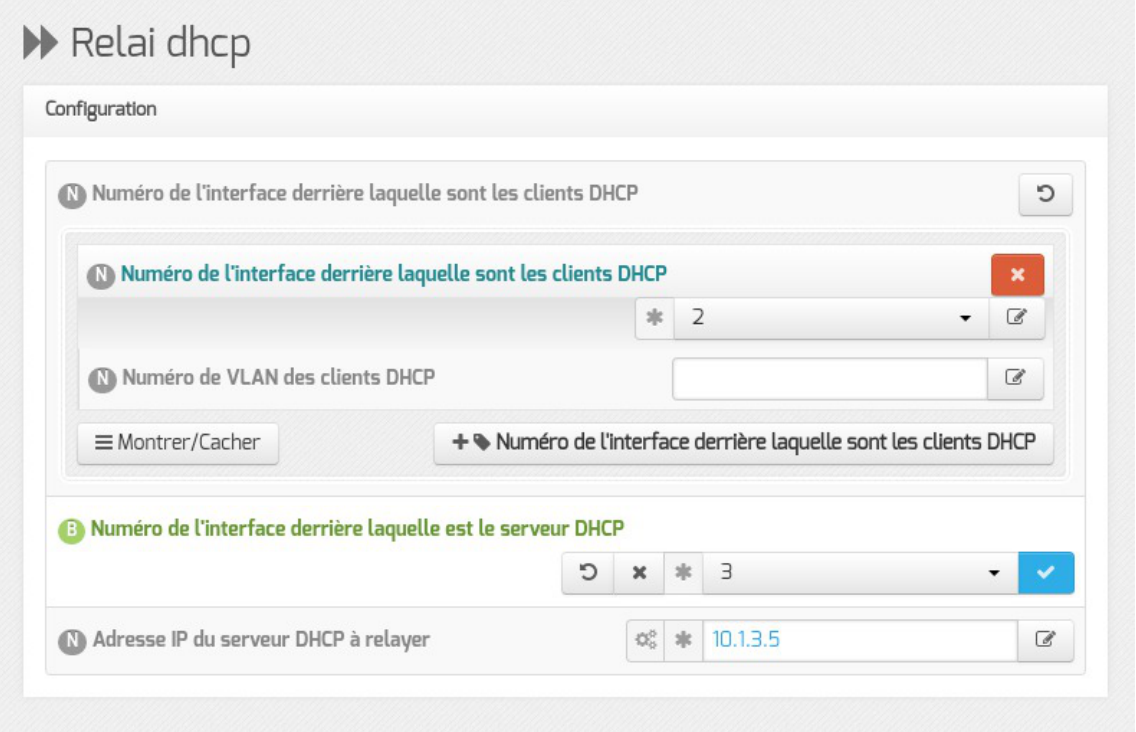
Il vaut mieux utiliser un autre module (module Scribe ou module Horus par exemple) pour fournir ce service.

Le protocole DHCP fonctionne en utilisant un mécanisme de broadcast[p.705].

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 (interface 3) vers le réseau pédagogique (interface 2).

Il est possible de restreindre le relayage sur un VLAN[p.734] 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> Amon, bien que déconseillée, est facilitée par le paquet `eole-dhcp`.

Voir aussi...

- eole-dhcp [p.569]
- Configuration du module Amon avec le module Scribe en DMZ [p.337]

4.18. Onglet Onduleur

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

Le logiciel utilisé pour la gestion des onduleurs est NUT[p.723]. 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.

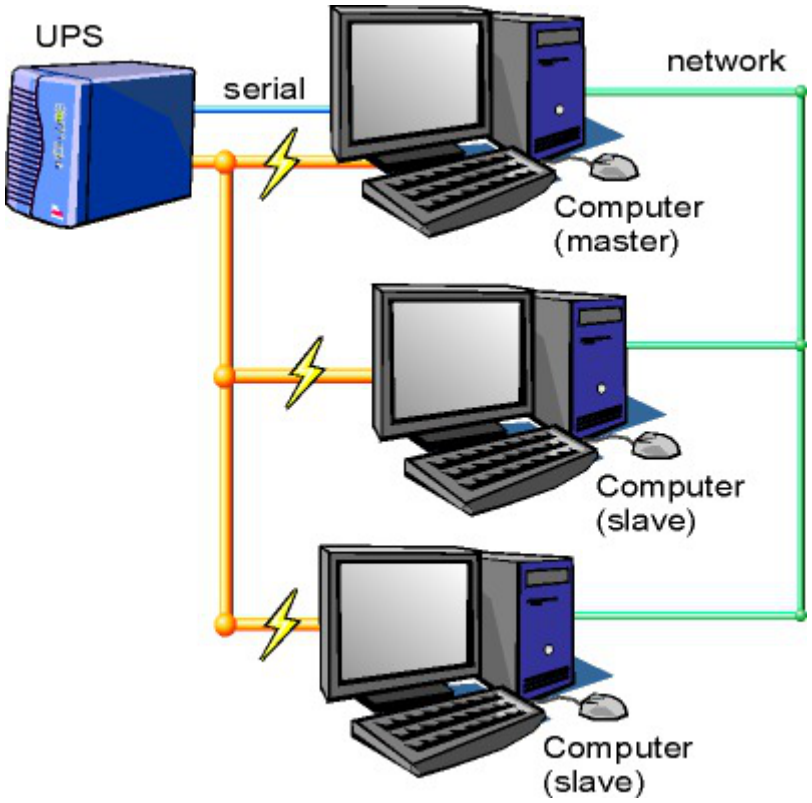


Schéma d'Olivier Van Hoof sous licence GNU FDL Version 1.2 - http://ovanhoof.developpez.com/upsusb/

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 :

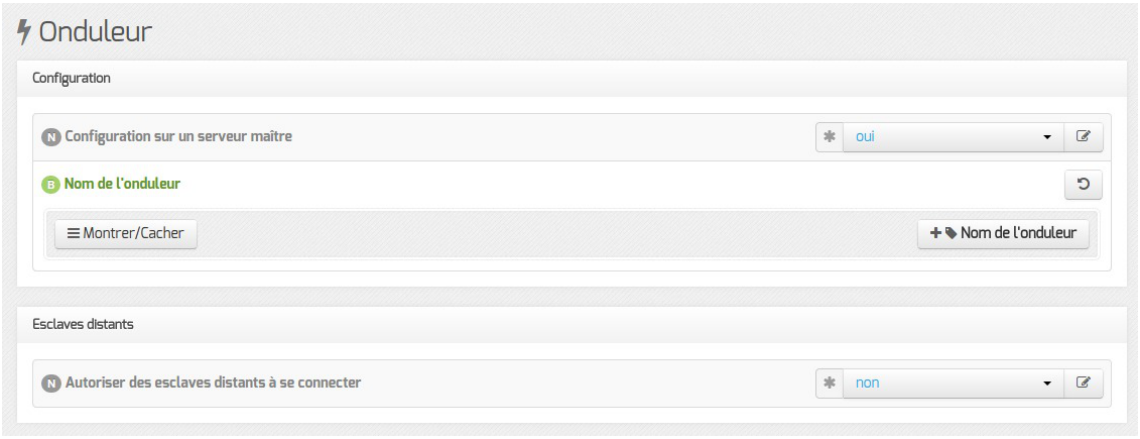
http://www.networkupstools.org/stable-hcl.html

> Pour connaître la version de NUT qui est installée sur le module :
>
> `# apt-cache policy nut`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

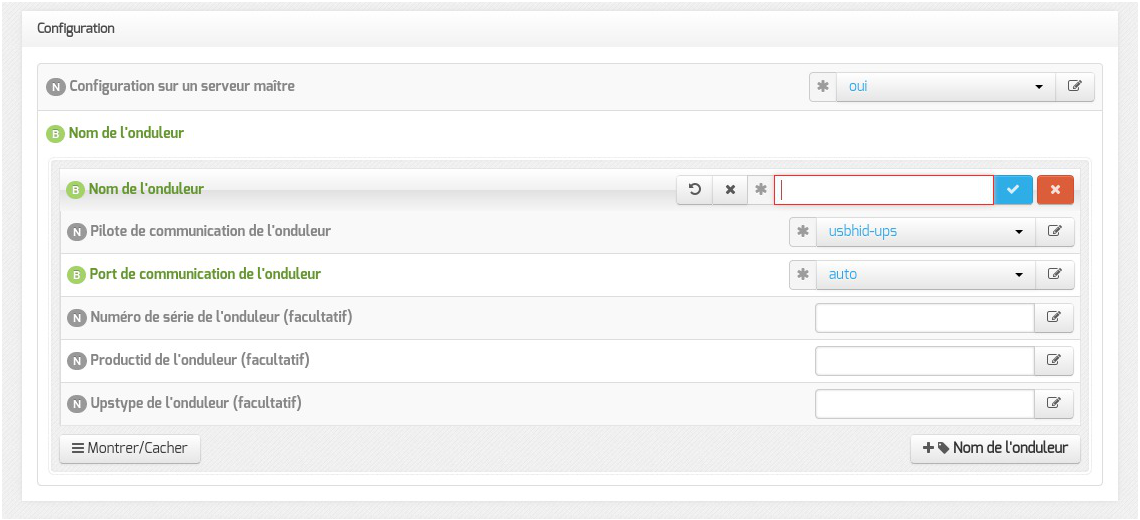
> ou encore :
>
> `# apt-show-versions nut`
>
> Si la version retournée est 2.7.1 on peut trouver des informations sur la prise en charge du matériel dans les notes de version à l'adresse suivante :
>
> http://www.networkupstools.org/source/2.7/new-2.7.1.txt
>
> Si le matériel n'est pas dans la liste, 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

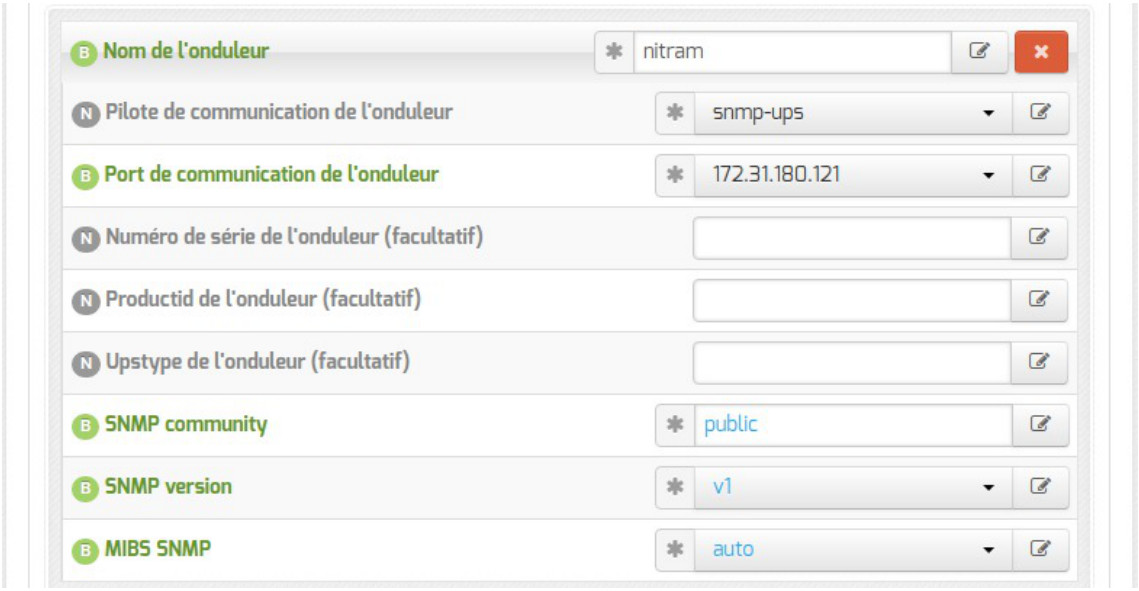
Les champs `Numéro de série de l'onduleur`, `Productid de l'onduleur` et `Upstype de l'onduleur` sont facultatifs si il n'y a pas de serveur esclave. Il n'est nécessaire d'indiquer ce numéro de série que dans le cas où le serveur dispose de plusieurs onduleurs et de serveurs esclaves.

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.

NUT SNMP

À partir d'EOLE 2.7.2, les onduleurs utilisant une connexion SNMP[p.731] (driver `snmp-ups`) sont gérés nativement et des variables supplémentaires apparaissent dans l'interface.

La configuration ci-dessous convient, par exemple, pour un onduleur NITRAM Cyberpower :



Si le driver `snmp-ups` est sélectionné, le paramétrage de la `Fréquence d'interrogation de upsmon` est également proposé mais en mode expert uniquement.

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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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`.

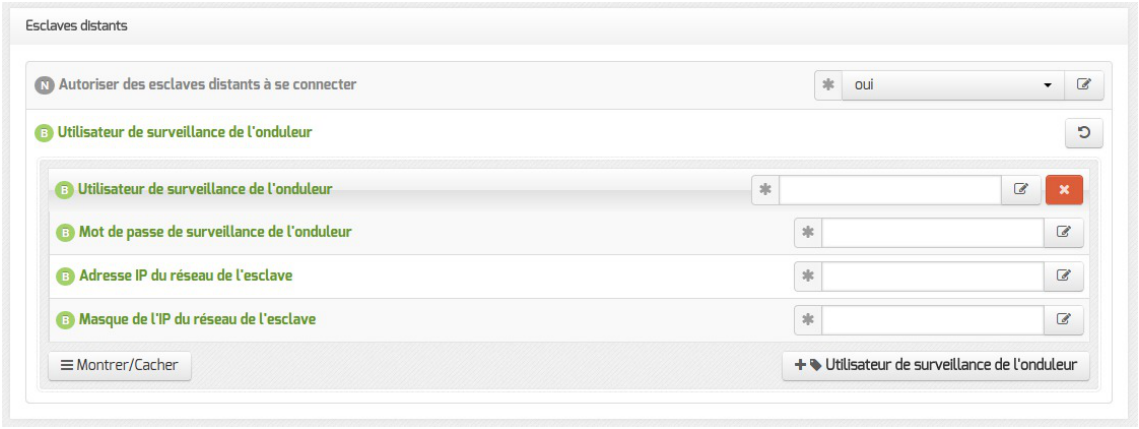
La majorité des onduleurs USB sont détectés automatiquement.

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 a se connecter avec cet utilisateur.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`

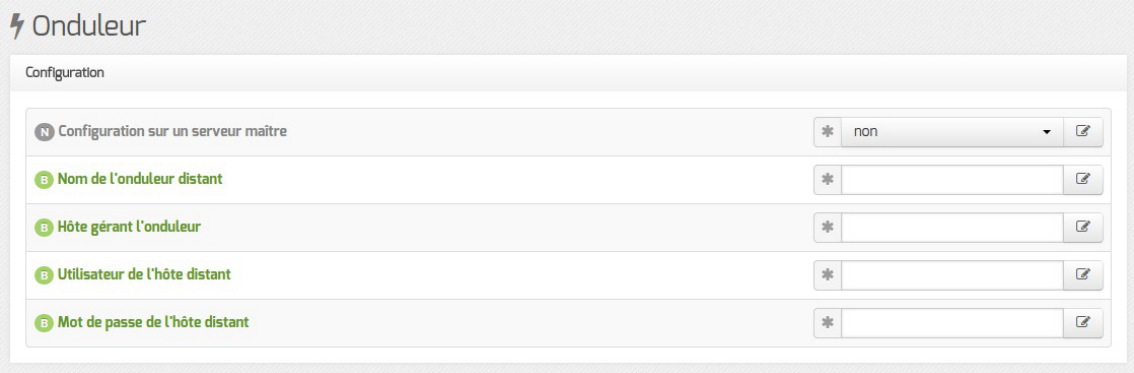
ou consulter la page web suivante : https://manpages.ubuntu.com/manpages/jammy/en/man5/ups.conf.5.html

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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).

À partir d'EOLE 2.7.2, il est possible de déclarer plusieurs onduleurs distants.

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 :

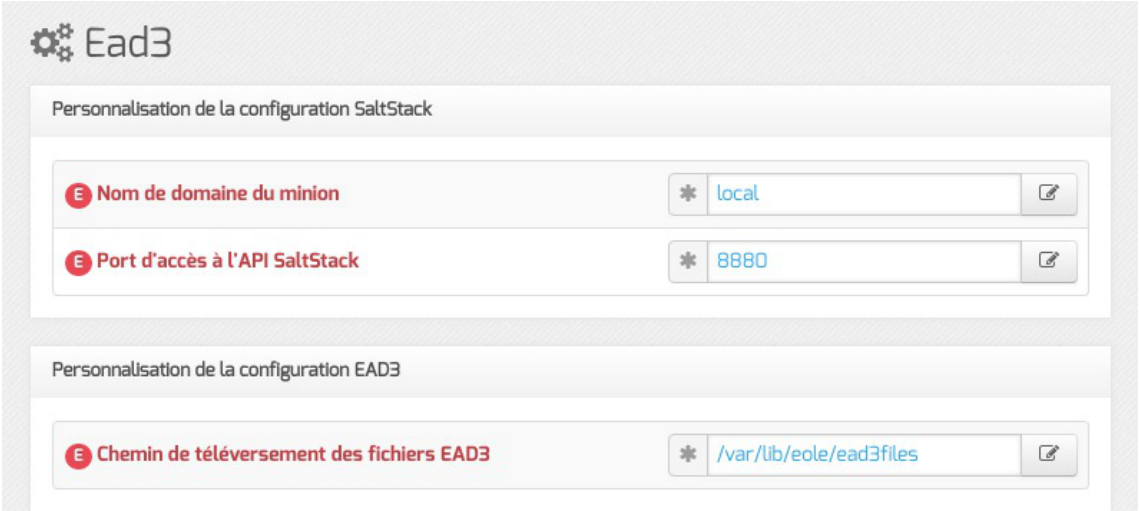
- Nom de l'onduleur distant : `eoleups` ;
- Hôte gérant l'onduleur : `192.168.30.10` ;
- Utilisateur de l'hôte distant : `scribe` ;
- Mot de passe de l'hôte distant : `99JJUE2EZOAI2IZI10IIZ93I187UZ8`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

4.19. Onglet Ead3

L'onglet `Ead3` est uniquement disponible après avoir passé `Activer l'interface d'administration du module (EAD3)` à `oui` dans l'onglet `Services`.

Il permet de personnaliser la configuration Saltstack[p.729] de l'EAD3.

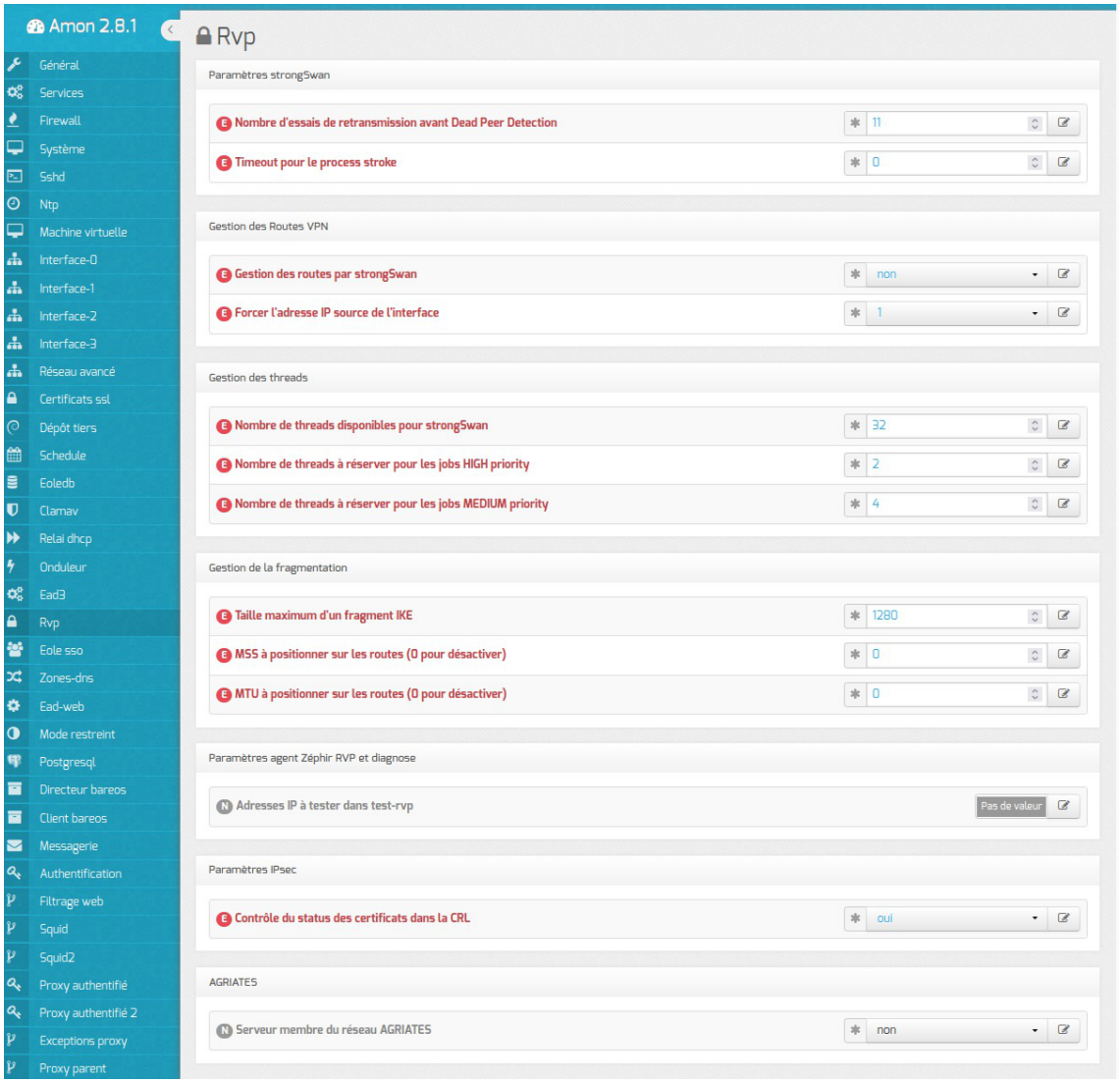


Le port d'écoute par défaut de l'API Saltstack est 8880.

Le choix du chemin de téléversement des fichiers EAD3 est par défaut `/var/lib/eole/ead3files`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

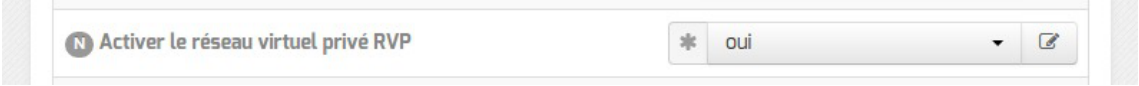
4.20. Onglet Rvp : Mettre en place le réseau virtuel privé



Le réseau virtuel privé[p.728] (RVP) peut être activé au moment de la configuration et de l'instanciation d'un module Amon ou sur un module 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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[p.702] 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.

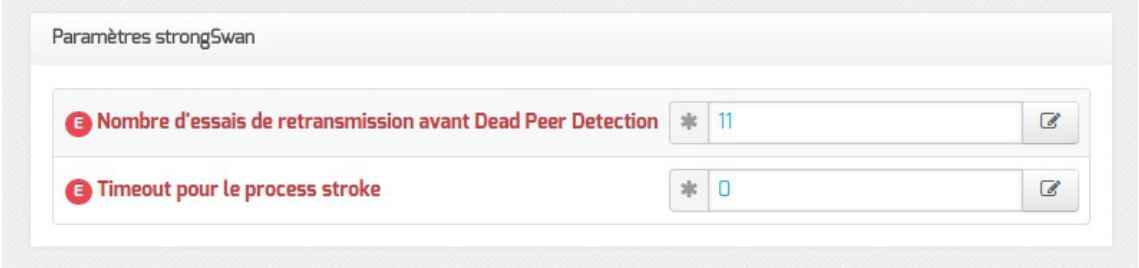
Paramètres propres au mode expert

Le mode Expert permet de personnaliser le fonctionnement de strongSwan[p.732].

`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



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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



`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.

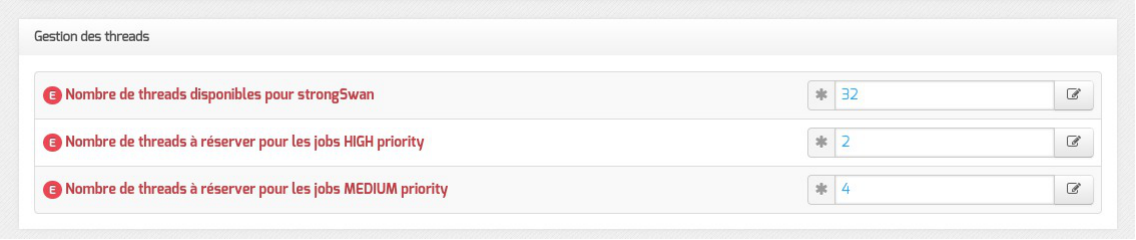
Exemple, dans notre cas et sur le module Amon uniquement :

/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 serveurs Amon afin d'éviter qu'ils utilisent aléatoirement l'adresse IP de l'une de ses interfaces lorsqu'ils passent dans un tunnel.

Avec la valeur `auto`, l'adresse IP source est définie automatiquement en fonction du réseau source.

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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Gestion de la fragmentation



`Taille maximum d'un fragment IKE` : valeur utilisée par strongSwan si la configuration IPSec est générée dans ARV avec l'activation de la fragmentation IKE ;

`MSS à positionner sur les routes (0 pour désactiver)` : valeur MSS[p.721] à positionner sur les routes (indépendant de la fragmentation IKE) ;

`MTU à positionner sur les routes (0 pour désactiver)` : valeur MTU[p.721] à positionner sur les routes (indépendant de la fragmentation IKE).

Paramètres IPsec



`Contrôle du status des certificats dans la CRL` : active ou non la vérification de la validité d'un certificat dans la liste de révocation (CRL[p.708]) ;

`Forcer l'encapsulation (Détection NAT)` :

- UDP/500 si valeur est à `non` et qu'il n'y a pas de NAT détecté ;
- UDP/4500 si valeur à `non` et qu'il y a du NAT détecté ou si valeur à `oui`.

`Autoriser le changement d'adresse IP d'une extrémité de connexion` :

- UDP/500 si valeur est à `non` ;
- UDP/4500 si valeur est à `oui`.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

Suppression du RVP

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

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

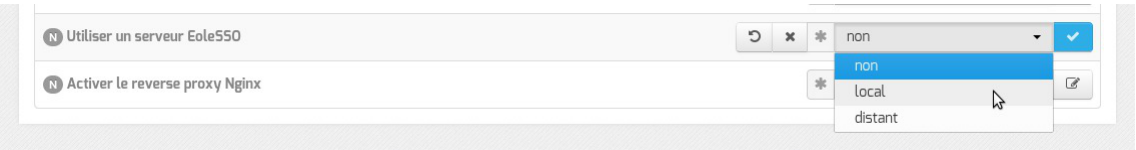
Le serveur EoleSSO est prévu pour être déployé sur un module EOLE.

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 SSO distant (configuration cliente).

Serveur EoleSSO local

À partir d'EOLE 2.9, l'outil EoleSSO s'exécute dans un conteneur[p.707] logiciel Podman[p.726].

L'image `eole-sso-server` est téléchargée depuis le site hub.eole.education [http://hub.eole.education].

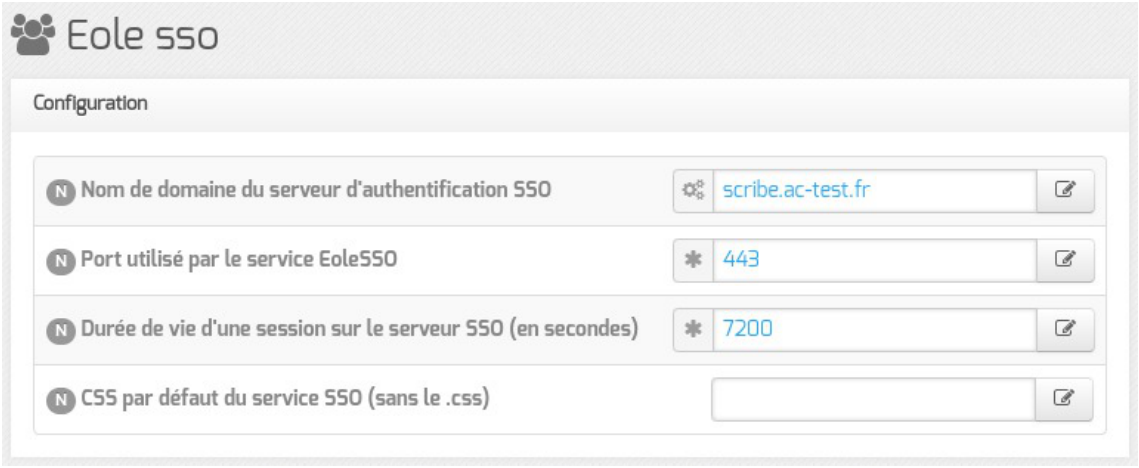
Le serveur doit donc pouvoir accéder à ce domaine au même titre qu'aux serveurs de mise à jour des modules.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Adresse et port d'écoute

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



Configuration d'un serveur EoleSSO local

- `Durée de vie d'une session (en secondes)` : indique la durée de validité d'une session SSO sur le serveur. Cela n'influence pas la durée de la session sur les applications authentifiées, seulement la durée de la validité du cookie utilisé par le serveur SSO. Au delà de cette durée, l'utilisateur devra obligatoirement se ré-authentifier pour être reconnu par le serveur SSO. Par défaut, la durée de la session est de 3 heures (7200 secondes).
- `CSS par défaut du service SSO (sans le .css)` : permet de spécifier une CSS différente pour le formulaire d'authentification affiché par le serveur EoleSSO. Le fichier CSS doit se trouver dans le répertoire `/usr/share/sso/interface/theme/style/<nom_fichier>.css`. *Se reporter au chapitre personnalisation pour plus de possibilités à ce sujet*.

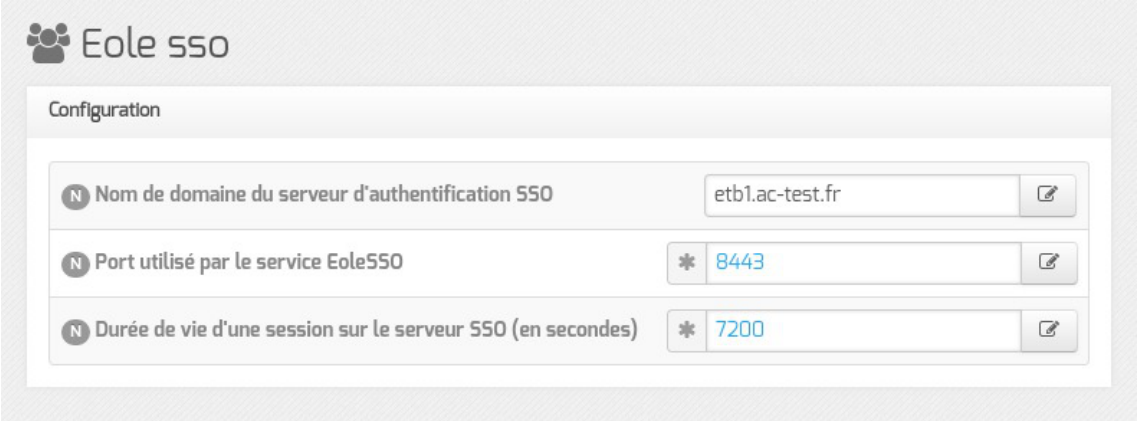
Port 443

Si le port HTTPS (`443`) est déclaré pour ce service, alors celui-ci est uniquement accessible via l'URL `https://<nom_du_serveur>/sso`.

L'URL de la forme `https://<nom du serveur>:<port>/` reste valable pour les autres valeurs de port que `443`.

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.

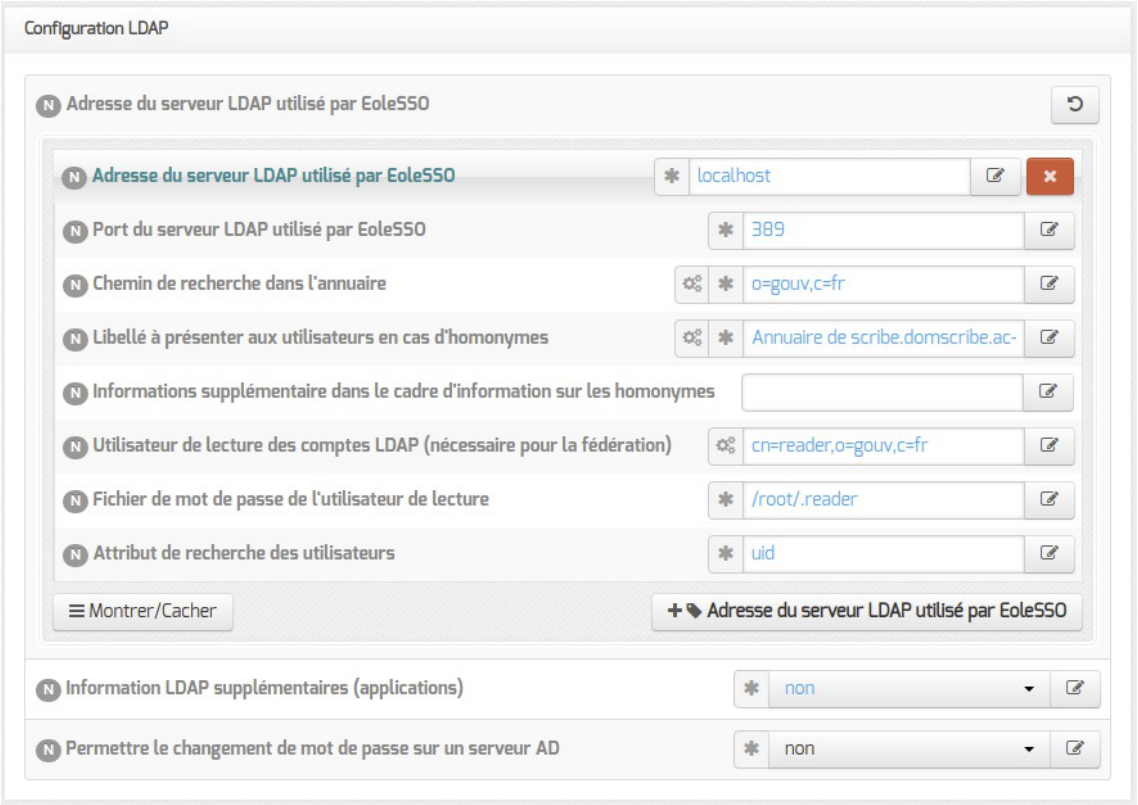
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Configuration d'un serveur EoleSSO distant

Configuration LDAP

Le serveur EoleSSO se base sur des serveurs LDAP[p.717] 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 (basedn) ;
- 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`) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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[p.709] 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.725] 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…).

Passer la variable `Permettre le changement de mot de passe sur un serveur AD` à `oui` permet à l'utilisateur de changer son mot de passe depuis la mire SSO si ce dernier à expiré.

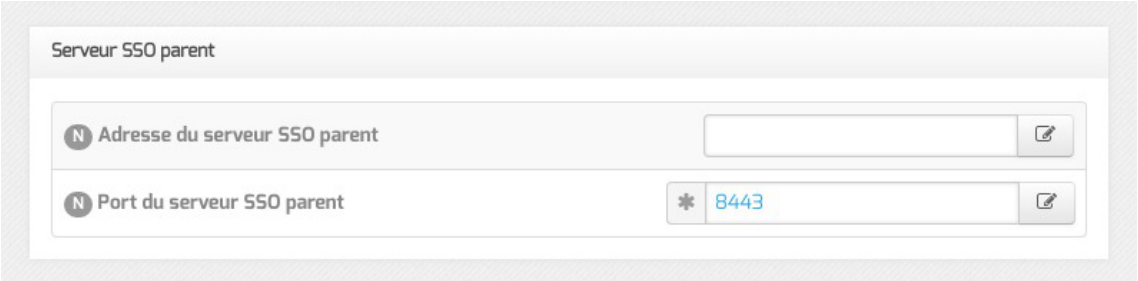
Il est alors nécessaire de renseigner le nom du domaine AD et le nom du serveur AD sur lequel changer le mot de passe.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Serveur SSO parent

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



Si un utilisateur n'est pas connu dans le référentiel du serveur EoleSSO, le serveur essayera de l'authentifier auprès de son serveur parent (dans ce cas, la liaison entre les 2 serveurs s'effectue par l'intermédiaire d'appels XML-RPC[p.735] en HTTPS, sur le port défini pour le serveur EoleSSO).

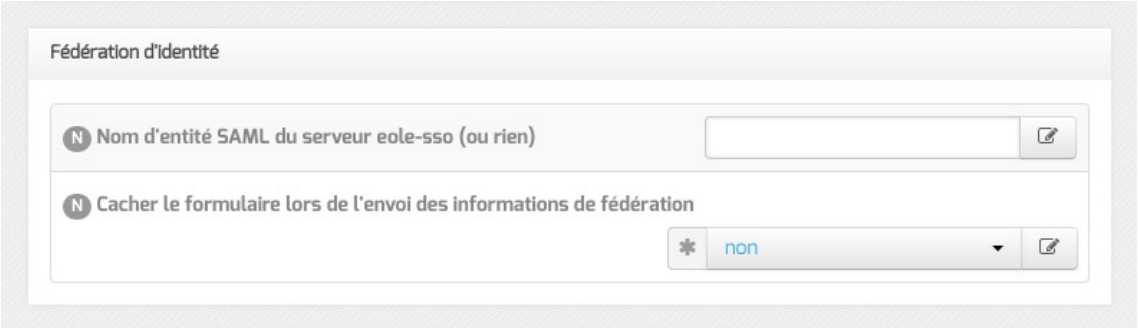
Si le serveur parent authentifie l'utilisateur, il va créer un cookie de session local et rediriger le navigateur client sur le serveur parent pour qu'une session y soit également créée (le cookie de session est accessible seulement par le serveur l'ayant créé).



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.

Fédération d'identité

Le serveur EoleSSO permet de réaliser une fédération vers un autre serveur EoleSSO ou vers d'autre types de serveurs compatibles avec le protocole SAML[p.730] (version 2).



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

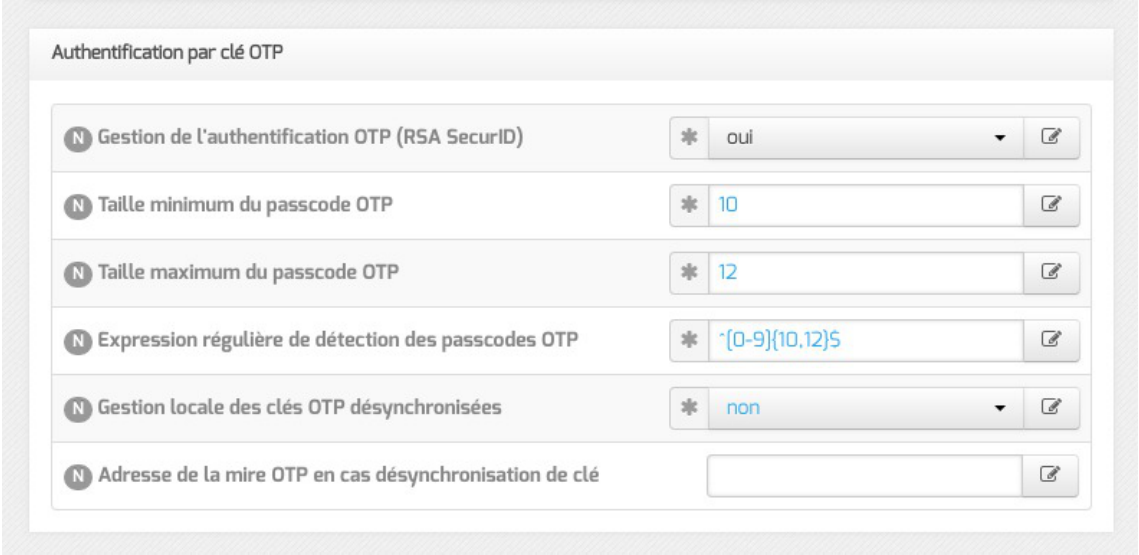
`Cacher le formulaire lors de l'envoi des informations de fédération` : permet de ne pas afficher le formulaire de validation lors de l'envoi des informations de fédération à un autre système. Ce formulaire est affiché par défaut et indique la liste des attributs envoyés dans l'assertion SAML permettant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

Authentification OTP

Il est possible de configurer EoleSSO pour gérer l'authentification par clé OTP à travers le protocole

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

securID[p.730] 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 :

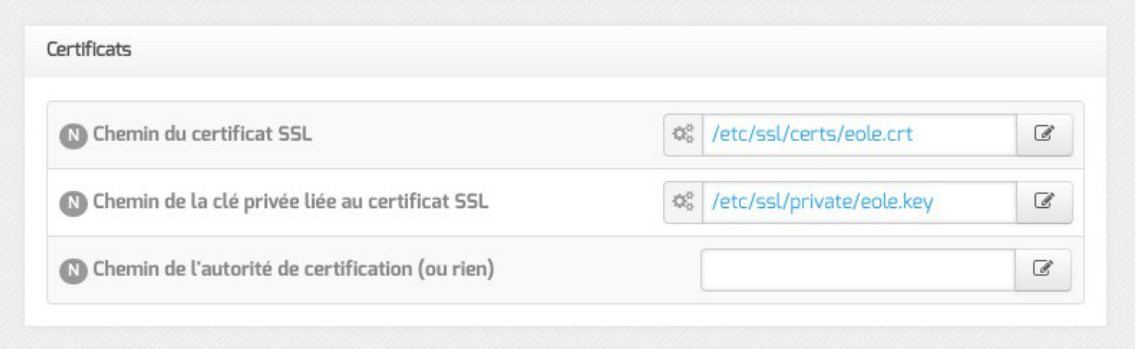
- Pour chaque annuaire configuré, un champ permet de choisir la manière dont les identifiants à destination du serveur OTP sont gérés. '`inactifs`' (par défaut) indique que l'authentification OTP n'est pas proposée à l'utilisateur. Avec `'identiques'`, le login local (LDAP) de l'utilisateur sera également 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.716] du serveur et sont utilisés par défaut.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



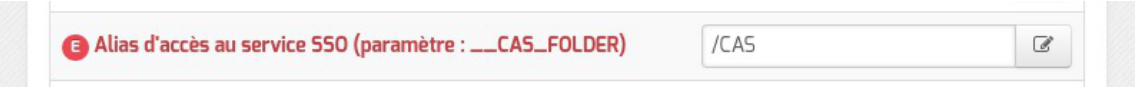
Il est possible de renseigner un chemin vers une autorité de certification et un certificat serveur dans le cas de l'utilisation d'autres certificats (par exemple, des certificat signés par une entité reconnue).

Les certificats doivent être au format PEM.

Configuration en mode expert

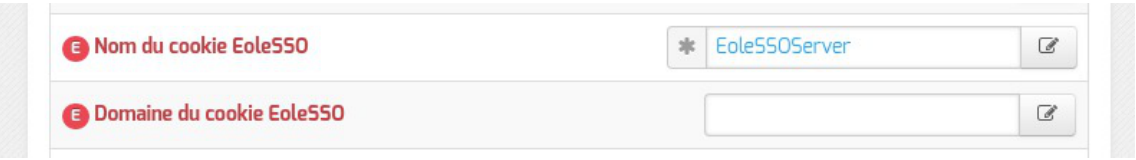
Autres options

En mode expert plusieurs nouvelles variables sont disponibles :

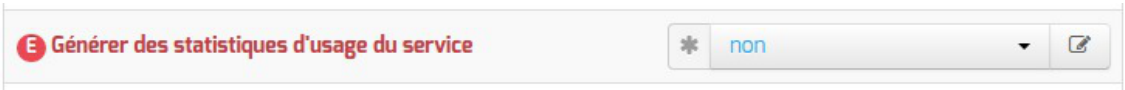


- `Alias d'accès au service SSO (paramètre : __CAS_FOLDER)` permet de créer un alias spécifique en plus du domaine et du port pour certains serveurs SSO tels que lemonLDAP[p.717] ou keycloak[p.717].

  Cette variable est disponible uniquement à partir de la version 2.6.2 d'EOLE.

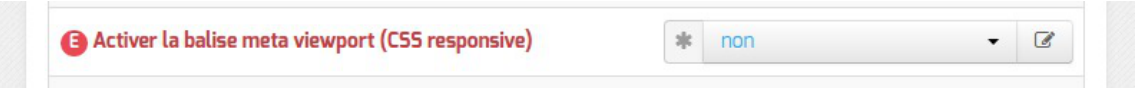


- `Nom du cookie EoleSSO` et `Domaine du cookie EoleSSO` permettent la gestion d'un cluster EoleSSO.



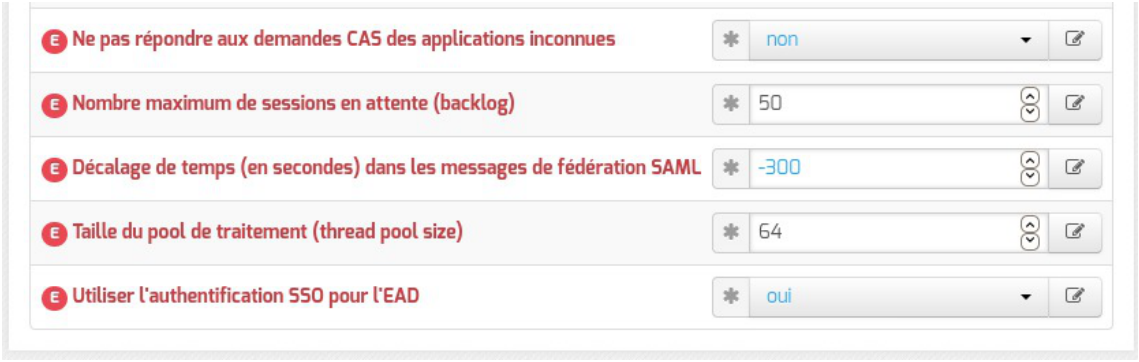
- `Générer des statistiques d'usage du service` est à `non` par défaut.

  Si ce paramètre est à `oui`, EoleSSO 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 disponibles 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- `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 ;

- `Nombre maximum de sessions en attente (backlog)` permet de définir la taille de la file d'attente des sessions.

  Augmenter cette valeur est susceptible de résoudre des problèmes de lenteur voir de rejet des demandes d'authentification ;

- `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 ;

- `Taille du pool de traitement (thread pool size)` permet de configurer la valeur du paramètre THREAD_POOL_SIZE.

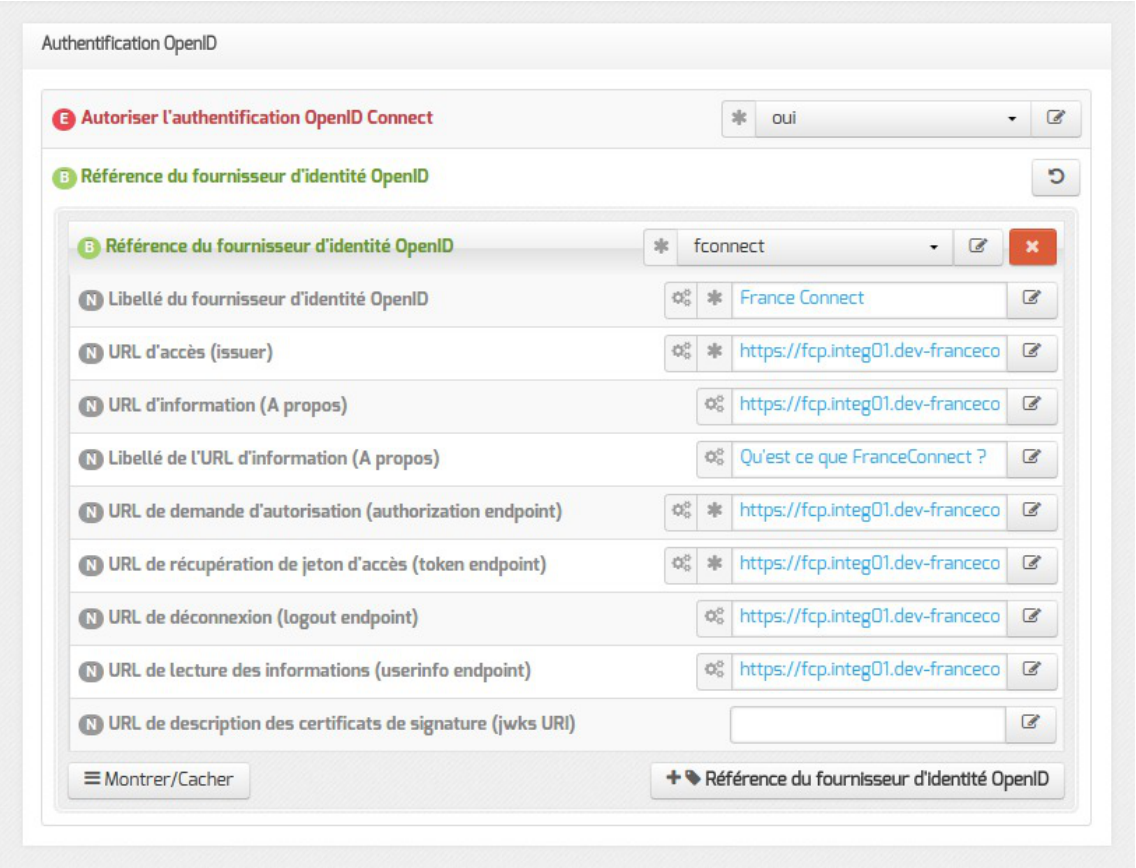
  Augmenter cette valeur est susceptible de résoudre les problèmes de charge rencontrés sur certaines infrastructures ;

- `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.

Authentification OpenID Connect

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- `Autoriser l'authentification OpenID Connect` est à `non` par défaut

  Si ce paramètre est à `oui`, il devient possible de configurer un ou plusieurs fournisseurs d'identité OpenID Connect ;
- `Référence du fournisseur d'identité OpenID` : renseigner un libellé pour identifier le fournisseur. Ce libellé est interne à l'application EoleSSO. Il est utilisé pour définir le nom des fichiers contenant les logos/boutons du fournisseur :
  - `/usr/share/sso/interface/images/<libelle>.png` : bouton de connexion présenté sur la page de login (par exemple : "se connecter avec France Connect") ;
  - `/usr/share/sso/interface/images/logo-<libelle>.png` : logo du fournisseur qui sera affiché sur la page d'association de comptes.
- `Libellé du fournisseur d'identité OpenID` : libellé à destination des utilisateurs pour décrire le fournisseur ("France Connect", "Google", ...) ;
- `URL d'accès (issuer)` : URL décrivant le fournisseur d'identité (la plupart du temps, l'URL de base de son service d'authentification) ;
- `URL de demande d'autorisation (authorization endpoint)` : URL permettant au client d'initier le processus d'authentification ;
- `URL de récupération de jeton d'accès (token endpoint)` : URL permettant de récupérer un jeton (éventuellement l'identifiant de l'utilisateur) après authentification ;
- `URL de déconnexion (logout endpoint)` : URL permettant de demander une déconnexion. Ce paramètre est ignoré pour les fournisseurs utilisant une cinématique de déconnexion spécifique comme Google, Facebook et Microsoft ;
- `URL de lecture des informations (userinfo endpoint)` : URL permettant de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

récupérer les informations de l'utilisateur à l'aide du jeton fourni ;

- `URL de description des certificats de signature (jwks URI)` : URL décrivant les certificats utilisés par le fournisseur (si disponible) ;

Définition de l'identifiant client (Client ID) et clé secrète (Client secret)

L'identifiant client (Client ID) et la clé privée secrète (Client secret) renvoyés par le fournisseur d'identité utilisés pour valider les échanges doivent être, pour des raisons de sécurité, stockés dans un fichier à part avec des droits restreints.

Pour chaque fournisseur d'identité, ajouter une ligne dans le fichier `/etc/eole/eolesso_openid.conf` :

```
<nom_fournisseur> = "<client id> :<client secret>"
```

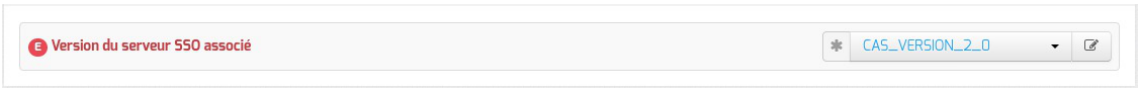
Le `nom_fournisseur` doit correspondre au paramètre `Référence du fournisseur d'identité OpenID` renseigné dans l'interface de configuration du module.

Si ces informations ne sont pas renseignées pour l'un des fournisseurs déclarés, un message l'indiquera au lancement de la commande `diagnose`.

Version du serveur SSO

Si le module est configuré pour utiliser le serveur SSO local, le protocole utilisé sera forcément CAS[p.705] version 2.

Si le module est configuré pour utiliser un serveur SSO distant, la variable `Version du serveur SSO associé` permet de choisir entre le protocole historique CAS et le protocole SAML[p.730] en version 1.1.



Dans le cas où le serveur SSO est déclaré en SAML, de nouvelles variables permettent de déclarer les correspondances (mapping) permettant de récupérer les principaux attributs des utilisateurs parmi celle transmises par le serveur.



Voir aussi...

Gestion des sources d'authentification multiples

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Compatibilité OpenID Connnect

4.22. Onglet Zones-dns : Configuration du DNS

EOLE propose un serveur DNS[p.709] 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 les modules Amon et 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

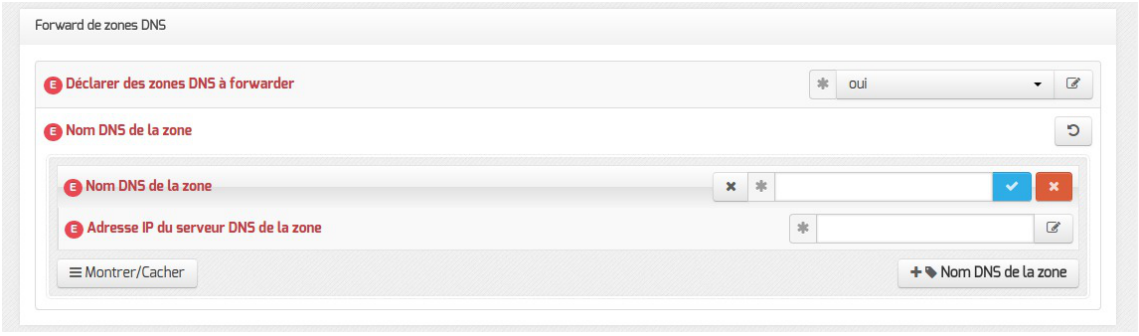
Le champ `Nom de domaine local supplémentaire ou rien` permet au serveur DNS de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.728]) est activé et configuré sur le serveur et que le serveur est membre du réseau privé de l'Éducation nationale (AGRIATES[p.702]), il devient possible de déclarer, dans l'onglet `Rvp`, le DNS interne à utiliser pour résoudre les noms de domaines.



L'onglet Rvp

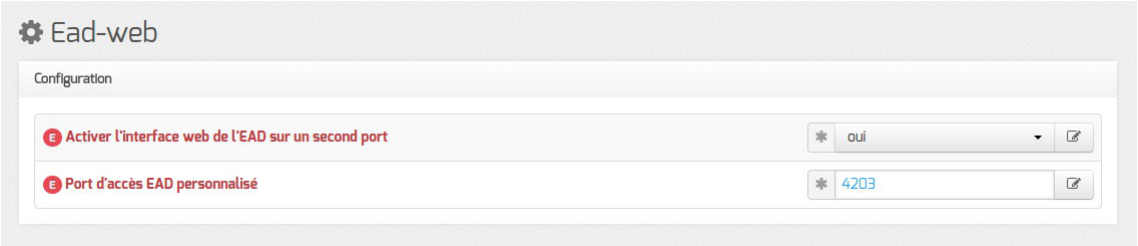
Il est possible de renseigner un ou plusieurs serveurs DNS AGRIATES dans le champ `Adresse du DNS permettant de resoudre les in.ac-acad.fr`. Des relais de zones "AGRIATES" sont prédéfinis et correspondent aux zones *in* du domaine académique. D'autres relais de zone pour le DNS AGRIATES peuvent être ajoutés dans le champ `Nom DNS de la zone resolue par le DNS AGRIATES`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La configuration des zones DNS AGRIATES est enregistrée dans le fichier templatisé : /etc/bind/agriates.zones.

4.23. 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.339]

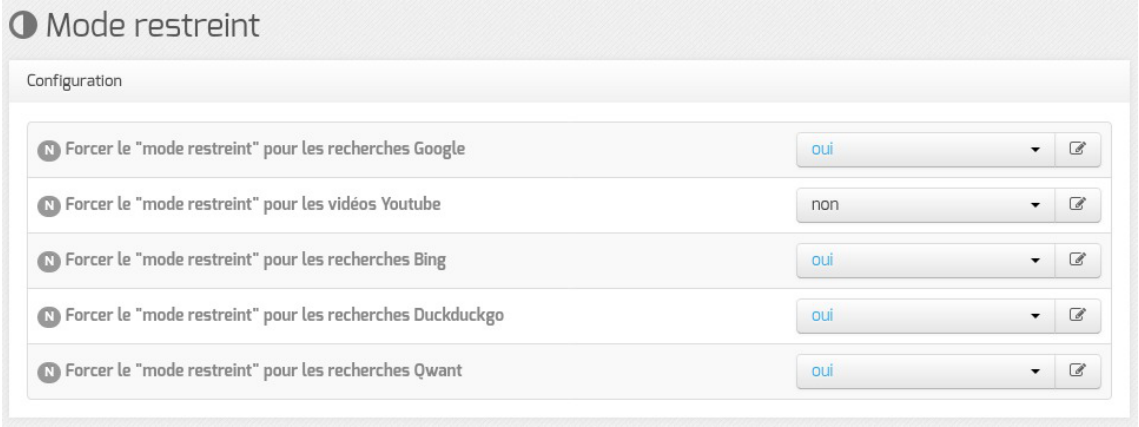
4.24. Onglet Mode Restreint : Configuration des restrictions de navigation

Le mode restreint ou safe search[p.729] permet d'activer la navigation restreinte, soit bloquer les contenus "sensibles" pour les utilisateurs du domaine.

Les différentes cibles du mode restreint

L'activation du mode restreint s'effectue dans l'onglet Mode restreint.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Il est possible d'activer le mode restreint pour certaines applications

- `Forcer le "mode restreint" pour les recherches Google` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Google ;
- `Forcer le "mode restreint" pour les vidéos Youtube` : bloque les contenus à caractères sensibles pour les vidéos Youtube ;
- `Forcer le "mode restreint" pour les recherches Bing` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Bing ;
- `Forcer le "mode restreint" pour les recherches Duckduckgo` : bloque les contenus à caractères sensibles pour les résultat de recherche sur Duckduckgo ;
- `Forcer le "mode restreint" pour les recherches Qwant` : bloque les contenus à caractères sensibles pour les résultats de recherche sur Qwant ;

Sur les versions précédentes, la mise en œuvre du mode restreint s'appuyait sur des réécritures d'URL gérées directement dans le logiciel de filtrage e2guardian[p.710].

À partir d'EOLE 2.8.1, ce sont des redirections DNS[p.709] qui sont utilisées. Cela nécessite d'avoir la main sur ce service, ce qui n'est pas le cas sur le module `Eolebase+Proxy`.

4.25. 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 courriers électroniques.

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

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

Serveur d'envoi/réception (SMTP)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 d'envoi pour le compte root`, saisir l'adresse que l'on souhaite utiliser pour l'envoi de courriers électroniques depuis le compte root.
- `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.
- `Taille maximale d'un message à envoyer en Mo`, indiquer la taille maximale des courrier électroniques qui seront envoyés par exim.



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

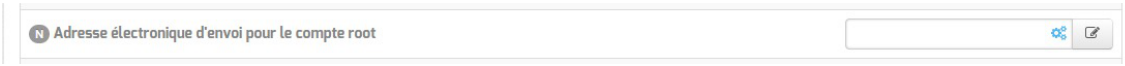
Dans le cas contraire les courriers électroniques utilisant le nom de domaine de la messagerie de l'établissement seront réécris et envoyés à l'adresse électronique d'envoi du compte root.

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



Dans le cas où le `Nom de domaine de la messagerie de l'établissement` n'est pas le même que la concaténation du `Nom de la machine` et du `Nom DNS du réseau local`, il peut être nécessaire d'activer la réécriture des en-têtes (cf. Onglet Messagerie) [p.276] pour avoir des informations cohérentes avec l'enveloppe des courriels.

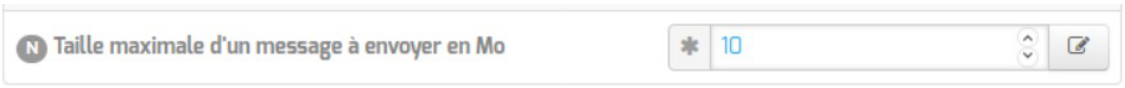
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.



Il est également possible de configurer la taille maximale des messages électroniques.



Sur les modules utilisant le webmail Roundcube, elle ne devrait pas dépasser la taille maximale d'un fichier à charger définie pour Apache.

En mode expert, il est possible d'écraser les en-têtes 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. 707] si l'expéditeur utilise la configuration définie dans `/etc/mailname`

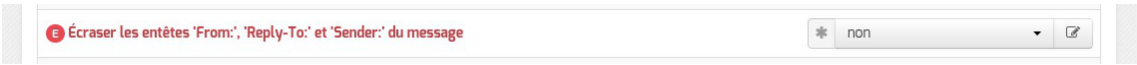
Si la valeur de `%%nom_domaine_local` est différente de la valeur de `%%domaine_messagerie_etab`, alors on force les formes suivantes pour le maître et les conteneurs uniquement :

- `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.

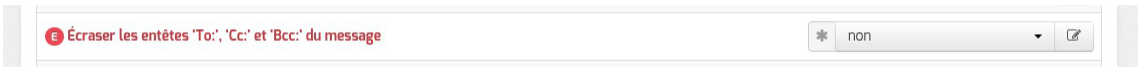
Les adresses expéditeurs et destinataires systèmes sont ensuite réécrites selon les tableaux suivants en fonction de variables expertes :

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



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `system mail to for headers` : écraser les en-têtes « To: », « Cc: » et « Bcc: » du message, par défaut à `non`



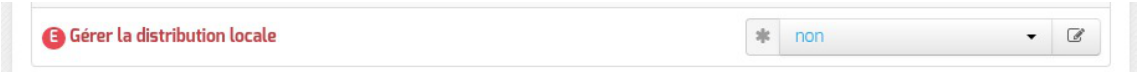
Réécriture de l'expéditeur :

	system_mail_from_for_headers = non	system_mail_from_for_headers = oui
MAIL FROM	system_mail_from	system_mail_from
From :	user@conteneur.machine.domaine	system_mail_from
Reply-To :	user@conteneur.machine.domaine	system_mail_from
Sender :	user@conteneur.machine.domaine	system_mail_from

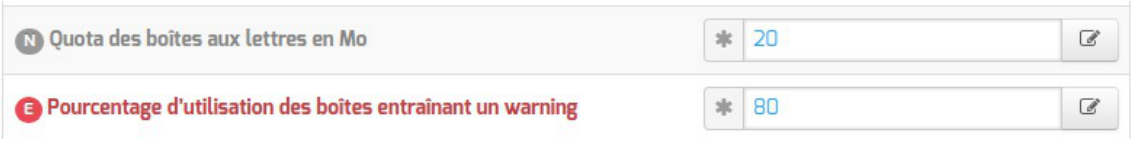
Réécriture du destinataire :

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

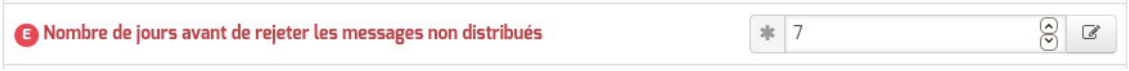
Par défaut, la distribution locale des messages est désactivée, sauf sur les modules Scribe et AmonEcole sur lesquels cette variable est masquée.



Son activation (forcée sur les modules Scribe et AmonEcole) permet d'avoir un domaine local et un domaine privé.



Lorsqu'elle est activée, il est possible d'agir sur le quota et sur le pourcentage d'occupation des boîtes, qui entraîne un message électronique d'avertissement.



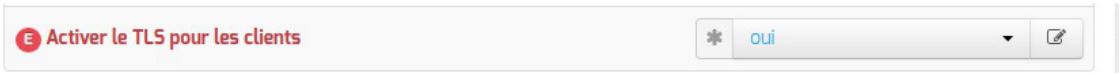
La variable `Nombre de jours avant de rejeter les messages non distribués` permet d'ajuster la durée de rétention des messages qui n'ont pas pu être envoyés (frozen).

La commande `exiqgrep` permet d'afficher la liste des messages en attente.

La ligne de commande suivante permet de purger la file d'attente :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

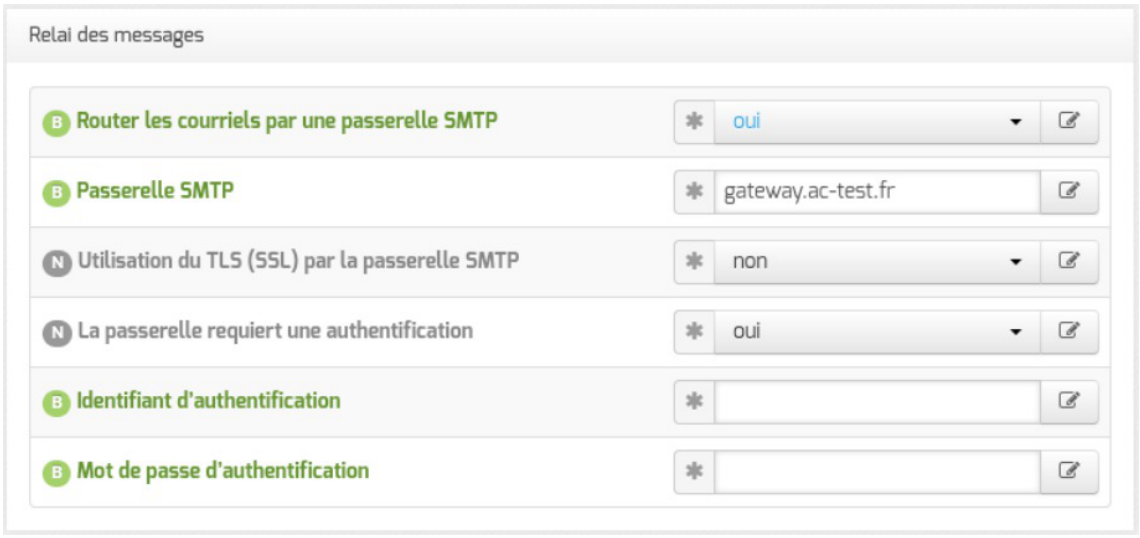
```
exiqgrep -i | xargs exim -Mrm
```



Le support du TLS[p.733] pour l'envoi de message est activé par défaut. La commande StartTLS[p.732] est supportée sur le port 25 (la connexion est initiée en mode non chiffré) et permet de basculer en TLS sur le port 465.

Passer cette variable à `non` rend l'authentification SMTP impossible ce qui empêche les utilisateurs d'envoyer des messages.

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.

Il est possible d'activer le support du TLS[p.733] pour l'envoi de messages.

Si la passerelle SMTP[p.731] accepte le TLS, il faut choisir le port en fonction de la prise en charge de la commande STARTTLS[p.732].

Pour cela il suffit d'indiquer le port spécifique dans l'option `Utilisation de TLS (SSL) par la passerelle SMTP` il y a cinq possibilités.

1. non

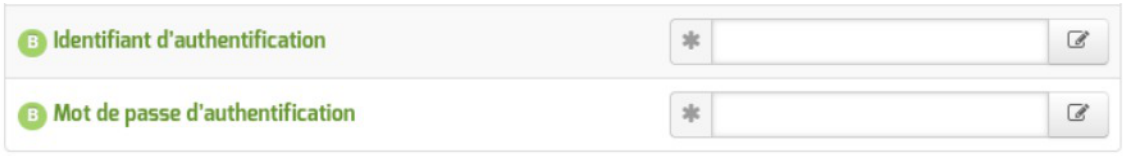
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2. port 25
3. port 465
4. port 587
5. port personnalisé

Le dernier choix permet à l'utilisateur de saisir un port différent de ceux proposés dans une nouvelle option appelée `Port de la passerelle SMTP`.

Dans le cas où la passerelle nécessiterait une authentification il est nécessaire de le signaler en passant la variable `La passerelle requiert une authentification` à `oui`.

Cette action affiche deux nouvelles variables :



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.



Configuration experte

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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

  - 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.

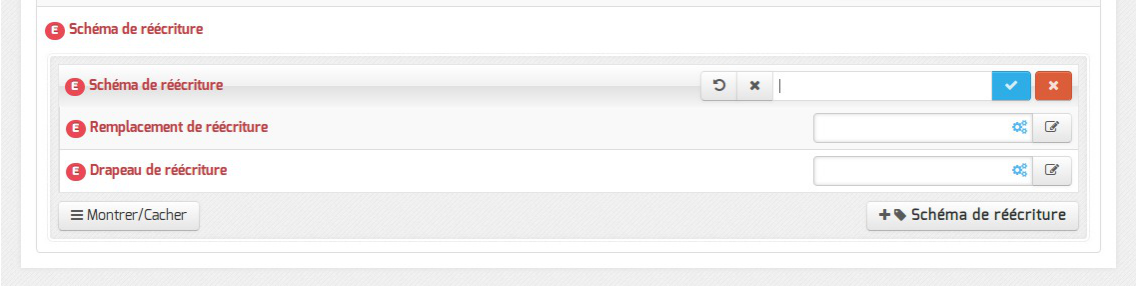
- `Dupliquer les logs dans des fichiers`

  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 domain local`.

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



  Les trois variables à saisir sont :

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

Fermeture de la messagerie

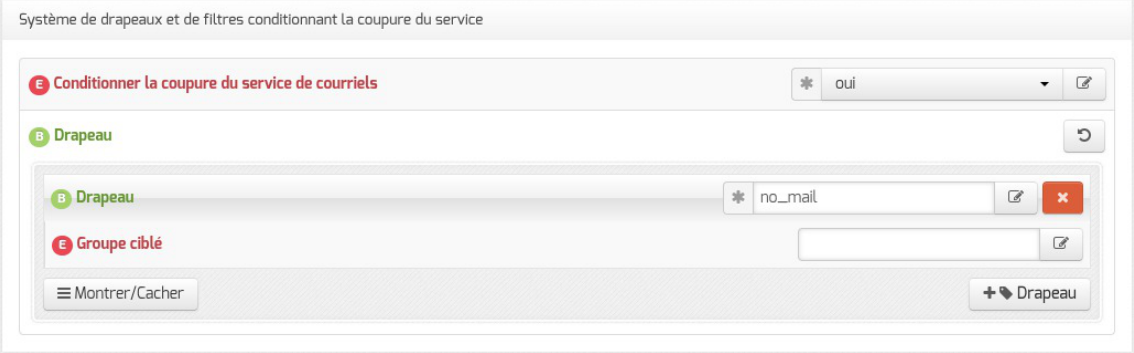
Le service de messagerie peut-être coupé sur la base de la présence d'un drapeau (fichier sur le système de fichiers).

Optionnellement, lorsque le serveur de messagerie est configuré pour accéder à l'annuaire (via la configuration du client LDAP), la coupure peut être conditionnée sur l'appartenance de l'utilisateur émetteur à un groupe de l'annuaire.

La configuration de la coupure repose sur l'identification du ou des drapeaux et sur l'identification optionnelle d'un groupe d'utilisateurs par drapeau.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

L'accès à ces paramètres est conditionné à la variable `Conditionner la coupure du service de courriels`.



- `Drapeau` : nom du fichier qui sera recherché dans le répertoire `/var/run/eole/flags` par le serveur de courriels.

  La présence du fichier est interprétée par le serveur de courriels comme un ordre de coupure du service. La coupure affecte tous les utilisateurs sauf si le paramètre optionnel suivant est renseigné.
- `Groupe ciblé` : groupe de l'annuaire permettant de restreindre la coupure à ses membres.

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

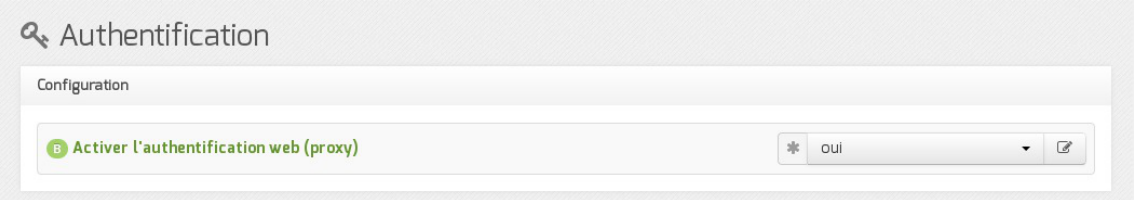
EOLE propose un mécanisme d'authentification web via un proxy.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



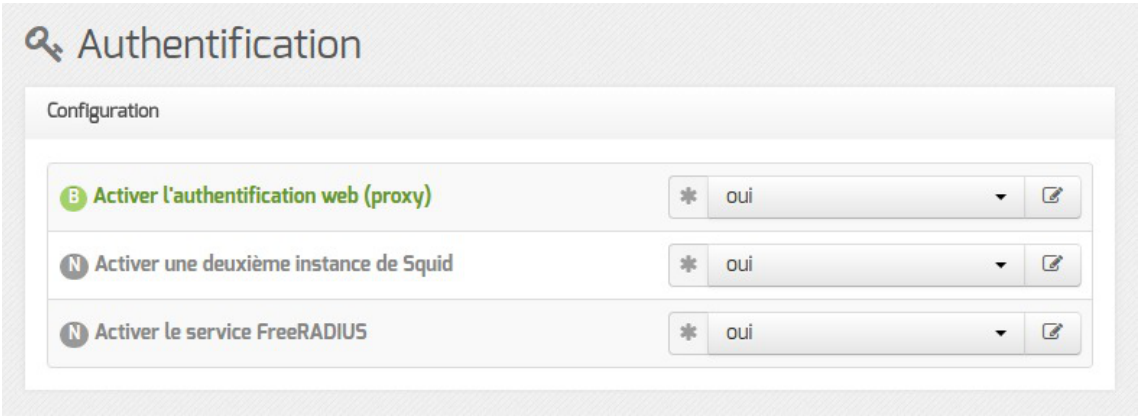
Cela fera apparaître l'onglet `Proxy authentifié 2`.

En mode expert cela fera apparaître également l'onglet `Squid2`.

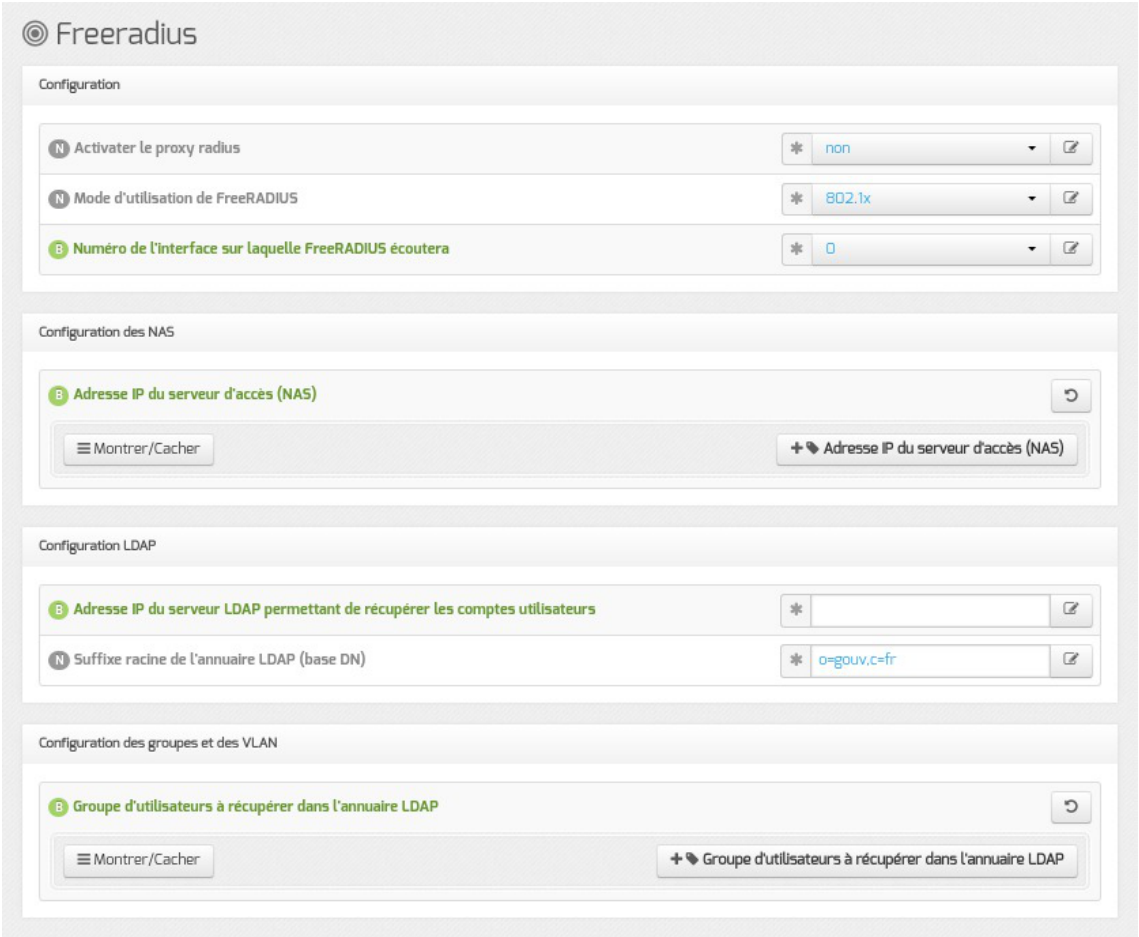
Activer le service FreeRADIUS

EOLE propose un mécanisme d'authentification réseau basée sur le protocole RADIUS[p.728].

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



Cela fera apparaître l'onglet `Freeradius`.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Voir aussi...

- Onglet Proxy authentifié : 4 méthodes d'authentification [p.300]
- Onglet Freeradius : Configuration de l'authentification Radius [p.171]

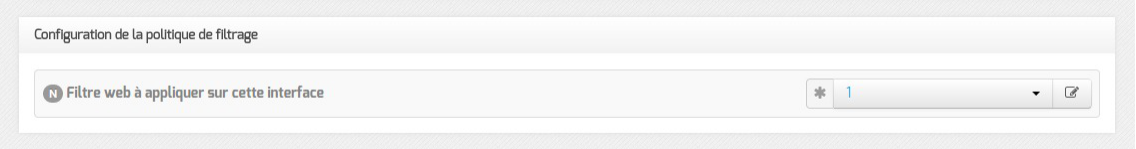
4.27. Onglet Filtrage web : Configuration du filtrage web

Le module Amon intègre le logiciel libre e2guardian[p.710] pour réaliser le filtrage web.

Configuration des zones de filtrage

La solution de filtrage permet de différencier 2 zones, ce qui permet de dissocier 2 politiques de filtrage majeures et distinctes comme par exemple une zone réseau administratif et une zone réseau pédagogique.

Il faut choisir à quelle zone appartient une interface. Cela s'effectue dans la configuration de chaque interface réseau en sélectionnant le numéro de la zone souhaité dans le champ `Filtre Web à appliquer à cette interface`.



Les zones `Filtre web 1` et `Filtre web 2` correspondent chacun à une instance du logiciel de filtrage. La configuration de chacune des instances s'effectue dans l'onglet `Filtrage web`.

En fonction de la configuration du filtrage effectuée dans l'interface de configuration du module deux sections nommées filtre web peuvent être disponibles dans l'EAD : `Filtre web 1` et `Filtre web 2`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 des politiques spécifiques en fonction de l'utilisation qui est faite des machines :

- machines du foyer (politique plus laxiste) ;
- machines du CDI (politique moins permissive).

Politiques de filtrage

Une politique de filtrage correspond à un ensemble d'autorisations ou interdictions d'accès à des sites, suivant différents critères.

Il existe 4 politiques prédéfinies :

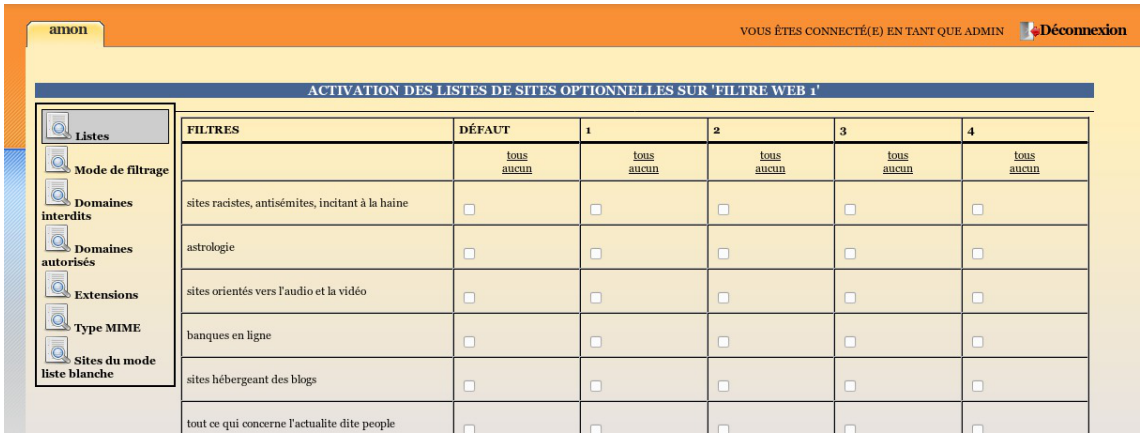
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- une politique « défaut » 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 prédéfinie `défaut` est modifiable via l'EAD.

En plus de ces politiques, il est possible d'ajouter de 1 à 4 autres politiques de filtrage (il y en a 3 par défaut).
Ces politiques de filtrage additionnelles seront alors paramétrables dans l'EAD.

Les politiques `défaut`, `modérateur`, `interdits`, `liste blanche`, et `1`, `2`, `3` et `4` si elles ont été activées, sont visibles dans l'EAD dans le filtrage par machine ou par groupe de machine.



Les politiques `1`, `2`, `3` et `4` si elles ont été activées, sont visibles dans l'EAD dans les filtres web 1 et/ou 2 dans les rubriques filtrage par bases de filtres optionnels, filtrage syntaxique, interdiction et autorisation des domaines, interdiction des extensions et des types MIME.

Configuration du nombre de politique



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.

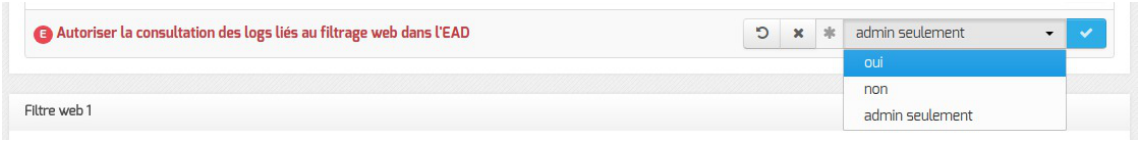


Plus vous définissez de politiques, plus e2guardian utilisera de ressources.
Adaptez le nombre de politiques activées en fonction de vos besoins.

L'observatoire des navigations

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.710].



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.717] permet de définir des valeurs adaptées 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.732]) .

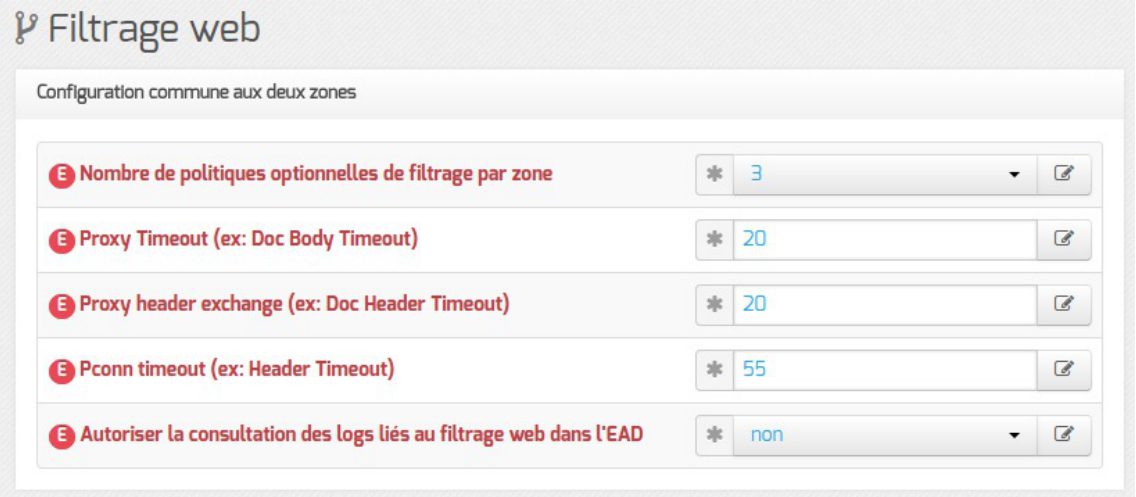
La commande `top` en console permet d'observer l'évolution de l'utilisation de la partition d'échange de façon dynamique.

Des logs aux format Dstat[p.709] sont désormais spécifiquement générés dans `/var/log/e2guardian/`.

Options de configuration communes

Les options de configuration proposées dans la première partie de l'interface de configuration sont communes à toutes les zones configurables :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Proxy Timeout (ex: Doc Body Timeout)

Délai d'attente TCP entre le proxy et e2guardian (en secondes).

Proxy header exchange (ex: Doc Header Timeout)

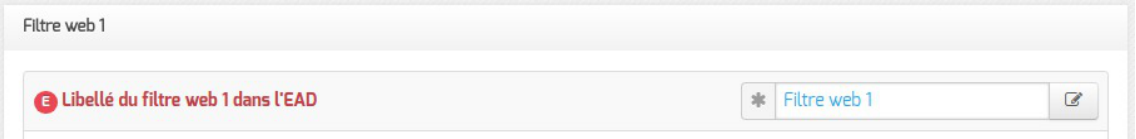
Délai d'attente entre le proxy et e2guardian (en secondes).

Pconn timeout (ex: Header Timeout)

Délai pendant lequel une connexion persistante attend de nouvelles requêtes (en secondes).

Options de configuration spécifiques à chacune des zones

Les options de configuration proposées dans les sections suivantes permettent de personnaliser la configuration de chacune des zones configurables.



Libellé du filtre web dans l'EAD

Il est possible de personnaliser le nom des zones de filtrages configurées affiché dans l'EAD.



Nombre de processus disponibles pour traiter les connexions

Depuis la version 4 du logiciel e2guardian, l'ensemble des paramètres liés à la gestion des processus a été remplacé par un seul.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Ce paramètre (`httpworkers`) définit le nombre de processus lancés au démarrage de l'instance de e2guardian.

Si le nombre de connexions dépasse sa valeur, les nouvelles connexions seront placées en file d'attente jusqu'à ce qu'un processus se libère.

Les variables `Nombre de processus disponibles pour traiter les connexions` permettent de personnaliser sa valeur pour chacune des instance de e2guardian.

Une valeur de 1000 processus convient pour une centaine d'utilisateurs, il est possible d'augmenter le nombre de processus à 5000 pour une structure de taille moyenne, 10000 pour une grosse structure.

La valeur est également dépendante du nombre de règles et de la quantité de mémoire RAM disponible.

Le nombre maximum de processus est limité à 20000.

Répertoire de cache

Permet de choisir le chemin du répertoire de cache, par défaut `/var/spool/guardianX`.

> Le script `/usr/share/eole/schedule/scripts/purgecache` purge les fichiers vieux de plus d'un jour du répertoire de cache de e2guardian.

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.727] 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.727] 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`.

Limite de pondération du filtrage

La limite de pondération est paramétrable pour chacun des filtres, la valeur par défaut (50) correspond à la valeur qui était appliquée avec le filtrage configuré pour s'appliquer sur les balises méta.

Chaque élément d'une page reçoit un score, la somme est faite et si le score est supérieur à la limite fixée alors la page est bloquée (jeunes enfants : 50, enfants : 100, jeunes adultes : 160).

Options de configuration spécifiques au filtrage associé à la deuxième instance de Squid

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le Filtre web 3 permet de contrôler les ressources de e2guardian lorsqu'une seconde instance de Squid et le filtrage web sont activés.

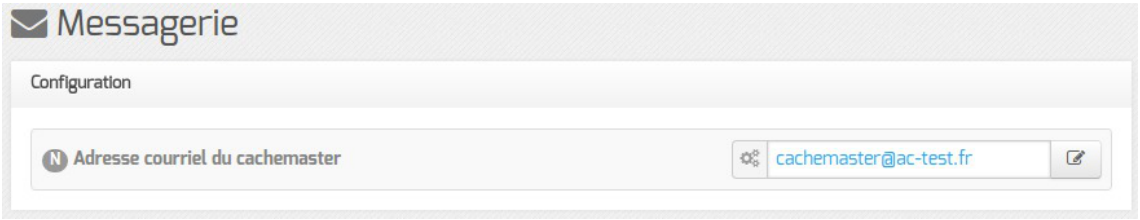


La variable `Port d'écoute pour le 3ème filtre web` permet de personnaliser le port du second proxy (3129 par défaut).

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 complétement le filtrage web.



Cela est possible en allant dans l'interface de configuration du module en mode expert et en répondant `non` à la question de l'onglet `Services`, `Activer le filtrage sur le proxy`.



Dans cette configuration, le proxy Squid écoute sur le **port 3128** en lieu et place du logiciel de filtrage e2guardian.

Voir aussi...

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Visites des sites : Observatoire des navigations [p.503]

4.28. Onglets Squid et Squid2 : activation du déchiffrement HTTPS

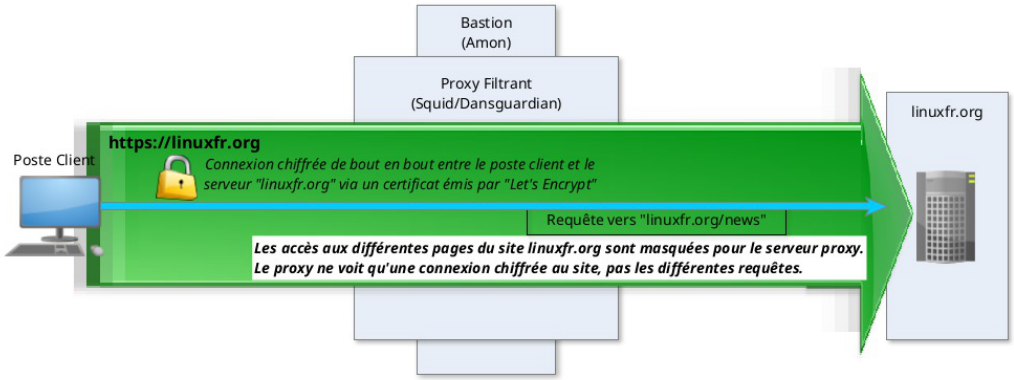
Déchiffrement et interception du protocole HTTPS

Par rapport au protocole HTTP[p.714], le protocole HTTPS permet de chiffrer la communication entre le navigateur du poste client et le serveur du site distant.

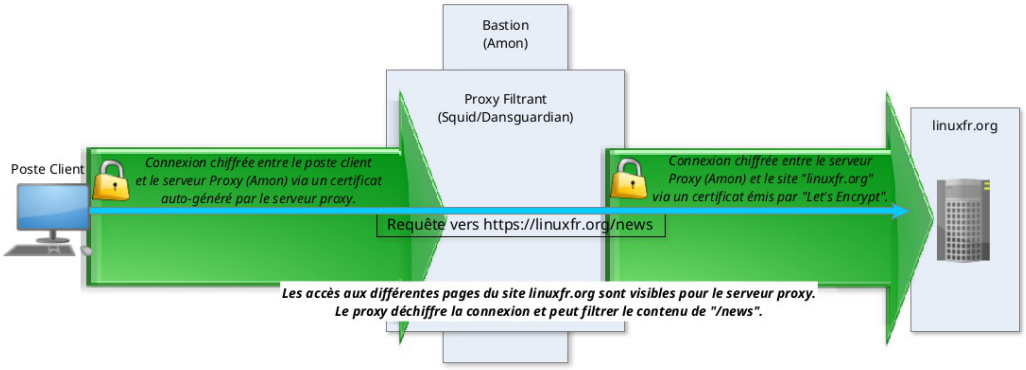
Dans ce cas, le serveur proxy ne journalise qu'une seule connexion vers le site distant (exemple : https://pcll.ac-dijon.fr) mais pas les différentes requêtes d'accès aux pages ou aux fichiers se trouvant sur ce serveur (exemple : https://pcll.ac-dijon.fr/eole/).

En HTTPS, le serveur Proxy ne peut pas filtrer le contenu des pages consultées ni scanner les fichiers téléchargés avec un antivirus.

Le déchiffrement HTTPS sur le serveur Proxy permet d'intercepter l'ensemble des requêtes et de les journaliser, de filtrer le contenu des pages visitées et de scanner les fichiers téléchargés.



Fonctionnement HTTPS normal



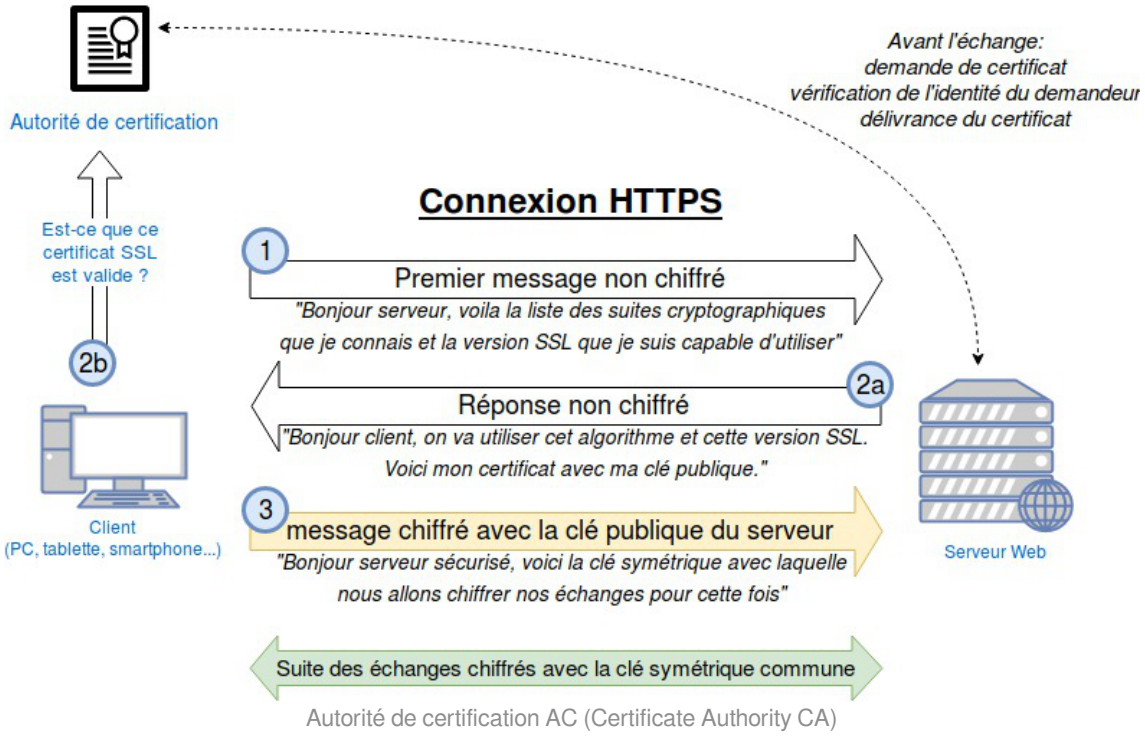
Fonctionnement HTTPS déchiffré par le Proxy

Certificat Racine de l'autorité de certification

Un certificat HTTPS est émis par une autorité de certification[p.704].

Let's Encrypt[p.717], par exemple, est une autorité de certification publique et connue des navigateurs ; son certificat racine est pré-installé dans les navigateurs et les systèmes d'exploitation.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



En revanche, le certificat racine utilisé par Amon pour déchiffrer le protocole HTTPS n'est pas public et il faut donc l'installer sur les postes clients dont le trafic doit être déchiffré et intercepté. La procédure est détaillée plus bas.

⚠ ATTENTION AUX LIMITATIONS LÉGALES

Dans la mesure où les connexions sont déchiffrées par le proxy, il convient de prévenir les utilisateurs, en particulier les adultes et le personnel. En effet, la loi reconnaît un droit à la vie privée même sur le lieu de travail : article 9 du Code civil et article L 1121-1 du Code du travail, entre autres.

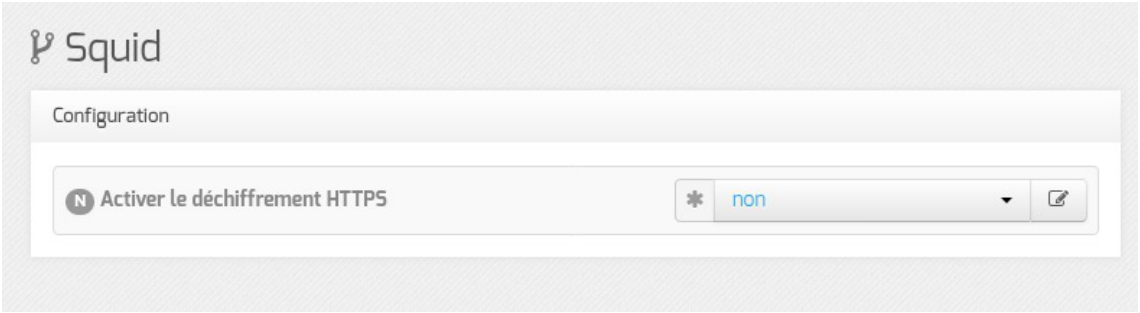
Dans certains cas, comme par exemple lors des accès aux sites bancaires ou aux sites médicaux, il ne semble pas évident que le déchiffrement HTTPS soit légal.

Mise en œuvre

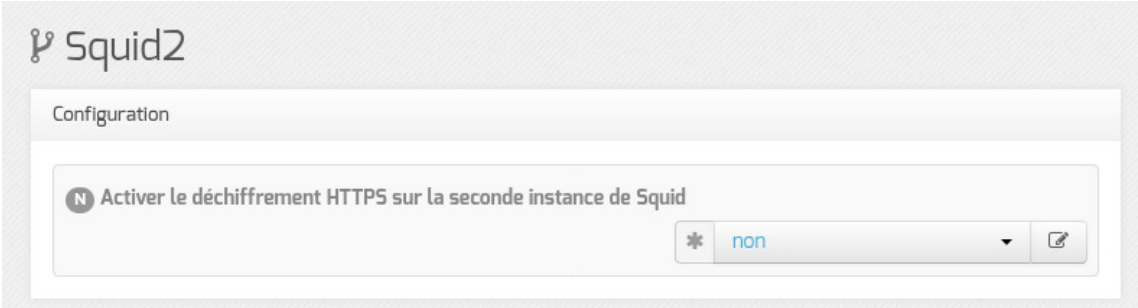
Deux variables ont été ajoutées dans les onglets `Squid` et `Squid2` :

- `Activer le déchiffrement HTTPS` ;
- `Activer le déchiffrement HTTPS sur la seconde instance de Squid`.

Ces deux variables permettent d'activer le déchiffrements des flux HTTPS transitant à travers le proxy.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Une fois le déchiffrement des flux HTTPS activé, le proxy a la capacité de connaître l'ensemble des URL consultées par l'utilisateur. Dans les journaux figureront donc les URL complètes et non uniquement les noms de domaines, comme c'est le cas sans le déchiffrement.

Dans ce mode de fonctionnement, le proxy génère un nouveau certificat pour chaque domaine visité et propose celui-ci à l'utilisateur. Tous ces certificats sont signés par une autorité de certification propre au proxy.

Pour que ces certificats soient perçus comme valides par les différentes applications utilisant le proxy, il est nécessaire de diffuser l'autorité de certification propre au proxy auprès de ces applications.

Sur un module Amon configuré pour l'interception des communications HTTPS, la commande `diagnose` permet de connaître le chemin et l'empreinte du certificat :

```
1 *** Validité du certificat racine du proxy (/etc/eole/squid_CA.crt)
2 .               signingCA.crt => Ok
3 .                   Empreinte => SHA256 Fingerprint=62
  :1B:BF:25:28:44:31:02:7E:09:31:A6:EA:FD:A5:A8:7C:D4:EB:B6:3D:83:88:62:0F:98:85:
4
```

Intégration de l'autorité de certification sur distributions Debian et dérivées

Copier le fichier `/etc/eole/squid_CA.crt` dans le répertoire du client : `/usr/local/share/ca-certificates/` et exécuter la commande :

```
sudo update-ca-certificates
```

Intégration de l'autorité de certification sur Windows

Copier le fichier `/etc/eole/squid_CA.crt` sur le poste. Cliquer droit dessus et faire "installer le certificat". Le certificat doit être mis dans le "magasin de certificat" : "Autorités de certification racines de confiance".

Les applications communes comme Edge, Chromium, les mises à jours, ... reconnaîtront ainsi cette autorité.

Intégration de l'autorité de certification dans le magasin du navigateur Firefox

Dans le "gestionnaire de certificats", présent dans l'onglet "Vie privée" des préférences du logiciel, se rendre dans l'onglet "Autorités". Il est alors nécessaire d'importer le fichier `/etc/eole/squid_CA.crt`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

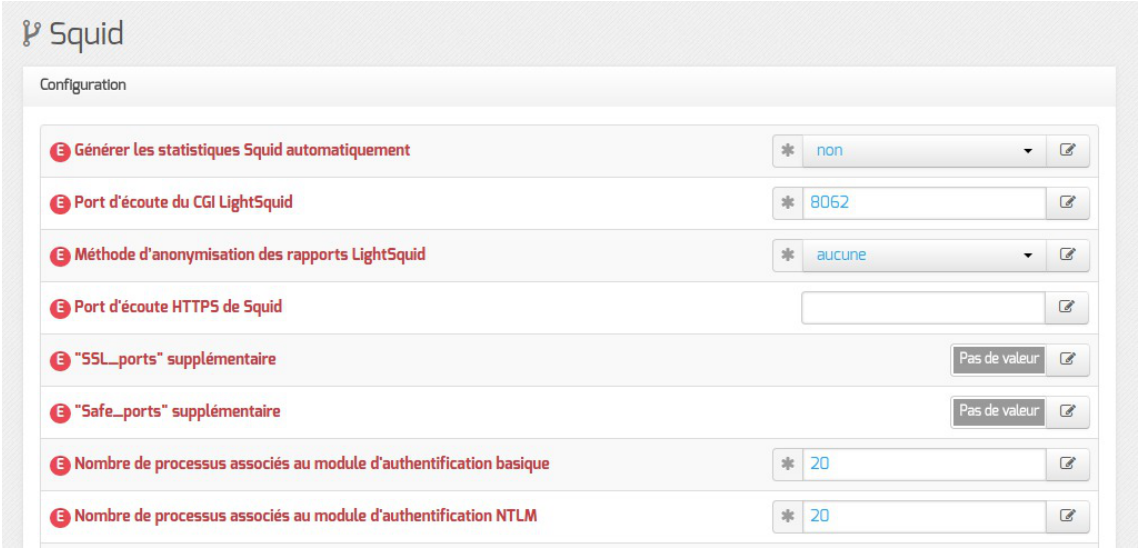
disponible sur l'Amon. Lors de l'importation, penser à cocher "Confirmer cette AC pour identifier des sites web".

> L'intégration du certificat peut être automatisée pour les postes joints à un domaine contrôlé par un module EOLE avec le paquet `eole-workstation-manager` installé.
>
> Dans ce cas précis, la configuration du module contrôleur de domaine propose l'option `Activer la configuration de Firefox` qui met en place la procédure de déploiement du certificat sur les postes clients salt.
>
> Pour plus d'informations, se reporter à la documentation des modules AmonEcole et Scribe, onglet `Workstation`.

4.29. Onglet Squid : Configuration du proxy

En mode expert, l'onglet `Squid` permet de modifier et de fixer une sélection des principaux paramètres du fichier de configuration : `/etc/squid/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).



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

Port d'écoute standard

À partir d'EOLE 2.8.1, le proxy Squid est placé en frontal et l'outil de filtrage web e2guardian passe en mode ICAP[p.715].

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le port d'écoute du proxy est toujours **3128** mais cette valeur n'est plus modifiable.

Ports d'écoute HTTPS spécifique

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` 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- **.** 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)
  - **lm_age** correspond à l'age de l'objet au moment de l'entrée dans le cache, temps, en secondes, écoulé entre la dernière modification de l'objet sur le serveur hébergeur et son entrée dans le cache. (lm_age = objet_date - objet_lastmod)
  - **expires** est la date d'expiration de l'objet éventuellement fournie par le serveur hébergeur au moment de l'entrée de l'objet dans le cache. Si elle est renseignée, la valeur de `Temps minimum de cache` prend le pas sur cette valeur.
- la valeur fournie par le client ;

  Squid tient compte de la variable **client_max_age** éventuellement fournie par le client,

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

elle indique l'âge maximal de l'objet accepté par le client. Si cette valeur est fournie par le client elle prend le pas sur la valeur `Temps maximum de cache` du fichier de configuration de Squid.

- les valeurs du fichier de configuration de Squid :
  - temps écoulé depuis le téléchargement (**age**), temps maximum et minimum de cache :
    - si `Temps maximum de cache` est défini et que le temps écoulé depuis le téléchargement est supérieur, l'objet est périmé et devra être mis à jour ;
    - si le temps écoulé depuis le téléchargement est inférieur ou égal au `Temps minimum de cache`, l'objet est considéré comme étant à jour.
  - date d'expiration de l'objet fournie par le serveur hébergeur :
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur et qu'elle est dépassée, l'objet est périmé et devra être mis à jour ;
    - si la date d'expiration de l'objet (**expires**) est définie par le serveur hébergeur mais qu'elle n'est pas encore dépassée, l'objet est considéré comme étant à jour.
  - rapport (**lm_factor**) entre le temps, en secondes, écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache :

    Plus le score du rapport entre le temps écoulé depuis l'entrée de l'objet dans le cache et son âge au moment de l'entrée dans le cache (**age**/**lm_age**) est élevé plus l'objet risque d'être périmé :
    - peu de temps écoulé (10) / objet vieux (1000) = rapport faible (0.01) → objet probablement à jour
    - beaucoup de temps écoulé (1000) / objet vieux (1000) = rapport élevé (1) → objet probablement périmé
    - peu de temps écoulé (10) / objet jeune (10) = rapport élevé (1) → objet probablement périmé
    - beaucoup de temps écoulé (1000) / objet jeune (10) = ce cas de figure n'arrive pas car géré par des règles en amont.

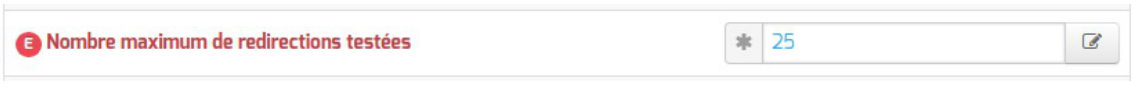
    Si le rapport est inférieur au pourcentage (**percent**) saisi dans `Rapport entre l'âge de l'objet dans le cache et son âge sur le site`, l'objet est considéré comme à jour. Diminuer la valeur du pourcentage diminue la probabilité (rapport faible) qu'un objet soit périmé.

Enfin, si aucune règle n'aboutit à considérer l'objet comme étant à jour, celui-ci est considéré comme périmé et devra être mis à jour.

Augmenter le nombre de redirections

Certains sites ont besoin de faire un grand nombres de redirections avant de fournir le contenu souhaité à l'utilisateur.

Par défaut, Squid n'accepte que 10 redirections (variable `forward max tries` du fichier de configuration de Squid) ce qui peut entraîner l'abandon des redirections et donc bloquer l'accès au site.



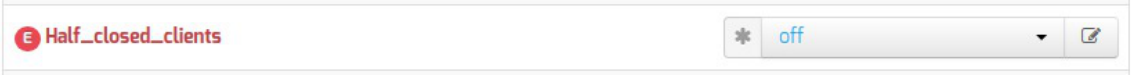
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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-fermées 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.

Personnaliser les valeurs de délai d'attente

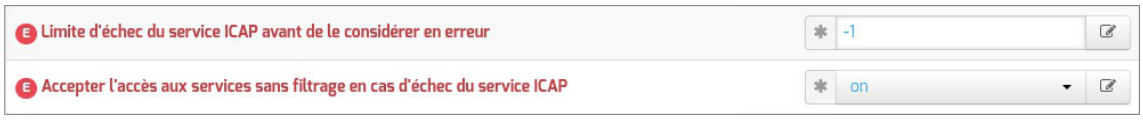
De nombreuses variables sont disponibles afin de paramétrer finement les valeurs de délai d'attente (timeout) de Squid.



À partir d'EOLE 2.6.2, l'unité de temps associée à plusieurs d'entre elles a été transformée de minute en seconde afin de permettre un paramétrage encore plus précis.

Ajustements ICAP

Le protocole ICAP permet de chaîner les traitements sur les requêtes adressées au proxy. Le filtrage de contenu est mis en œuvre en exploitant cette fonctionnalité. Deux variables sont proposées pour adapter le fonctionnement.



`La limite d'échec du service ICAP avant de le considérer en erreur` définit le

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

nombre de tentatives de connexion infructueuses au service de filtrage de contenu avant abandon. Un nombre négatif désactive la limite et implique que le service de filtrage de contenu n'est jamais considéré en erreur.

`Accepter l'accès aux services sans filtrage en cas d'échec du service ICAP` définit si une erreur de communication avec le service de filtrage de contenu entraîne le rejet de la requête. En d'autre terme, si le filtrage de contenu est une étape optionnelle de traitement de la requête.

Autres paramètres

L'onglet expert Squid permet de modifier et de fixer un nombre conséquent de paramètres optionnels du fichier de configuration : `/etc/squid/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/squid-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.285]

> Outil d'analyse de logs LightSquid [p.513]

4.30. Onglet Proxy authentifié : 4 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)`.



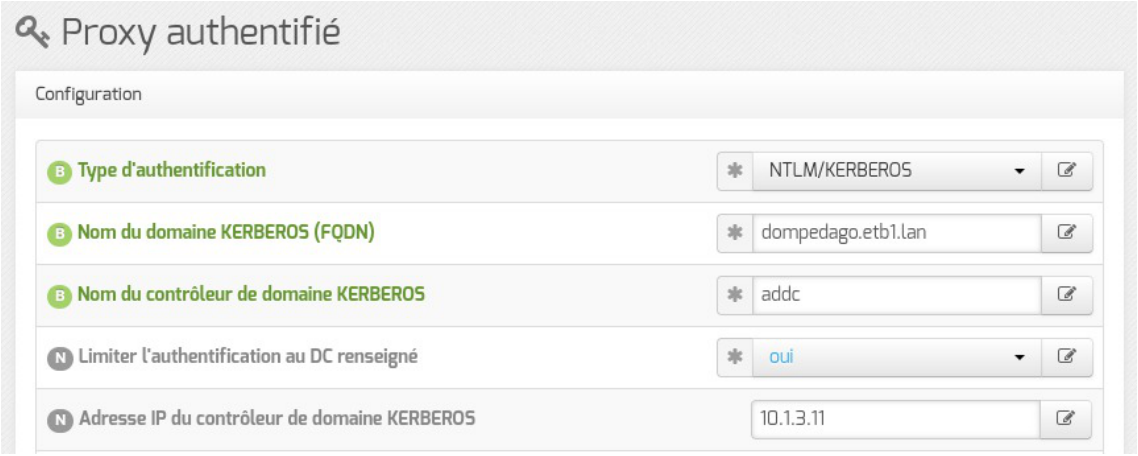
Cinq méthodes d'authentification sont alors disponibles dans l'onglet `Proxy authentifié`.

Authentification NTLM/KERBEROS

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory[p.702].

Cette configuration est à choisir si vous disposez d'un serveur Scribe ou Horus en mode AD ou d'un serveur Microsoft AD.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Si l'authentification `NTLM/KERBEROS` est activée sur le proxy, le `Nom de machine`, qui se paramètre dans l'onglet `Général`, ne peut être supérieur à 15 caractères.

En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.



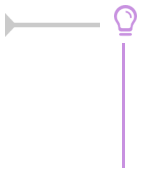
À partir d'EOLE 2.8.1,

- il n'est plus obligatoire de fournir explicitement l'`Adresse IP du contrôleur de domaine KERBEROS` ;
- il est possible de désactiver la limitation de l'authentification au DC renseigné dans `Nom du contrôleur de domaine KERBEROS`.

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 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

À partir d'EOLE 2.8.1, lorsque l'authentification est configurée en mode `NTLM/KERBEROS`, les postes hors domaine peuvent utiliser directement le proxy authentifié.

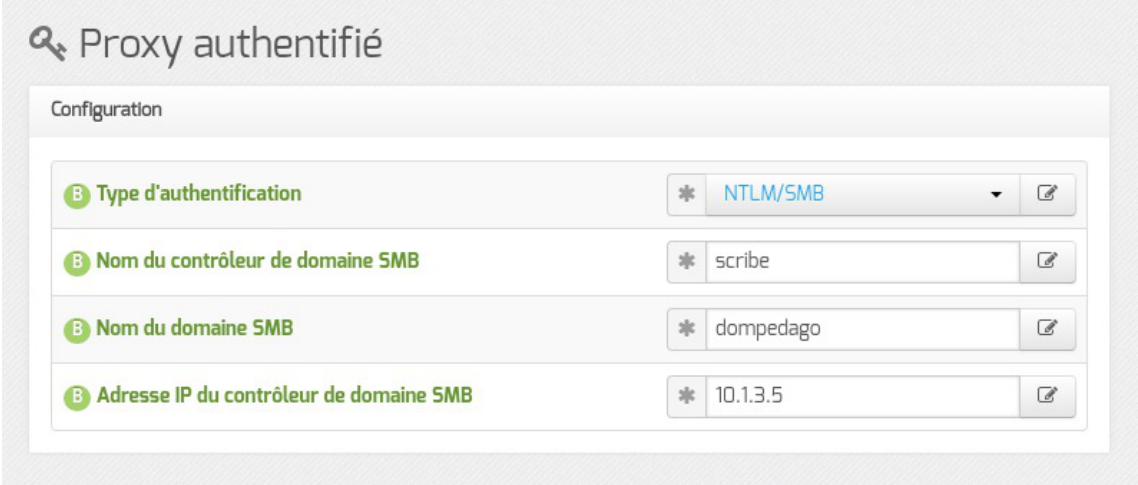
Contrairement aux versions précédentes pour lesquelles il était recommandé d'activer le proxy NTLM, les navigateurs proposent nativement une fenêtre d'authentification dans laquelle l'utilisateur saisit uniquement ses login et mot de passe Active Directory.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Authentification NTLM/SMB

Il s'agit d'une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Samba[p.730] NT.

Cette configuration est à choisir si vous disposez d'une version ancienne du serveur pédagogique Scribe ou du serveur administratif Horus.



Cette méthode d'authentification nécessite l'intégration du serveur au domaine Samba.

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 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`.

L'enregistrement au domaine étant proposé lors de l'instanciation du module, de ce fait l'authentification NTLM/SMB n'est plus proposée pour une deuxième authentification.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

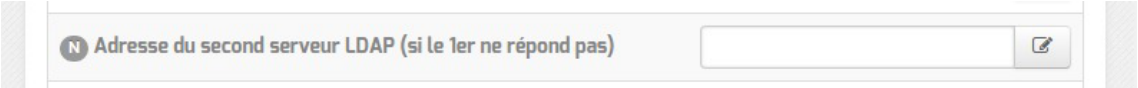
Authentification LDAP

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



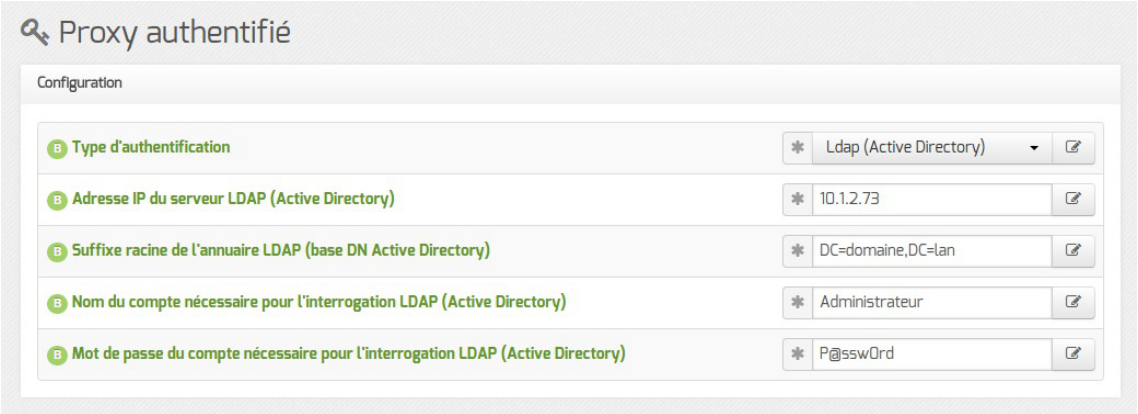
Ce type d'authentification est recommandé pour les postes hors domaine.

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



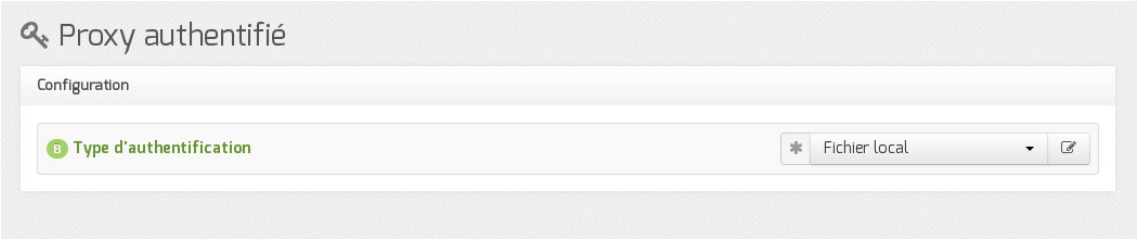
Cet annuaire est interrogé uniquement si le premier ne répond pas.
Cette fonctionnalité est recommandée dans le cas d'annuaires répliqués.

Authentification LDAP (Active Directory)



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

Authentification sur Fichier local



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

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



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

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

ou

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

Désactivation de l'authentification sur une interface

Pour chacune des interfaces (hors interface 0 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 de l'interface 2, 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)`.

Notes techniques

Les fichiers de logs spécifiques au premier type d'authentification sont les suivants :

- `/var/log/rsyslog/local/squid/squid1.info.log` → 1ère instance de squid
- `/var/log/rsyslog/local/e2guardian/e2guardian0.info.log` → 1ère instance de e2guardian (filtre web 1)
- `/var/log/rsyslog/local/e2guardian/e2guardian1.info.log` → 2ème instance de e2guardian (filtre web 2)

4.31. Onglets Squid2 et Proxy authentifié 2 : Double authentification

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

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

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

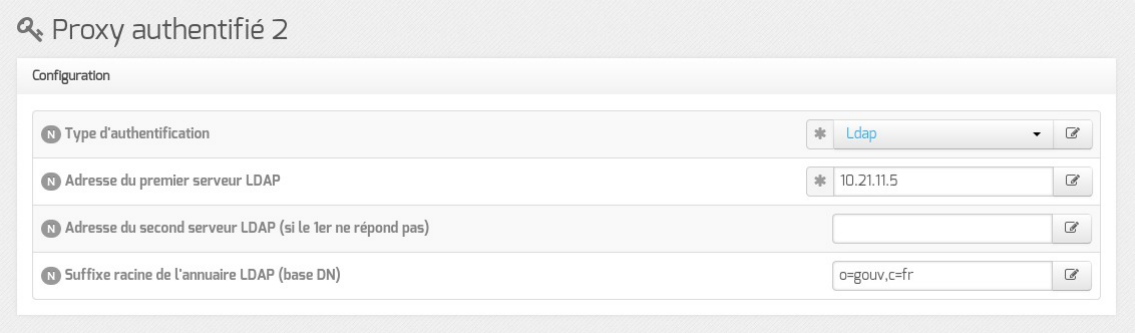
Configuration pas à pas

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



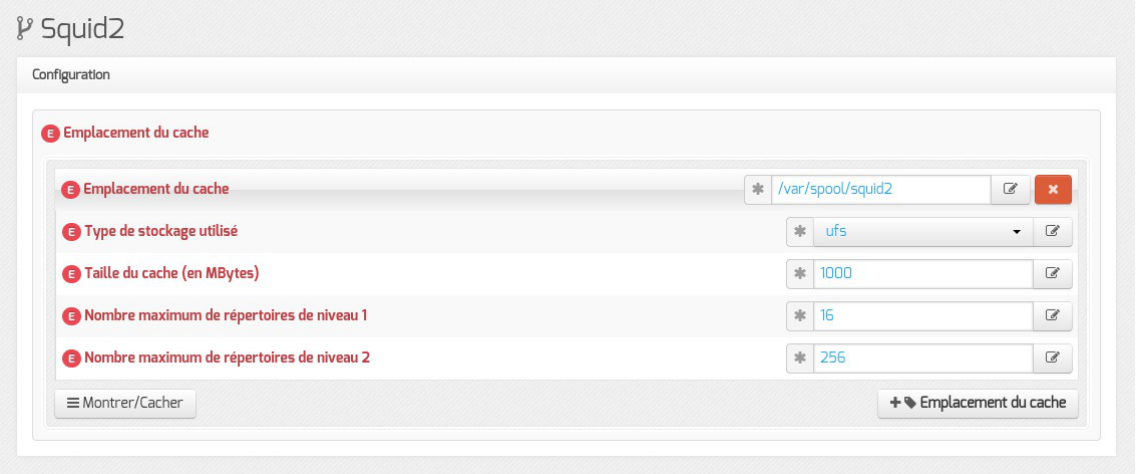
2. Configuration du type d'authentification dans l'onglet `Proxy authentifié 2` :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



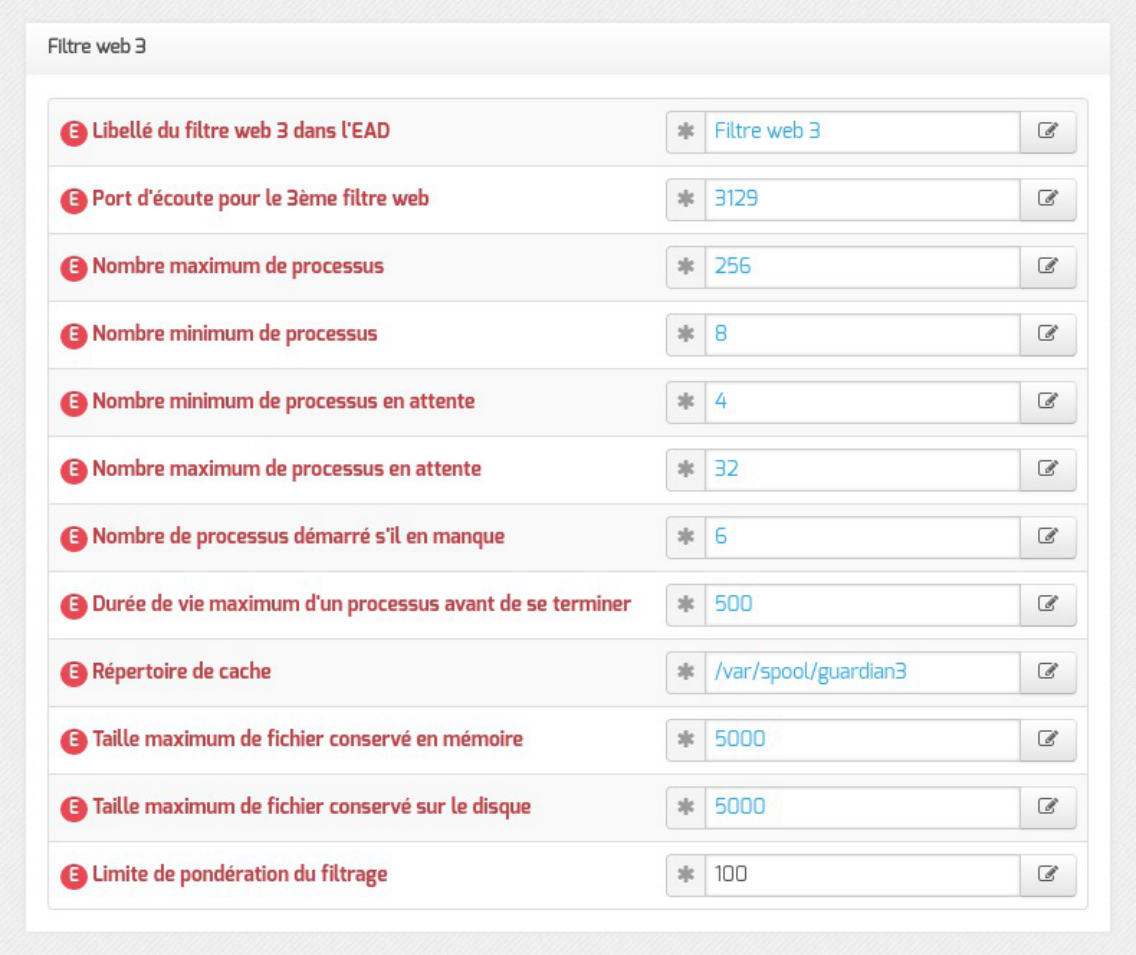
L'enregistrement au domaine est proposé lors de l'instanciation du module, de ce fait l'authentification NTLM/SMB n'est plus proposée pour une deuxième authentification.

3. Paramétrage de la seconde instance de Squid dans l'onglet expert `Squid2`



4. Paramétrage du filtrage web associé dans l'onglet expert `Filtrage web` (section `Filtre web 3`)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Si le filtrage web est activé (`Activer le filtrage sur le proxy` à `non` dans l'onglet `Services`), le port du second proxy (3129 par défaut) est personnalisable dans l'onglet `Filtrage web`, section `Filtre web 3`, présenté au pas n°4.

Dans le cas contraire (filtrage web désactivé), la personnalisation de ce port s'effectue dans l'onglet `Squid2`, présenté au pas n°3.

Notes techniques

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

- `/var/log/rsyslog/local/squid/squid2.info.log` → 2ème instance de squid
- `/var/log/rsyslog/local/e2guardian/e2guardian2.info.log` → 3ème instance de e2guardian (filtre web 3)

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).

4.32. Onglet Exceptions proxy

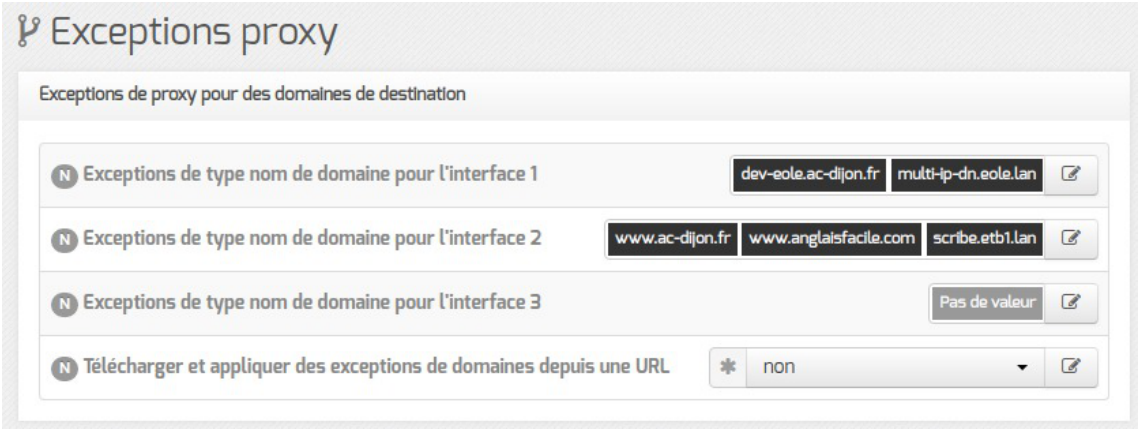
Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

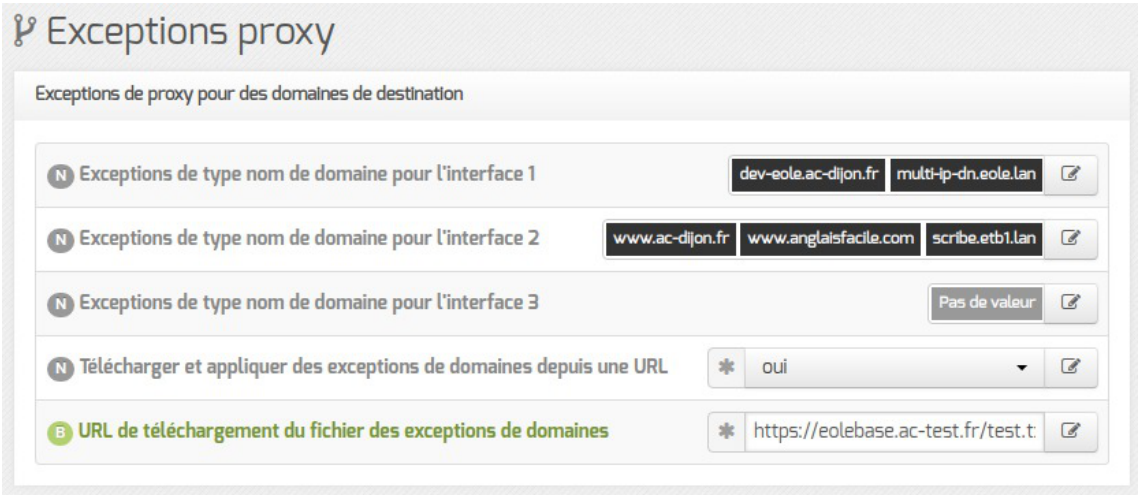
Il est possible de déclarer différents types d'exceptions.

Exception de proxy pour des domaines de destination

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



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



Il est également possible de fournir une liste de noms de domaine ou d'IP à inclure dans les exceptions au proxy depuis une URL, en activant la variable `Télécharger et appliquer des exceptions de domaine depuis une URL`.

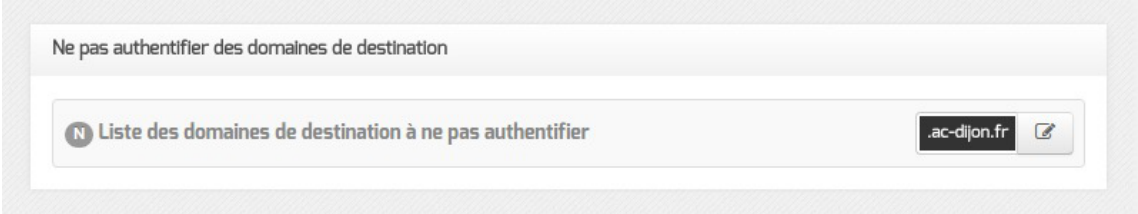


Si vous utilisez une copie des modèles ERA fournis, il faudra l'adapter pour obtenir les règles supplémentaires

Exception au niveau de l'authentification des domaines de destination

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



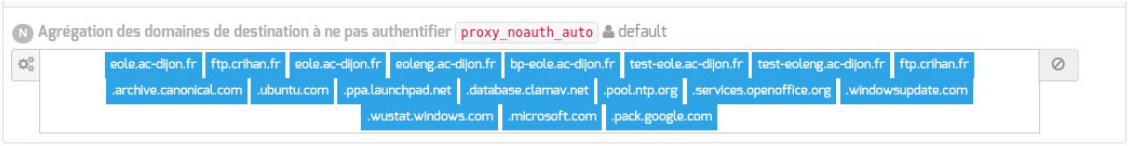
Si WPAD est activés sur l'interface réseau, les utilisateurs utiliseront directement Squid pour accéder à ces sites.

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`.

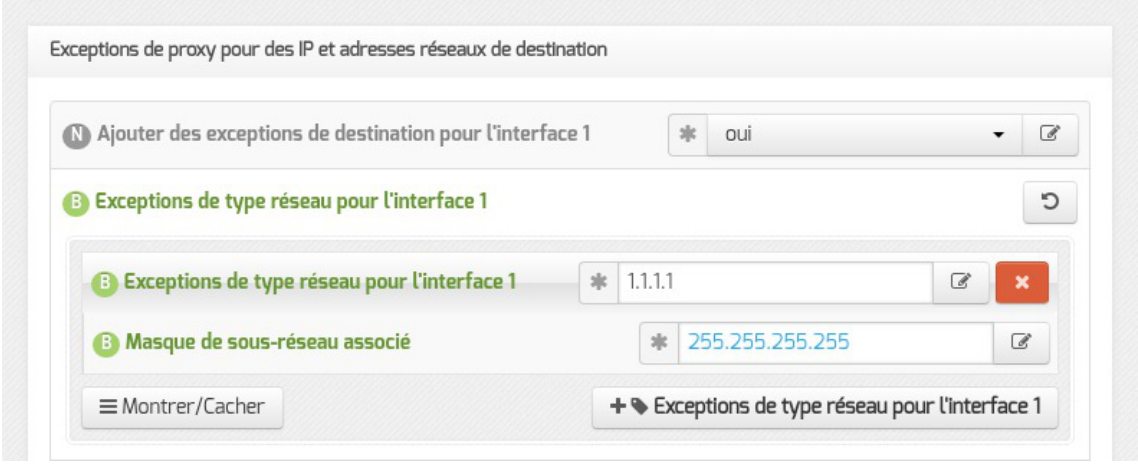
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



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

Exceptions de proxy pour des IP et adresses réseaux de destination

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.

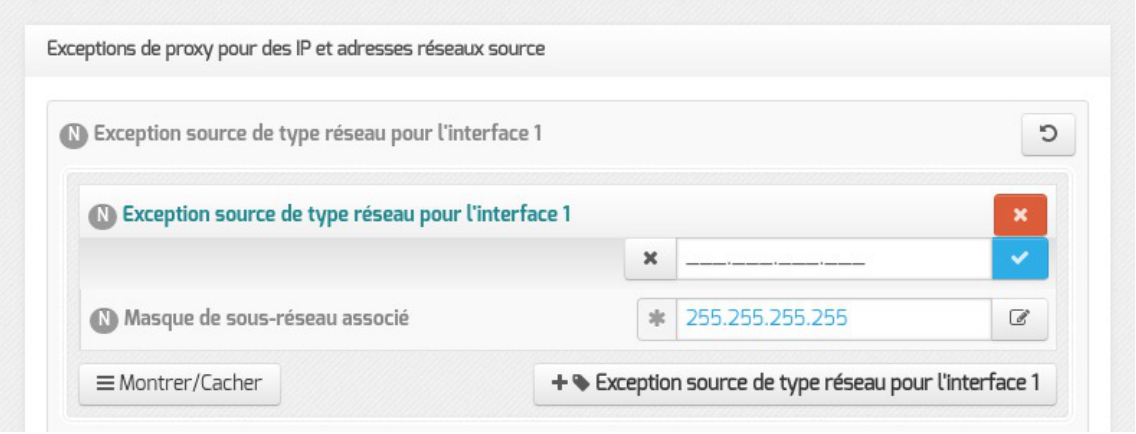


Le bouton `Exceptions de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Exceptions de proxy pour des IP et adresses réseaux source

Cette exception spécifique à ERA permet de déclarer une adresse IP ou une plage d'adresses IP **source** pour laquelle on ne passe pas par le proxy.



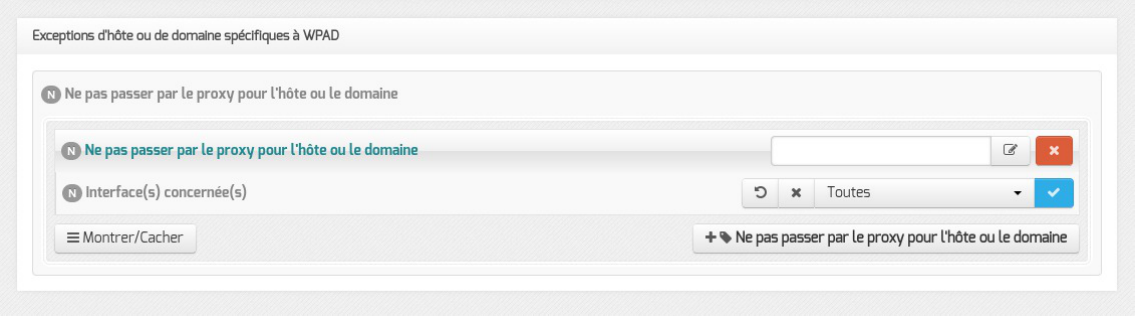
Le bouton `+ Exception source de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.



Cette fonctionnalité permet à une machine de contourner le proxy ce qui constitue un non respect des règles légales de sécurité. Elle peut servir pour effectuer des tests de proxy et d'exceptions de filtrage.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

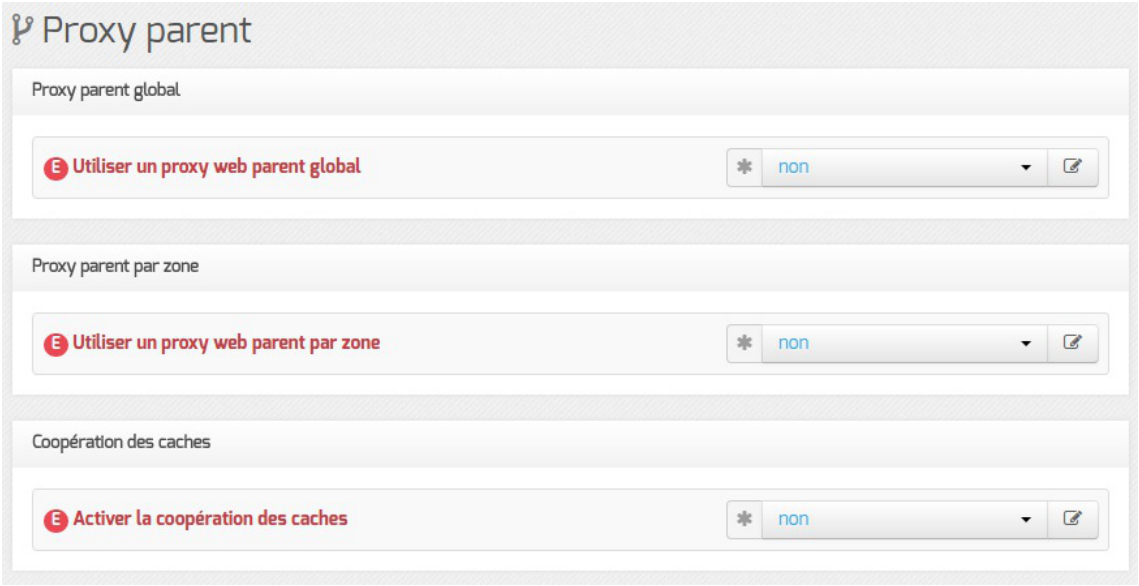
Compléments sur `Ne pas passer par le proxy pour l'hôte ou le domaine` (localHostOrDomainIs) :

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

4.33. 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.



Si plusieurs proxy parents sont déclarés, un mécanisme de type round-robin[p.729] est utilisé afin de répartir la charge sur les différents serveurs.

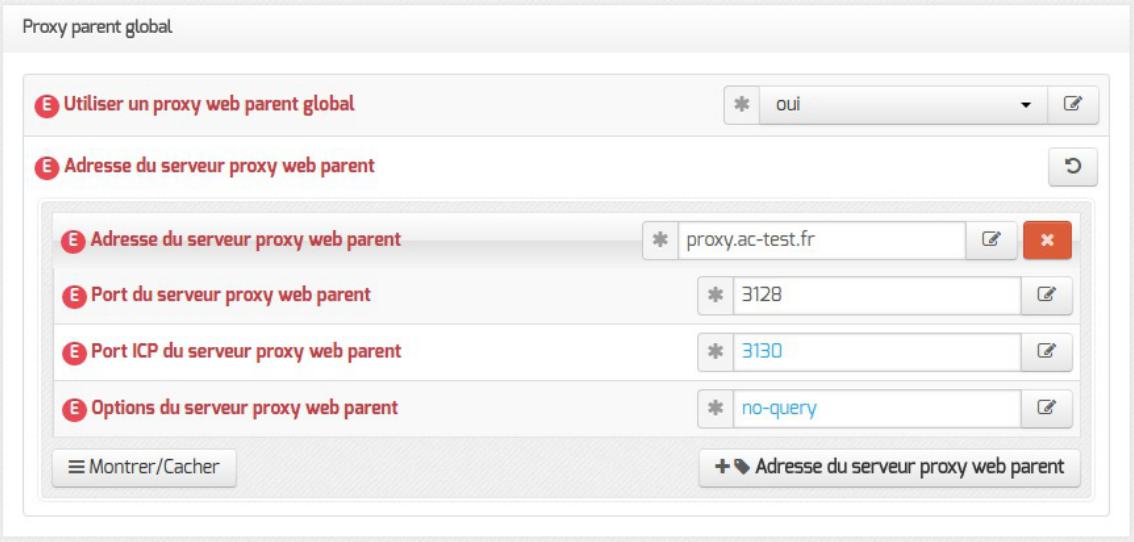
Les proxy déclarés ici ne seront pas utilisés par le serveur lui-même.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



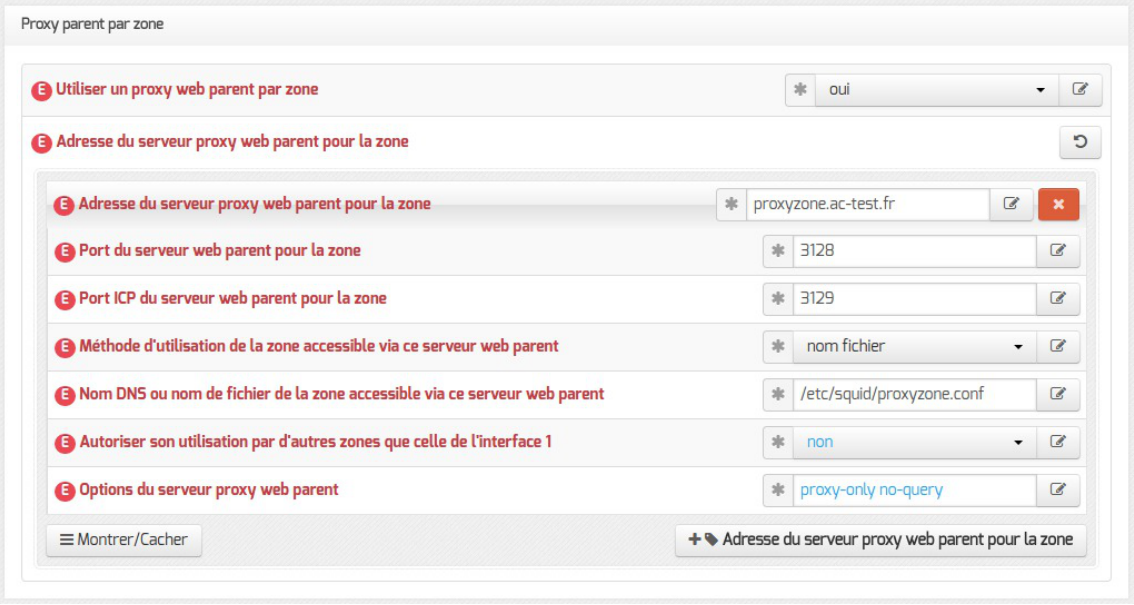
Si le réseau virtuel privé est actif la variable supplémentaire `Accès aux zones RVP en passant par le serveur proxy web parent global` est disponible. Elle permet de forcer l'utilisation du proxy web parent pour l'accès aux zones RVP.

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` ;



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

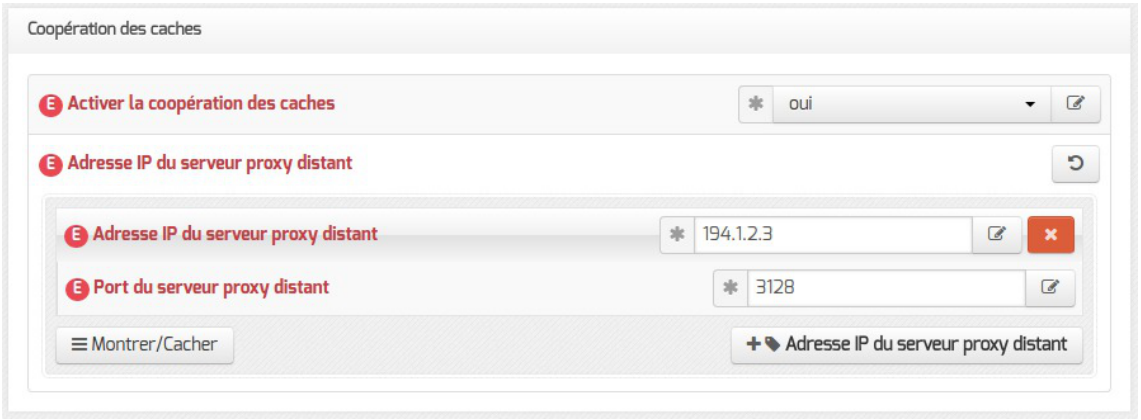
Pour que ces sous-domaines soient également pris en compte, le nom DNS du domaine doit impérativement être précédé d'un point.

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.727].



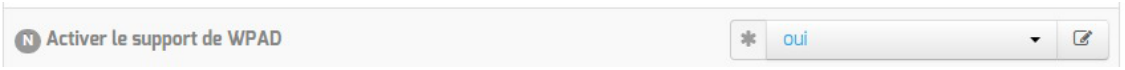
4.34. Onglet Wpad : découverte automatique du proxy

WPAD est mis à disposition sur les modules Amon et AmonEcole au travers du paquet `eole-wpad`.

Sur un module personnalisé, il n'est fonctionnel que si le paquet `eole-proxy` est installé.

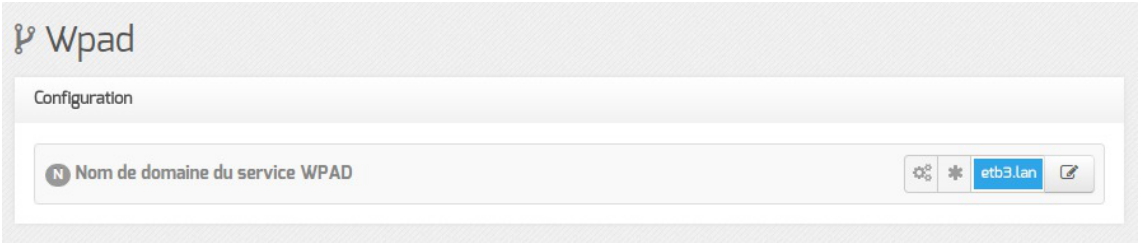
Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.348]

4.35. Onglet Nginx

L'onglet Nginx est disponible si au moins l'un des deux paramètres suivants est activé dans l'onglet Services :

- Activer la publication d'applications web par Nginx ;
- Activer le reverse proxy Nginx.



Nom de domaine par défaut

En mode normal, cet onglet permet de saisir le Nom de domaine par défaut vers lequel sera redirigé un client qui accède au serveur avec un nom de domaine non déclaré.

Restriction Nginx

À partir d'EOLE 2.8.1, la variable : Appliquer des restrictions pour les ports Nginx permet de restreindre l'accès aux ports ouverts pour Nginx aux adresses autorisées à administrer le serveur.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Des restrictions supplémentaires au niveau des connexions SSH sont disponibles dans le bloc `Administration à distance` de l'onglet `Interface-0`.

En mode expert, la configuration du service peut être affinée.



Dégrader la sécurité en HTTP

Il est possible de dégrader la sécurité du service Nginx en désactivant l'utilisation du HTTPS.

Si le protocole HTTPS est désactivé, certaines applications critiques publiées par Nginx telles que l'outil d'administration EAD3 ou l'interface de configuration du module ne seront plus disponibles.

Longueur maximum pour un nom de domaine

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

Taille maximale des données reçues par la méthode POST

L'option `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`).

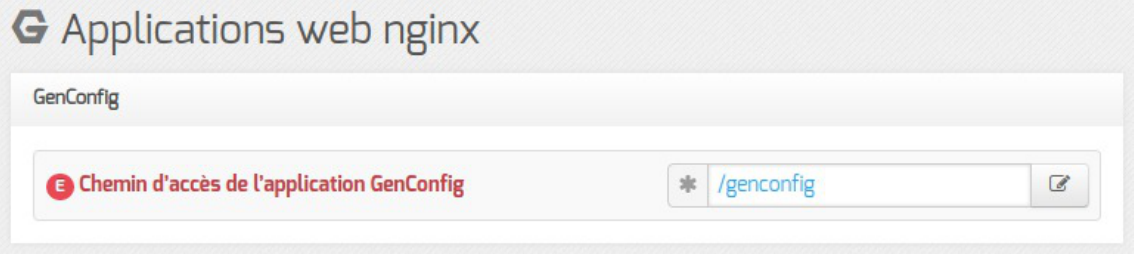
Sur les versions antérieures à 2.6.2, cette variable était située dans l'onglet `Reverse Proxy`.

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 les modules AmonEcole), le paramétrage de cette option s'effectue dans l'onglet `Apache`. Sa valeur est alors utilisée à la fois pour le serveur web Apache et pour le proxy inverse Nginx.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

4.36. Onglet Applications web nginx

L'onglet `Applications web nginx` n'est visible qu'après activation de l'une des applications utilisant ce service (interface de configuration du module, interface d'administration du module…) dans l'onglet `Services` en mode expert. Dans cet onglet `Activer la publication d'applications web par Nginx` doit également être à `oui` ce qui est le cas par défaut.



Le chemin d'accès aux applications activées est personnalisable.

4.37. Onglet Reverse proxy : Configuration du proxy inverse

EOLE propose un serveur proxy inverse (reverse proxy) basé sur le logiciel libre Nginx[p.722].

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.709] par exemple). Cela le différencie grandement d'un proxy classique comme Squid[p.731].

Concrètement, le proxy inverse permet d'ouvrir des services web installés sur des serveurs situées "derrière" le pare-feu l'accès sur Internet sans avoir recours à des règles *iptables*[p.716]*/DNAT*.

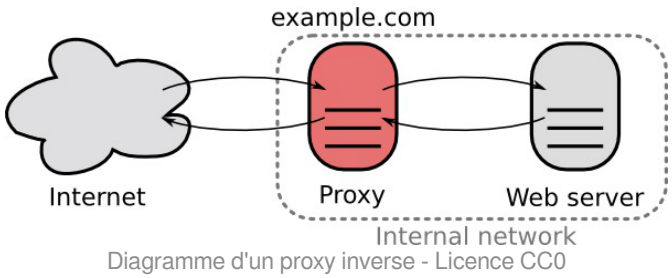
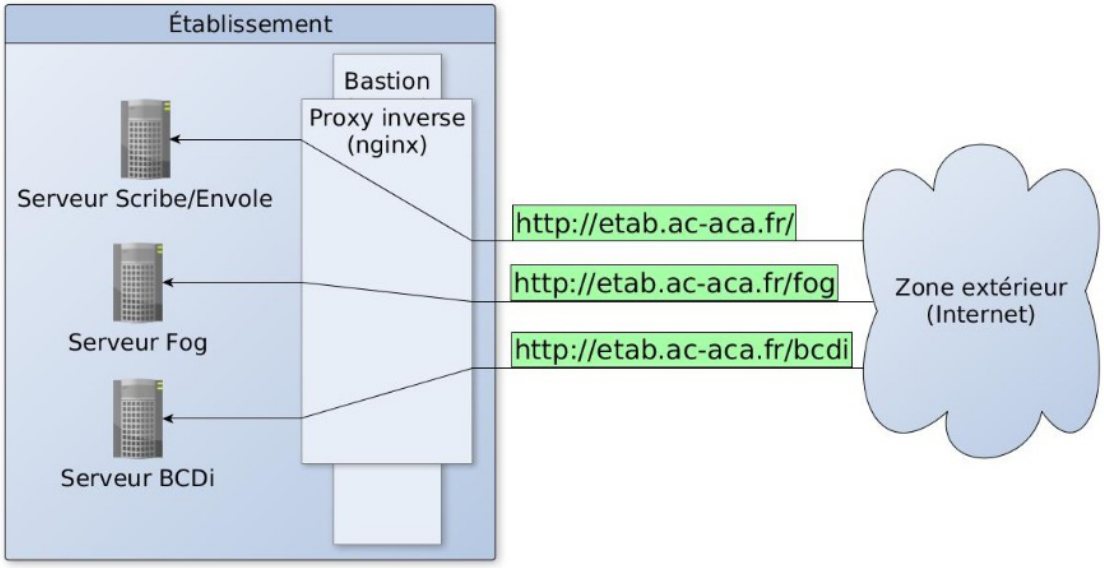


Diagramme d'un proxy inverse - Licence CC0

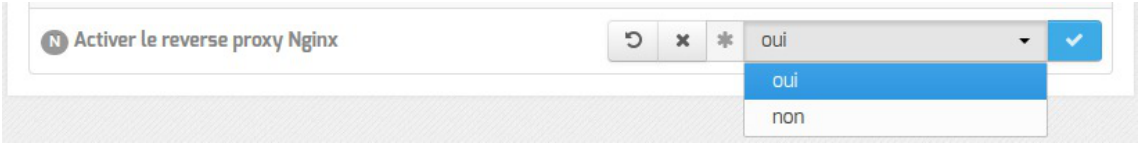
Le proxy inverse EOLE peut relayer des requêtes vers les services suivants :

- serveur EoleSSO ;
- outil d'administration EAD[p.710] ;
- application EOP ;
- protocole HTTP[p.714] ;
- protocole HTTPS[p.714].

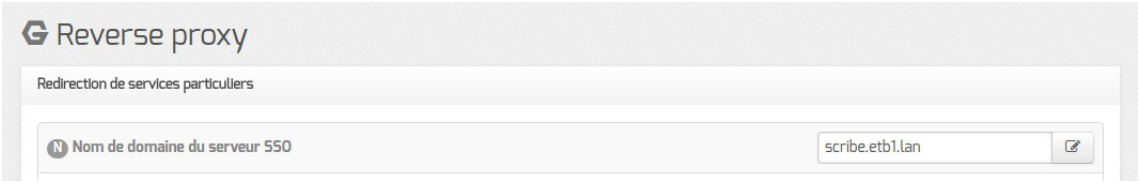
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

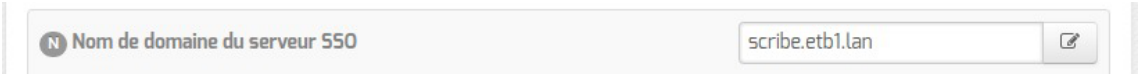


L'activation du service fait apparaître un nouvel onglet.



Redirection de services particuliers

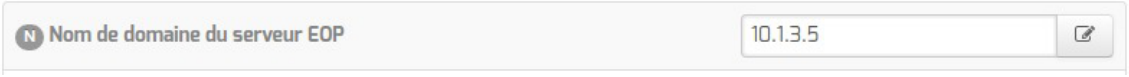
Redirection du service EoleSSO



Pour rediriger le service EoleSSO (port 8443), il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

Cette fonctionnalité n'est disponible que dans le cas ou le serveur EoleSSO n'est pas activé en local (`Utiliser un serveur EoleSSO` doit être différent de `local` dans l'onglet `Services`).

Redirection de l'application EOP



Afin d'être totalement fonctionnelle derrière un reverse proxy, l'application EOP nécessite des règles de redirection particulières (redirection du port 6080 pour l'observation VNC[p.734]).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour rediriger l'application EOP, il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (en général l'adresse IP ou le nom de domaine interne du module Scribe).

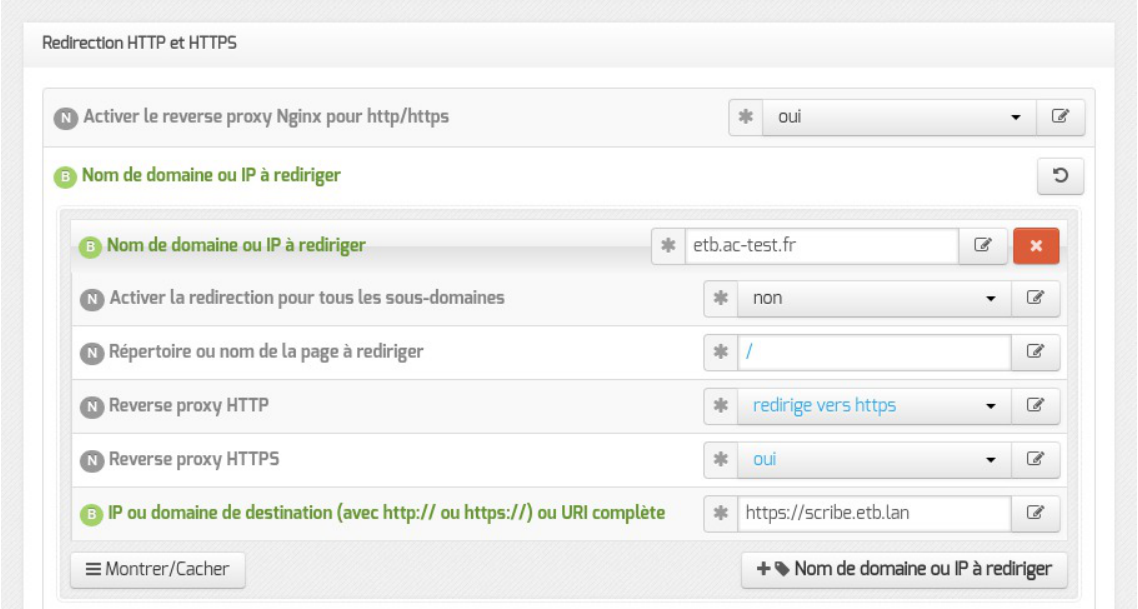
Redirection de l'interface d'administration EAD



Pour accéder de manière sécurisée à l'EAD d'un serveur depuis l'extérieur de l'établissement, il est recommandé :

- d'activer l'interface web de l'EAD du serveur interne sur un second port (4203 par défaut) dans l'onglet expert `Ead-web` de ce module ;
- d'activer la redirection sur le serveur faisant office de reverse proxy en configurant l'adresse IP ou le nom de domaine interne de la machine de destination et son port d'écoute.

Redirection HTTP et HTTPS



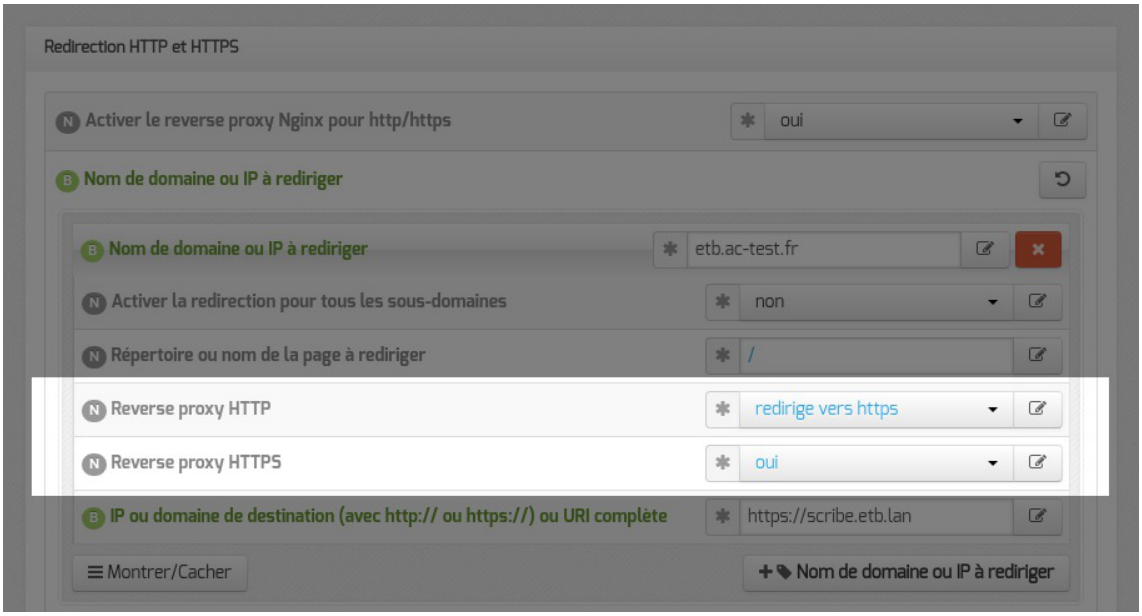
Pour rediriger HTTP et HTTPS il est nécessaire de passer la variable `Activer le reverse proxy Nginx pour le http/https` à `oui` et de renseigner plus d'informations :

- 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 ;
- `Activer la redirection pour tous les sous-domaines` : cette variable est disponible à partir de la version 2.6.2 d'EOLE, elle permet la prise en charge de tous les sous-domaines par le proxy inverse ;
- `Demander un certificat à Let's Encrypt pour ce domaine` ? : cette variable est disponible à partir de la version 2.6.2 d'EOLE si la redirection pour tous les sous-domaines n'est pas activé et que le certificat SSL est Let's Encrypt ;
- le `Répertoire ou nom de la page à rediriger` permet de rediriger un sous-répertoire vers

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.734] (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`.

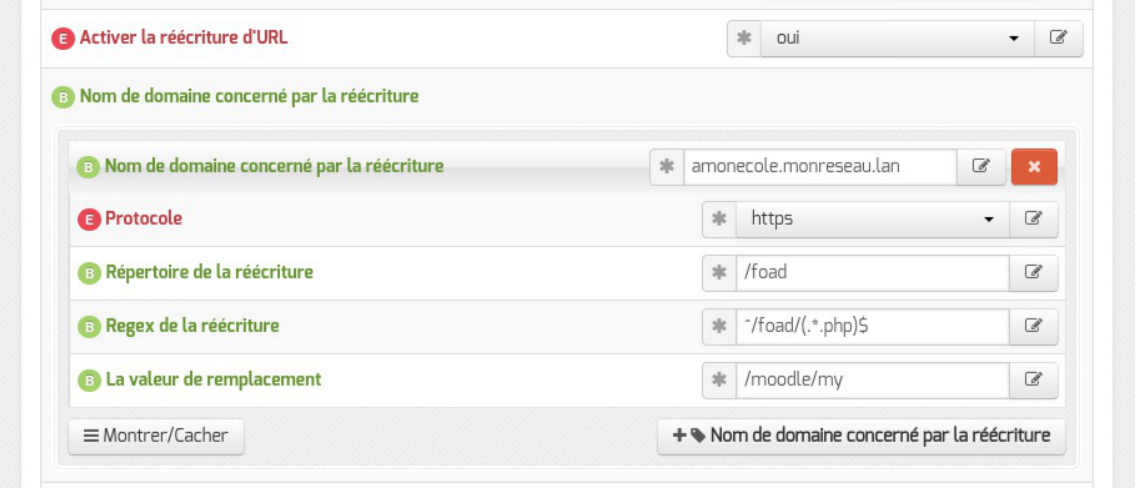
Il est possible d'ajouter plusieurs redirections en cliquant sur le bouton `+ Nom de domaine ou IP à rediriger`.

> Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.727], `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).

Réécriture d'URL

L'activation de la réécriture d'URL permet d'ajouter une expression rationnelle et une valeur de remplacement.

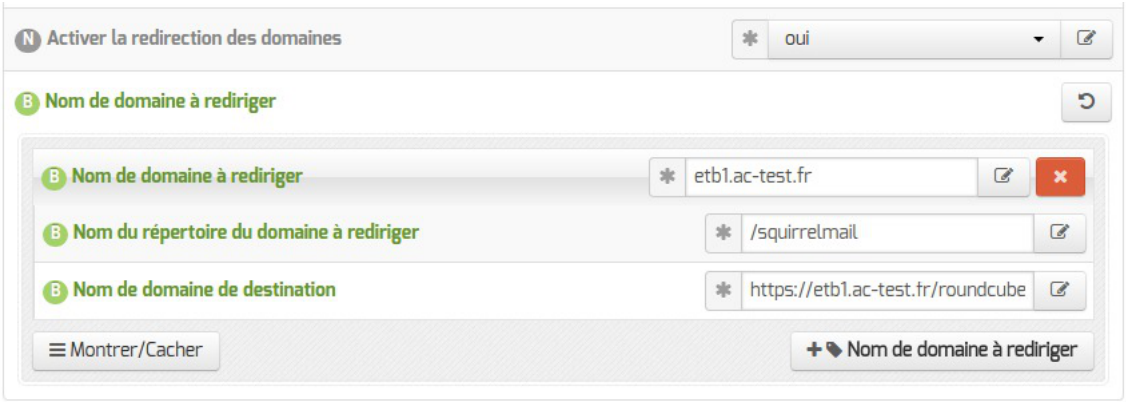
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

Redirection de domaines



Le reverse proxy permet de rediriger automatiquement les utilisateurs voulant accéder à une page particulière vers une autre page.

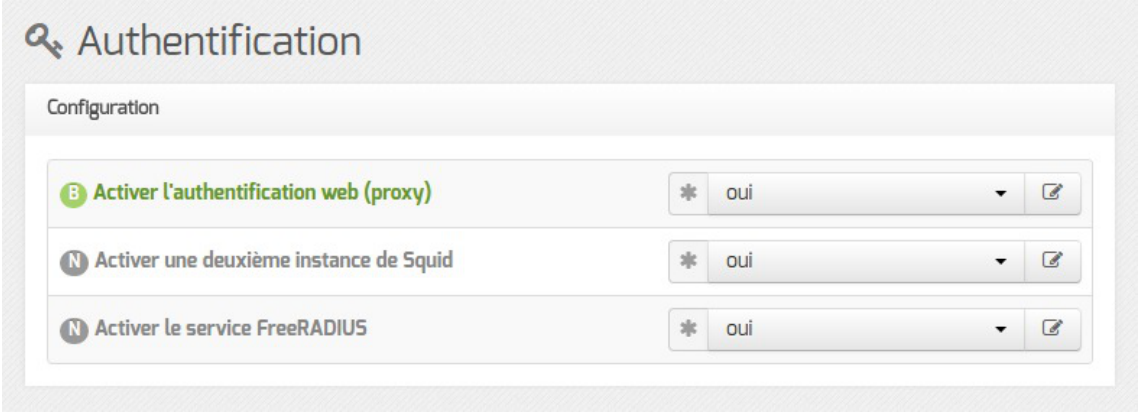
L'exemple ci-dessus illustre le remplacement de SquirrelMail par Roundcube : si l'utilisateur cherche à accéder à l'adresse `http://etb1.ac-test.fr/squirrelmail/`, la page se recharge automatiquement avec l'URL de la nouvelle messagerie : `http://etb1.ac-test.fr/roundcube/`.

4.38. Onglet Freeradius : Configuration de l'authentification Radius

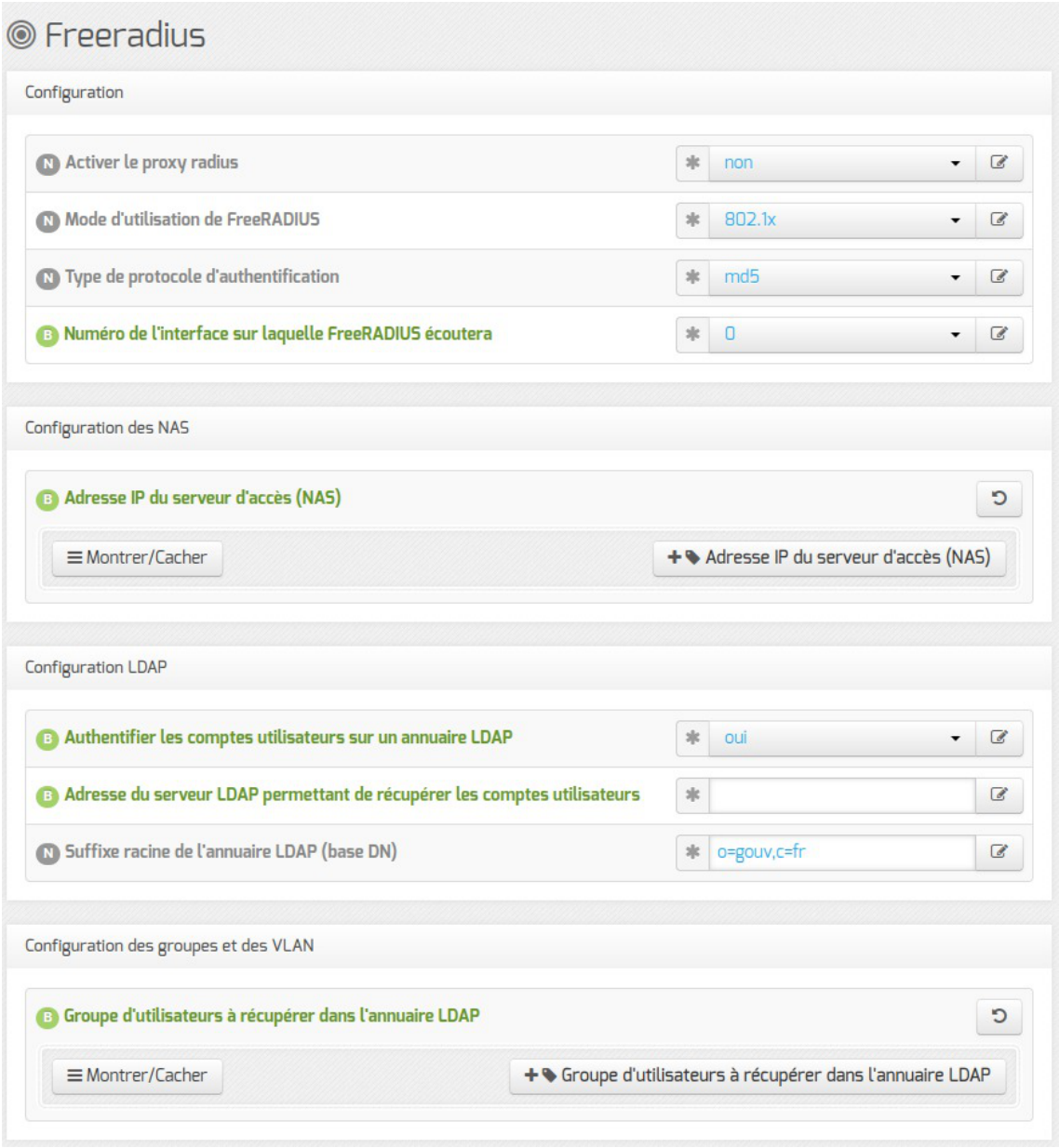
EOLE propose un mécanisme d'authentification réseau basé sur le protocole RADIUS[p.728].

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Cela fera apparaître l'onglet `Freeradius`.

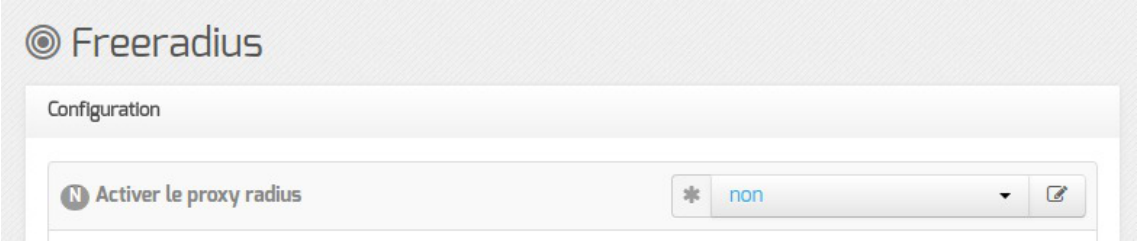


Proxy RADIUS

L'activation du proxy RADIUS permet de relayer les requêtes d'authentification vers un autre serveur RADIUS.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le paramétrage fin du serveur proxy RADIUS n'est pas implémenté. La configuration est celle proposée par défaut dans le logiciel.



Certains serveurs NAS[p.721] nécessitent un serveur proxy RADIUS pour le bon fonctionnement de l'authentification.

Requêtes d'authentification

Certains attributs externes comme le nom d'utilisateur doivent parfois être copiés dans la requête de d'authentification de tunnel ainsi que dans la réponse.

Les variables suivantes permettent d'activer ou non la copie des attributs externes dans la requête.



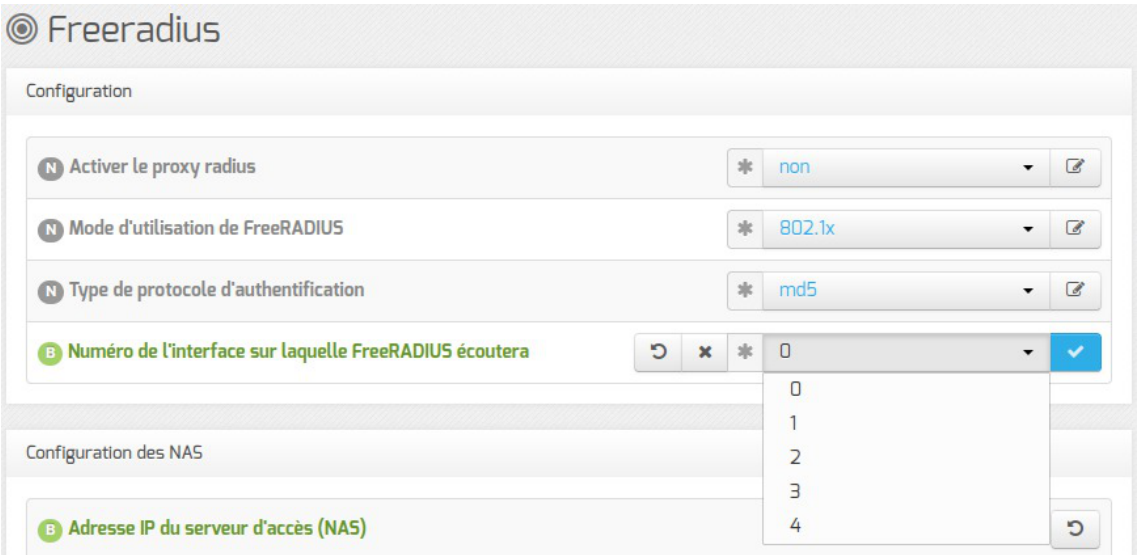
Modes de fonctionnement

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

- 802.1x ;
- accounting.

Le mode 802.1x

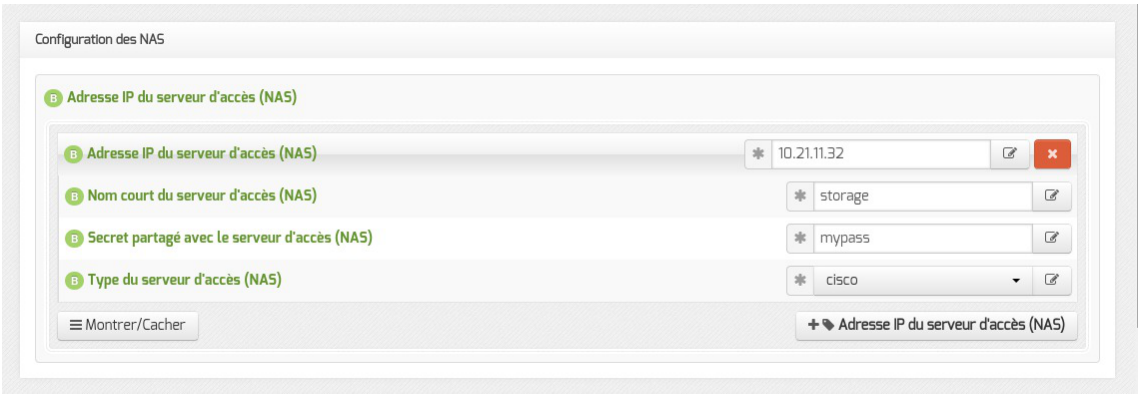
Le mode `802.1x` permet de marquer dynamiquement des ports d'un switch (NAS[p.722]) sur lesquels sont brassées des stations en fonction du compte LDAP de connexion.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`Numéro de l'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



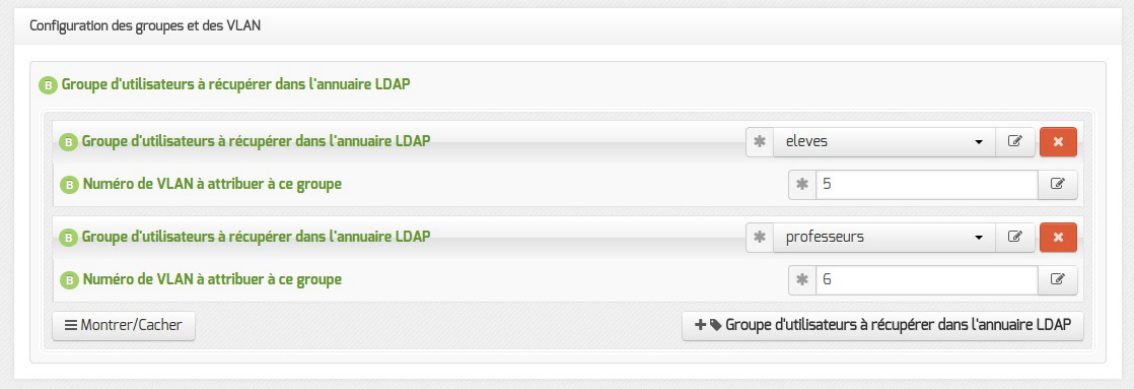
`Authentifier les comptes utilisateurs sur un annuaire LDAP` : L'authentification LDAP permet de s'assurer que l'utilisateur est autorisé à accéder aux réseaux. Mais si on gère une flotte de machine, l'authentification par clé TLS peut être jugée comme suffisante. Pour désactiver l'authentification LDAP, sélectionner `non`.

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

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 marqué avec ce numéro de VLAN.

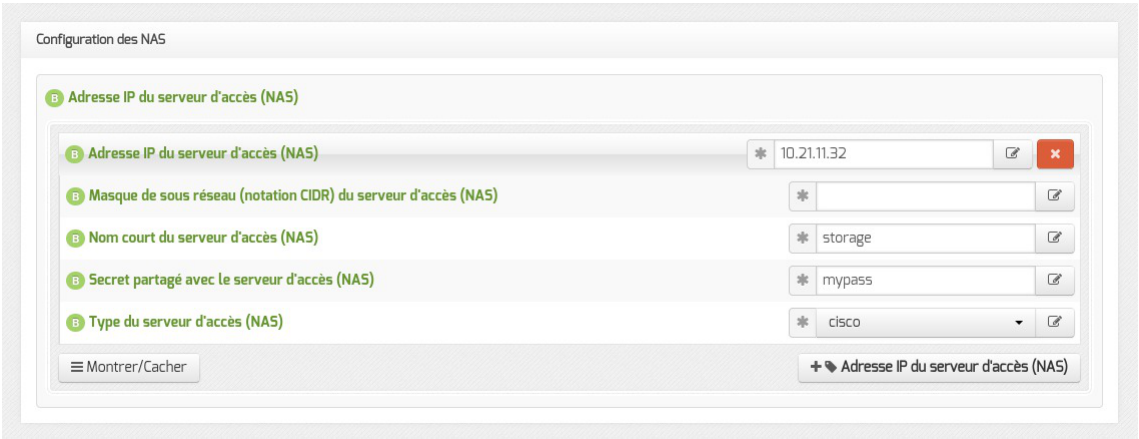
Le mode accounting

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



`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.706]) si le réseau est de classe C.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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



`Authentifier les comptes utilisateurs sur un annuaire LDAP` : L'authentification LDAP permet de s'assurer que l'utilisateur est autorisé à accéder aux réseaux. Mais si on gère une flotte de machine, l'authentification par clé TLS peut être jugée comme suffisante. Pour désactiver l'authentification LDAP, sélectionner `non`.

`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.

Pour tester la connexion à Freeradius en mode accounting il est possible d'utiliser la commande `radtest` :

```
root@amon:~# radtest -x admin <mdp admin> <Adresse IP sur laquelle FreeRADIUS écoute> <port d'écoute du NAS> <Secret partagé avec le serveur d'accès>
```

ou encore

```
root@amon:~# radtest -x admin <mdp admin> $(CreoleGet "freerad_listen_addr") <port d'écoute du NAS> $(CreoleGet "freerad_nas_passwd")
```

Les journaux systèmes sont disponibles dans `/var/log/rsyslog/local/freeradius/` :

```
root@amon:/usr/share/eole/creole# tail -f /var/log/rsyslog/local/freeradius/freeradius.notice.log
2017-06-09T16:49:36.420151+02:00 amon.etb1.lan freeradius[32240]: Login OK: [admin] (from client other port 10)
2017-06-09T16:49:57.807213+02:00 amon.etb1.lan freeradius[32240]: Login OK: [admin] (from client other port 10)
```

Choix du protocole d'authentification

FreeRADIUS supporte plusieurs versions du protocole EAP (Extensible Authentication Protocol) :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

https://wiki.freeradius.org/protocol/EAP

MD5

La version historique et la plus basique est la version MD5[p.720].

Le client est authentifié par le serveur qui utilise une authentification défi réponse. Une valeur aléatoire constituant le défi est envoyée au client, qui concatène à ce défi le mot de passe et en calcule, en utilisant l'algorithme MD5, le hash, une empreinte qu'il renvoie au serveur. Le serveur calcule sa propre empreinte connaissant le mot de passe, puis il compare les deux et valide ou non l'authentification.

La sécurité de cette version est faible. En cas d'écoute du trafic, il est possible de retrouver le mot de passe via force brute.

EAP-TLS

La version EAP-TLS[p.733] permet d'avoir un trafic chiffré entre le client et le serveur mais permet aussi, d'identifier le certificat présent sur le poste client.

Le serveur et le client possèdent chacun leur certificat qui va servir à les authentifier mutuellement, dans un fonctionnement similaire au protocole https.

Pour activer EAP-TLS, sélectionner `tls` dans la variable `Type de protocole d'authentification`.



Version TLS

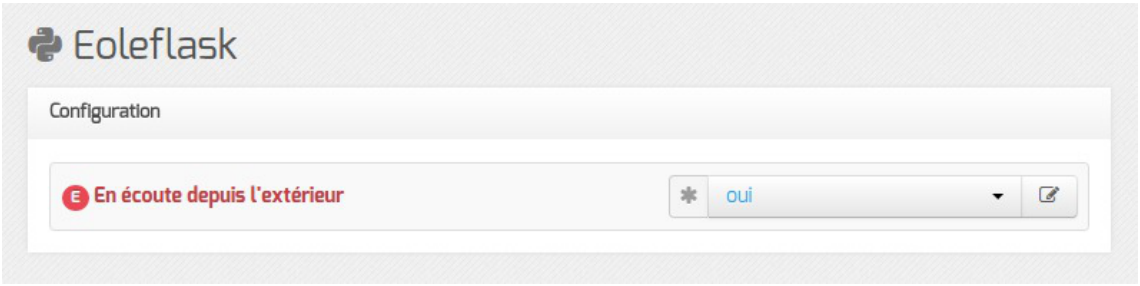
La version TLS 1.1 est désactivée au profit de la version 1.2 !

MD5

Ce mode n'est plus considéré comme sécurisé et ne permet pas d'identifier le poste.

4.39. 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

4.40. Onglet Lemonldap : Configuration du service SSO pour l'authentification unique (mode Expert)

Cette section décrit la configuration du serveur depuis l'interface de configuration du module disponible sur tous les serveurs EOLE.

Les valeurs définies par défaut simplifient la configuration dans le cadre d'une utilisation prévue sur certains des modules.

Installation de LemonLDAP::NG

Installation sur Scribe, AmonEcole ou Seth Éducation

Pour activer le serveur LemonLDAP::NG[p.717] sur les modules Scribe, AmonEcole ou Seth Éducation, il faut installer le paquet **eole-lemonldap-ng-auto**.

```
apt install eole-lemonldap-ng-auto
```

Le service sera alors pré-configuré pour utiliser l'annuaire du module.

Installation sur les autres modules

Pour activer le serveur LemonLDAP::NG sur les autres modules EOLE (Eolebase par exemple), il faut installer le paquet **eole-lemonldap-ng**.

```
apt install eole-lemonldap-ng
```

Les sources d'authentification seront à saisir dans l'interface de configuration du module.

Module Seth

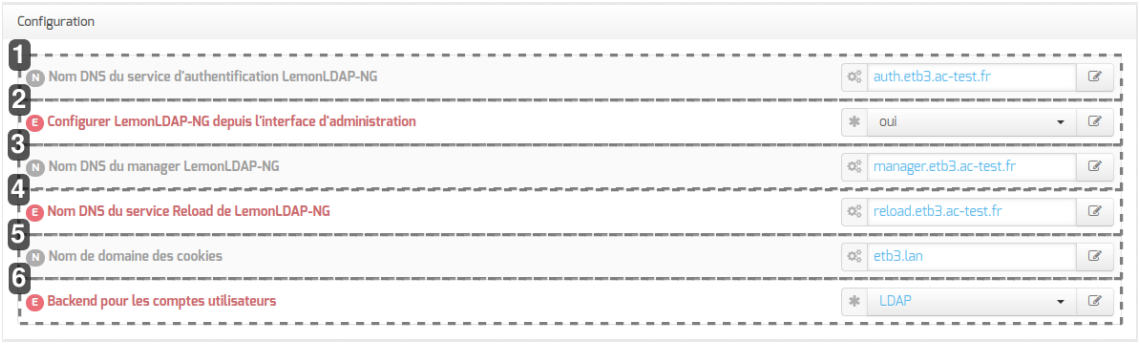
L'installation du paquet eole-lemonldap-ng-auto sur un module Seth transformera ce dernier en Seth Éducation !

LemonLDAP vs EoleSSO

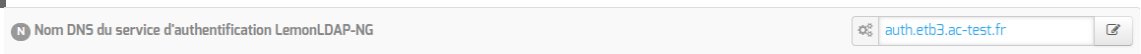
L'installation des paquets eole-lemonldap-ng et/ou eole-lemonldap-ng-auto entraîne la désinstallation du paquet **eole-sso-server** par le jeu des dépendances de paquets (dpkg[p.704]).

Partie Configuration

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



1



Nom DNS du service d'authentification LemonLDAP-NG

Variable calculée.

Nom interne de la variable

authWebName

2



Configurer LemonLDAP-NG depuis l'interface d'administration

Permet d'activer l'interface d'administration fournie par le projet LemonLDAP::NG.

Par défaut, cette interface est désactivée, les cas classiques de configuration étant pris en charge via les mécanismes EOLE.

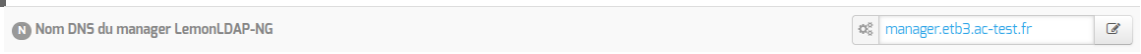
Conflit des modes de configuration

La configuration de LemonLDAP::NG depuis son interface d'administration écrase et remplace celle générée via les mécanismes EOLE.

Nom interne de la variable

ll_activer_manager

3



Nom DNS du manager LemonLDAP-NG

Indique le nom de domaine avec lequel le manager de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

managerWebName

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

4



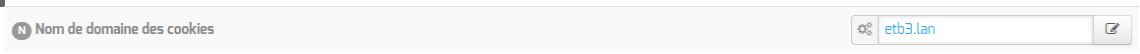
Nom DNS du service Reload LemonLDAP-NG

Indique le nom de domaine avec lequel le service de rechargement de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

reloadWebName

5



Nom de domaine des cookies

Cette variable est pré-remplie.

Nom interne de la variable

cookieDomain

6



Backend pour les comptes utilisateurs

Permet d'adapter le protocole utilisé en fonction du type d'annuaire associé. Le choix s'effectue entre les types LDAP et AD (annuaire de type OpenLDAP ou annuaire de type Active Directory).

Nom interne de la variable

lemon_user_db

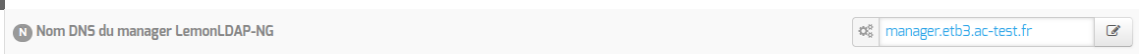
La variable `Nom DNS du service d'authentification LemonLDAP-NG` doit être renseignée avec le nom DNS du serveur précédé du nom du service.

La variable `Configurer LemonLDAP-NG depuis l'interface d'administration` permet d'activer l'interface d'administration de LemonLDAP::NG.

Si la variable est à oui une nouvelle variable apparaît en mode Normal et deux en mode Expert.



1



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nom DNS du manager LemonLDAP-NG

Indique le nom de domaine avec lequel le manager de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

managerWebName

2



Nom DNS du service Reload LemonLDAP-NG

Indique le nom de domaine avec lequel le service de rechargement de LemonLDAP::NG sera joignable. Cette variable est pré-remplie automatiquement.

Nom interne de la variable

reloadWebName

Si vous activez l'interface d'administration de LemonLDAP::NG vous perdrez la possibilité d'utiliser les outils EOLE pour interagir avec LemonLDAP::NG.

À ne choisir que si vous savez ce que vous faites !

La variable `Nom de domaine des cookies` à renseigner en cas d'utilisation d'un reverse proxy. Les cookies sont associés au nom utilisé par l'utilisateur pour accéder à un service web. Par défaut la valeur est celle du FQDN. Si vous utilisez un reverse proxy cette valeur n'est plus valable, il faut la remplacer par le chemin d'accès à la redirection du reverse proxy.

La variable `Backend pour les comptes utilisateurs` permet de choisir entre LDAP ou AD. pour les échangent.

Si vous utilisez Scribe mettre en mode LDAP

Si vous utilisez un seth ou un amonecole passer en mode AD.

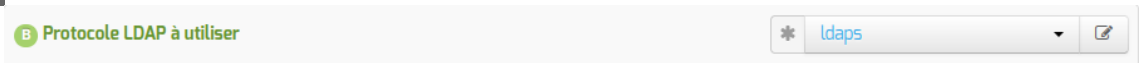
Partie Configuration LDAP

Dans cette partie vous avez accès aux paramètres propres à LemonLDAP::NG.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



1



Protocole LDAP à utiliser

Il est possible d'adapter le protocole à utiliser selon les capacités du serveur LDAP associé. Le choix se fait entre **ldaps** et **ldap**.

Nom interne de la variable

ldapScheme

2



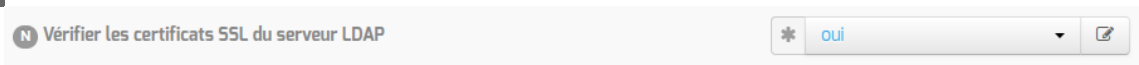
Port d'écoute du LDAP utilisé par LemonLDAP::NG

Port utilisé pour contacter l'annuaire.

Nom interne de la variable

ldapServerPort

3



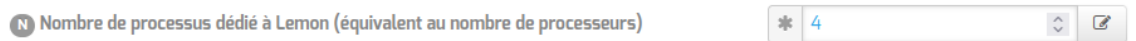
Vérifier les certificats SSL du serveur LDAP

Active ou désactive la vérification du certificat SSL fourni par l'annuaire dans le cas du protocole LDAPS

Nom interne de la variable

ldldapverify

4



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nombre de processus dédié à Lemon (équivalent au nombre de processeurs)

Permet de limiter les ressources allouées

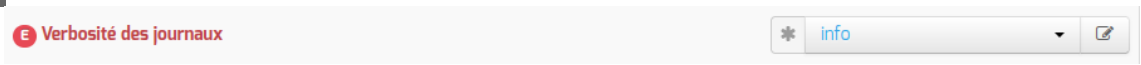
★

> Il est conseillé de ne pas allouer la totalité des files de traitement pour éviter de bloquer le système complètement en cas de charge excessive.

Nom interne de la variable

> lemonproc

5



Verbosité des journaux

Détermine la quantité d'informations rapportées par les services LemonLDAP::NG

- Info : remonte uniquement les logs informatifs
- notice : remonte les logs informatifs + notifications
- warn : remonte les logs informatifs + notifications + warning
- error : remonte les logs informatifs + notifications + warning + error
- debug : remonte tous les logs possible

Nom interne de la variable

> lm_loglevel

6



LemonLDAP Administrator username

Personnalise le nom de l'utilisateur avec les droits d'administration.

Nom interne de la variable

> lemonAdmin

Le serveur LemonLDAP::NG prend en charge LDAP over SSL (LDAPS). La fonction Strict SSL est définie par défaut. La fonction Strict SSL nécessite une certification de serveur.

La variable `Protocole LDAP à utiliser` permet de choisir entre `LDAP` et `LDAPS`

⚠

> Pour des interactions en LDAP avec Active Directory, prendre en compte que certaines actions nécessitent l'utilisation de LDAPS (LDAP sur SSL) entre le client et Active Directory

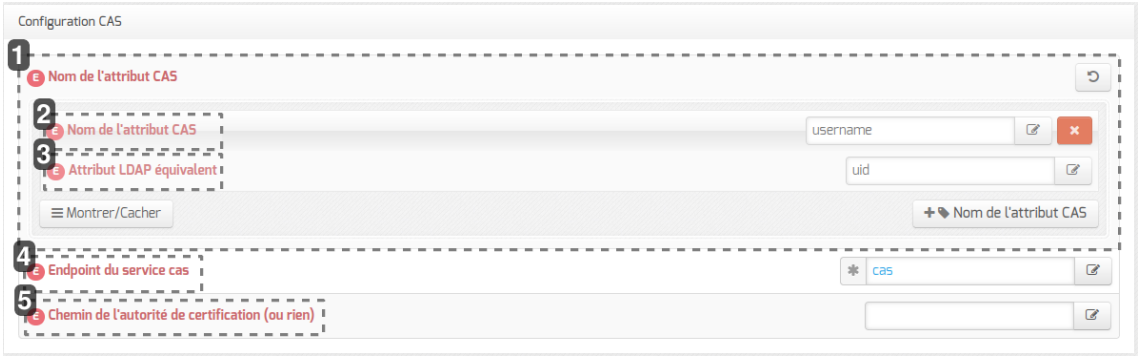
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La variable `Port d'écoute du LDAP utilisé par LemonLDAP::NG` permet de changer le port associé pour LDAP. Par défaut il s'agit du port `636`

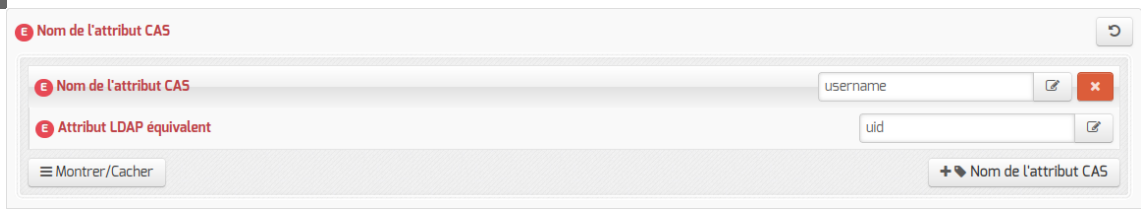
La variable `Vérifier les certificats SSL du serveur LDAP` permet de valider les certificats SSL pour l'authentification du serveur LemonLDAP::NG.

La variable `Nombre de processus dédié à Lemon (équivalent au nombre de processeurs)` indique le nombre de processus utilisés par LemonLDAP::NG. Par défaut cette variable est à 4, néanmoins il est préférable d'avoir ce nombre légèrement inférieur au nombre de processeurs.

Configuration CAS



1



Nom de l'attribut CAS

Cette variable multivaluée permet d'associer des noms d'attribut CAS avec des noms d'attribut LDAP. Cette association permet de fournir au protocole CAS les attributs qui lui sont nécessaires quand ils n'existent pas avec le même nom dans l'annuaire.

2



Nom de l'attribut CAS

Le nom de l'attribut CAS correspond au membre du couple utilisé côté CAS.

⚠

> Les attributs sont sensibles à la casse.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Nom interne de la variable

casAttribute

3

Attribut LDAP équivalent

Attribut LDAP équivalent

Le nom de l'attribut LDAP correspond à l'attribut LDAP dont la valeur sera associée au nom de l'attribut CAS précédent.

⚠

Les attributs sont sensibles à la casse.

Nom interne de la variable

casLDAPAttribute

4

Endpoint du service cas

Endpoint du service cas

Complément d'url qui permet d'accéder au service CAS.

Nom interne de la variable

casFolder

5

Chemin de l'autorité de certification (ou rien)

Chemin de l'autorité de certification

Emplacement du certificat de l'autorité de certification permettant de valider l'accès si nécessaire.

Nom interne de la variable

ssoCALocation

LemonLDAP::NG. peut être utilisé comme un serveur CAS[p.705]. Il peut permettre de fédérer LemonLDAP::NG. avec :

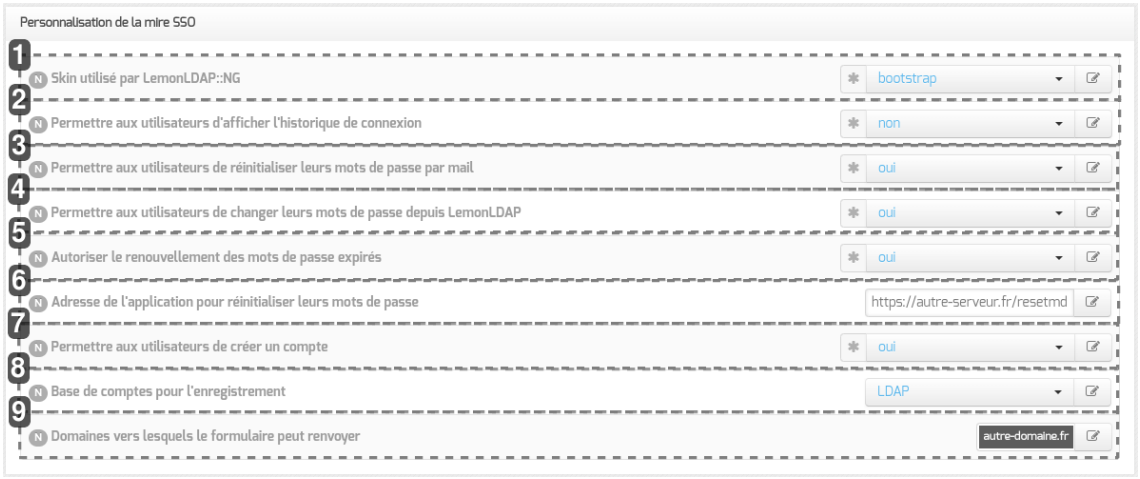
- Un autre fournisseur d'authentification CAS LemonLDAP::NG.
- Tout client CAS

LemonLDAP::NG. est compatible avec le protocole CAS versions 1.0, 2.0 et une partie de la 3.0

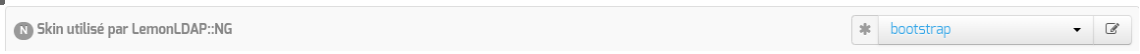
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

(échange d'attributs).

Partie Personnalisation de la mire SSO



1



Skin utilisé par LemonLDAP::NG

Sélectionne l'aspect visuel de la mire d'authentification parmi les thèmes proposés par l'application LemonLDAP::NG :

- bootstrap
- dark
- impact
- pastel

Nom interne de la variable

llSkin

2



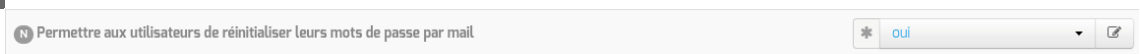
Permettre aux utilisateurs d'afficher l'historique de connexion

Active l'affichage de son historique de connexion pour chaque utilisateur.

Nom interne de la variable

llCheckLogins

3



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Permettre aux utilisateurs de réinitialiser leurs mots de passe par mail

Active la fonctionnalité de réinitialisation autonome de mot de passe en cas de perte.

Nom interne de la variable

llResetPassword

4



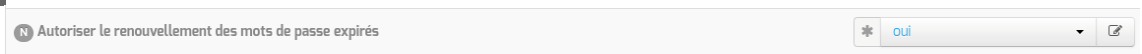
Permettre aux utilisateurs de changer leurs mots de passe depuis LemonLDAP

Active le formulaire de changement de mot de passe.

Nom interne de la variable

llChangePassword

5



Autoriser le renouvellement des mots de passe expirés

Permet le renouvellement du mot de passe depuis la mire dans le cas d'une expiration.

Nom interne de la variable

llResetExpiredPassword

6



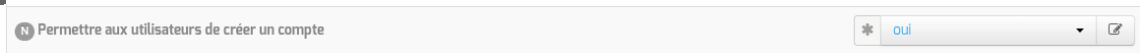
Adresse de l'application pour réinitialiser leurs mots de passe

Adresse du formulaire à présenter aux utilisateurs pour leur permettre de réinitialiser leur mot de passe

Nom interne de la variable

llResetUrl

7



Permettre aux utilisateurs de créer un compte

Donne le droit aux utilisateurs de créer un compte.

Nom interne de la variable

llRegisterAccount

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

8



Base de comptes pour l'enregistrement

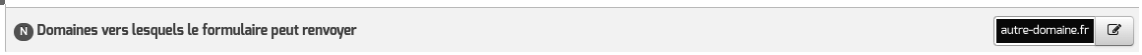
Type de base pour l'enregistrement des comptes créés parmi les choix suivants :

- LDAP
- AD
- Demo
- Custom

Nom interne de la variable

llRegisterDB

9



Domaines vers lesquels le formulaire peut renvoyer

Liste des domaines autorisés depuis le formulaire.

Nom interne de la variable

llCSPTargets

La variable `Skin utilisé par LemonLDAP:NG` permet de choisir le skin utilisé par LemonLDAP::NG.

La variable `Permettre aux utilisateurs d'afficher l'historique de connexion` permet aux utilisateurs lorsqu'elle est à `oui`, d'afficher leur historique de connexion.

La variable `Permettre aux utilisateurs de réinitialiser leurs mots de passe par mail` met en place la possibilité pour les utilisateurs de modifier leurs mots de passe depuis la fenêtre de connexion. La méthode consiste à demander la confirmation de l'adresse mail de l'utilisateur, si celle-ci correspond il recevra un mail avec un lien pour changer son mot de passe.

La variable `Permettre aux utilisateurs de changer leurs mots de passe depuis LemonLDAP` permet aux utilisateurs de changer librement leur mot de passe de depuis la page de gestion LemonLDAP::NG correspondant par défaut à la variable `Nom DNS du service d'authentification LemonLDAP-NG` ou variable Creole `authWebName`

La variable `Autoriser le renouvellement des mots de passe expirés` autorise le renouvellement par l'utilisateur.

Dans ce cas il est possible avec la variable `Adresse de l'application pour réinitialiser leurs mots de passe` d'indiquer une application ou un service spécifique (compatible LDAP,

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

LDAPS, et LemonLDAP::NG) pour cette opération.

La variable `Permettre aux utilisateurs de créer un compte` autorise les utilisateurs à créer des comptes supplémentaires en lieu et place de l'administrateur, depuis l'interface LemonLDAP::NG.

La Variable `Base de comptes pour l'enregistrement` vous permet de choisir le type de base que vous voulez parmi 4 possibilités :

- Une base LDAP
- Une base AD
- Une base de démonstration
- Une base personnalisable.

Si vous choisissez une base personnalisable une nouvelle variable apparaîtra. `Adresse de l'application de création de compte` qu'il faut remplir en indiquant le service ou l'application qui va remplir la base.



1

Adresse de l'application de création de compte

Indiquer l'adresse de l'application de création de compte alternative. (https://.....)

Nom interne de la variable

llRegisterURL

La variable `Domaines vers lesquels le formulaire peut renvoyer`, concerne tous services ou applications externes au domaine du serveur LemonLDAP::NG vers lesquels il doit cependant pouvoir, soit donner accès, soit interagir.

Documentation annexe

Site officiel : LemonLDAP::NG [https://lemonldap-ng.org/]

Documentation officielle (en anglais) : Documentation [https://lemonldap-ng.org/documentation/latest/]

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.709] permet de les isoler d'attaques provenant de l'intérieur (par exemple des services saturés par un virus utilisant le broadcast[p.705]) et de les placer dans une zone où l'accès aux autres réseaux de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

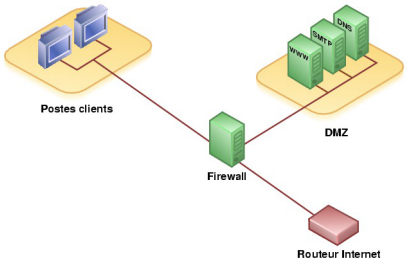


Diagramme d'une DMZ

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.722]) 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.

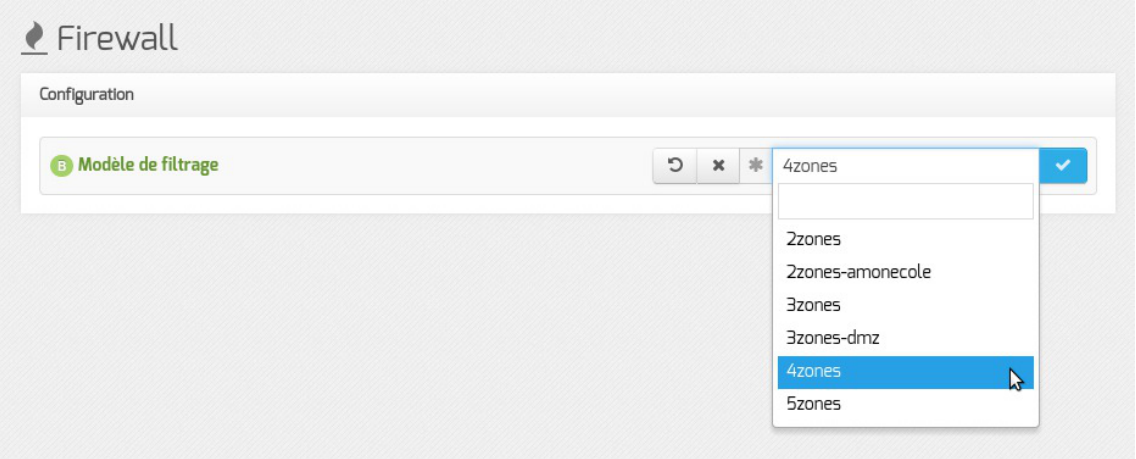
Configuration automatique

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 l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.



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/`.

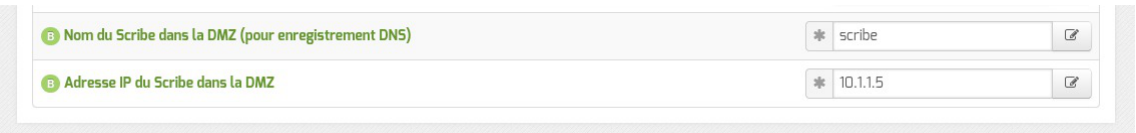
Avec ERA il est possible de créer un nouveau modèle personnalisé dans le répertoire `/usr/share/era/modeles/`. Celui-ci apparaîtra dans la liste des modèles proposés par défaut.

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.133]

ERA, éditeur de règles pour le module Amon [p.517]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.



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`.



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

L'autorisation d'accès au port configuré est gérée par ERA via la directive optionnelle cachée [p.709] : `ead scribe`.

Voir aussi...

Onglet Ead-web : EAD et proxy inverse [p.275]

Onglet Reverse proxy : Configuration du proxy inverse [p.167]

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.723] (exemple : `monetab.ac-acad.fr`). Celui-ci doit être résolvable depuis Internet et il faut le renseigner partout où cela est nécessaire.

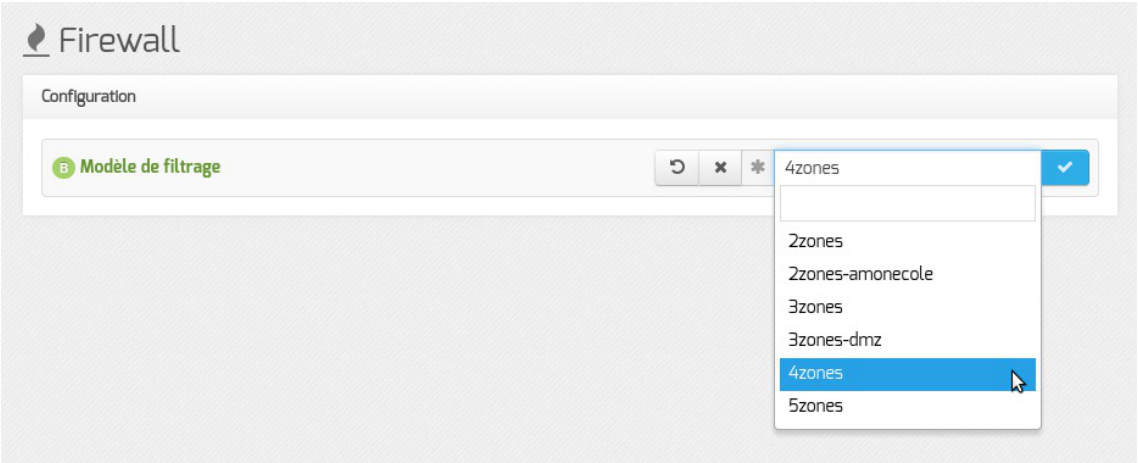
Ce nom de domaine sera à utiliser tant depuis l'extérieur de l'établissement que depuis l'intérieur.

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 l'interface 1 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 2 ;
- **4zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2 et d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 ;
- **5zones** : gestion d'une zone admin sur l'interface 1, d'une zone pedago sur l'interface 2, d'une zone DMZ publique pouvant accueillir un module Scribe sur l'interface 3 et d'une zone DMZ privée sur l'interface 4.



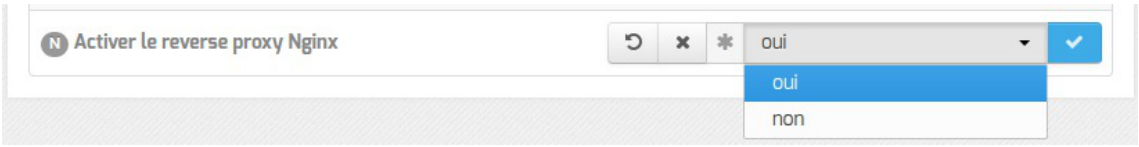
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

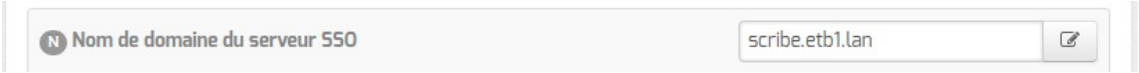


L'activation du service fait apparaître un nouvel onglet nommé `Reverse proxy`.



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

Redirection de services particuliers

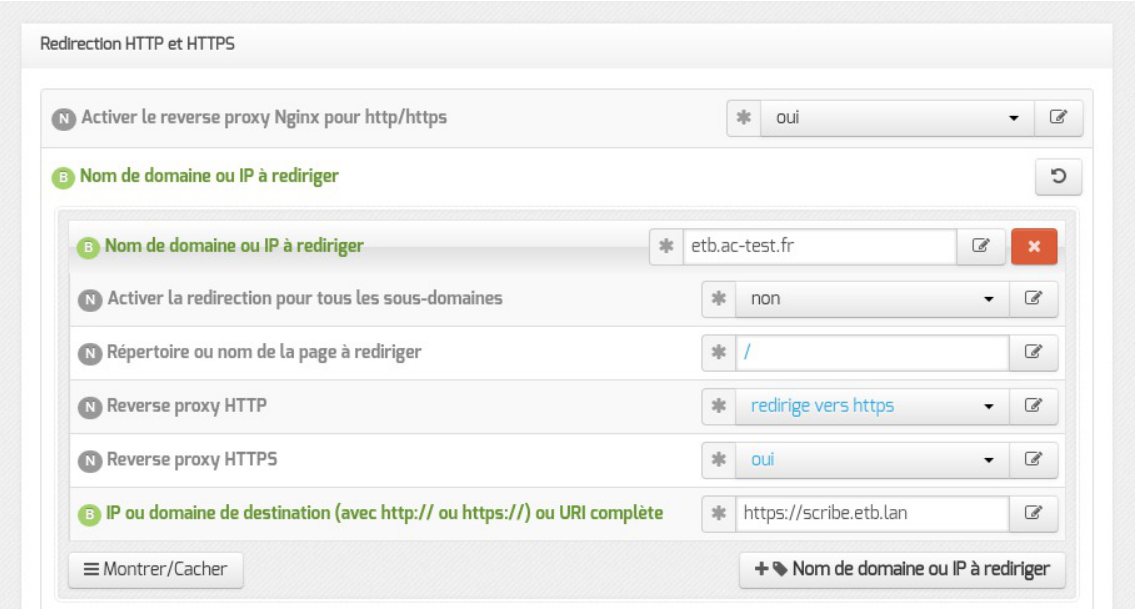


Pour rediriger le service EoleSSO (port 8443) il faut indiquer l'adresse IP ou le nom de domaine interne de la machine de destination (adresse IP ou le nom de domaine interne du module Scribe). Si le service EoleSSO est activé localement il est impossible de réaliser une redirection pour ce service.

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

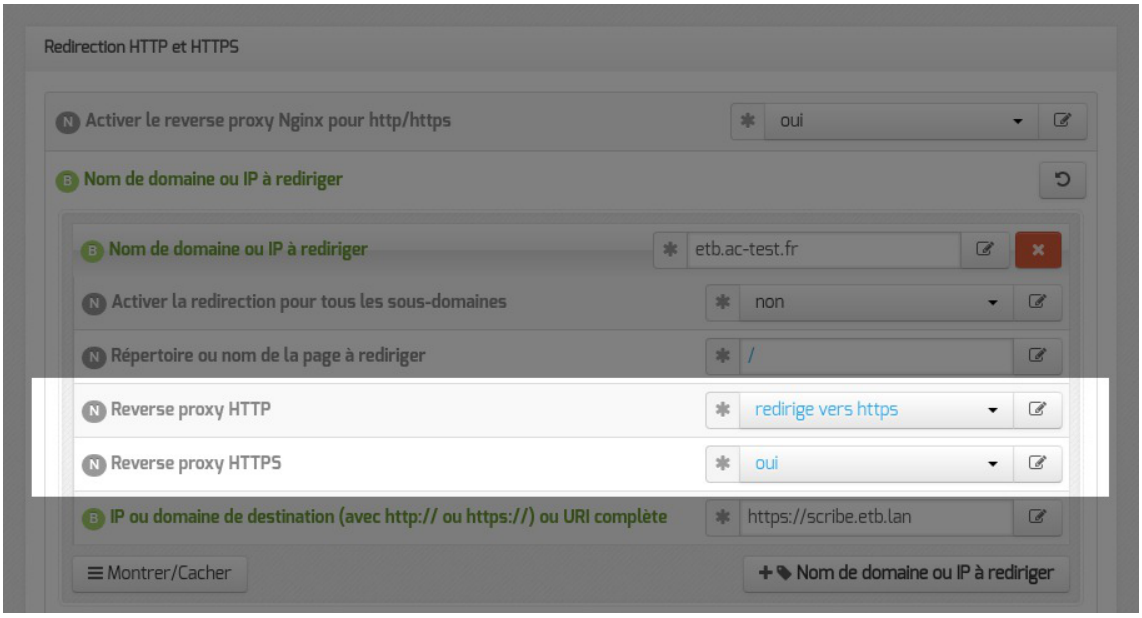
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 ;
- `Activer la redirection pour tous les sous-domaines` : cette variable est disponible à partir de la version 2.6.2 d'EOLE, elle permet la prise en charge de tous les sous-domaines par le proxy inverse ;
- `Demander un certificat à Let's Encrypt pour ce domaine` ? : cette variable est disponible à partir de la version 2.6.2 d'EOLE si la redirection pour tous les sous-domaines n'est pas activé et que le certificat SSL est Let's Encrypt ;
- 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.734] (exemple : `http://scribe.monetab.fr/webmail/`) du serveur de destination hébergeant la ou les applications.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

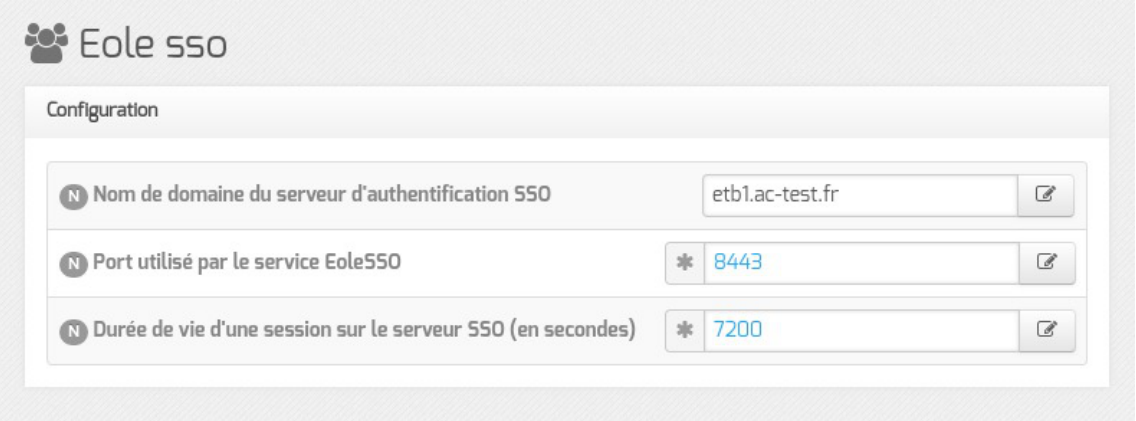


Un répertoire déterminé peut également être redirigé vers un serveur différent. Par exemple le lien vers l'application Pronote[p.727], `https://monetab.fr/pronote/` peut être redirigé vers `http://pronote.monetab.fr/` (attention, le "/" final est important, puisqu'il faut rediriger à la racine du serveur de destination).

Activation de l'authentification unique

Si vous voulez activer le service EoleSSO sur le module Amon, `Utiliser un serveur EoleSSO` à `distant` dans l'onglet `Services`, dans l'onglet `Eole sso`, seuls les paramètres `Nom de domaine du serveur d'authentification SSO` et `Port utilisé par le service EoleSSO` sont requis et les autres options ne sont pas disponibles car elles concernent le paramétrage du serveur local.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Configuration d'un serveur EoleSSO distant

L'option `Nom de domaine du serveur d'authentification SSO` doit être configurée avec le nom de domaine public utilisé dans Envole (typiquement : *monetab.ac-monacad.fr*).

Dans ce cas l'utilisateur `admin` du module Scribe sera administrateur du module Amon.

Dans le cas de l'utilisation du serveur EoleSSO local, `Nom de domaine du serveur d'authentification SSO` doit être renseigné avec le nom DNS du serveur.

Nom de domaine et récapitulatif de la configuration

Le nom de domaine doit être renseigner à de multiples endroits de la configuration.

- onglet `Général` : choisir le modèle de filtrage ;
- onglet `Services` :
  - Activer le proxy inverse Nginx : `oui` ;
- onglet `Eole sso` :
  - Nom de domaine du serveur d'authentification SSO : `etab.ac-acad.fr` ;
- onglet `Applications web` si module AmonEcole :
  - Nom de domaine des applications web (sans http://) : `etab.ac-acad.fr` ;
- onglet `Reverse proxy` :
  - Nom de domaine par défaut : `etab.ac-acad.fr` ;
  - Nom de domaine du serveur SSO : `etab.ac-acad.fr` ;
  - Activer la configuration automatique pour les applications locales à `oui`.
- onglet `Certificats ssl` uniquement en mode expert :
  - Nom DNS/IP alternatif du serveur : `etab.ac-acad.fr` *(ré-générer les certificats si nécessaire)*.

Voir aussi...

Onglet Firewall [p.112]

Onglet Reverse proxy : Configuration du proxy inverse

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

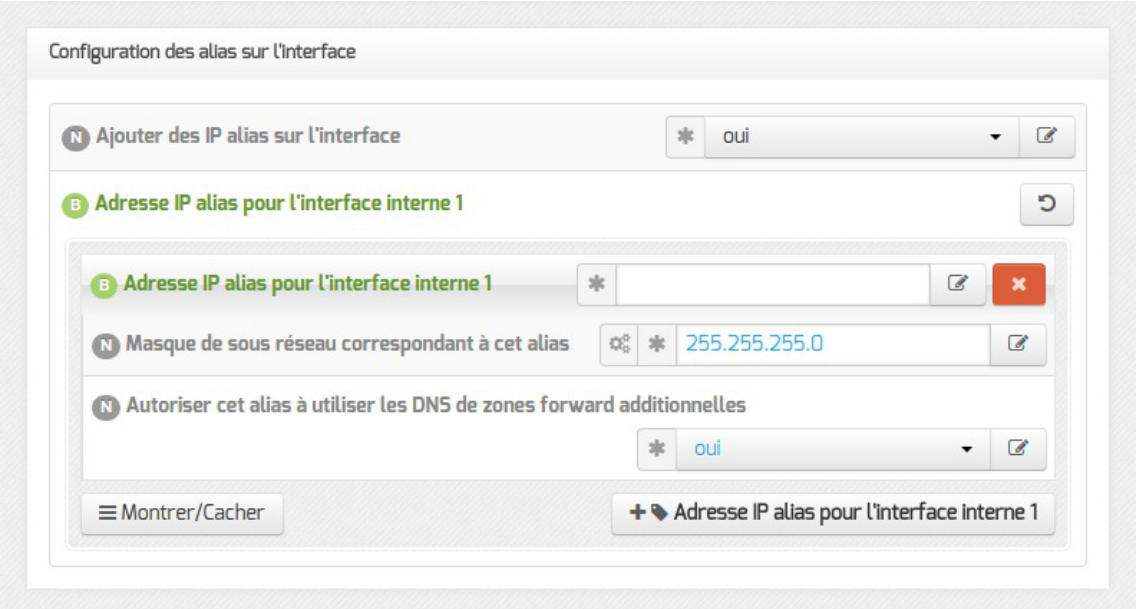
Onglet Eole sso : Configuration du service SSO pour l'authentification unique

ERA, éditeur de règles pour le module Amon [p.517]

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

La variable `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`.

Il est possible d'ajouter d'autres adresses IP alias sur l'interface en cliquant sur le bouton `+ Adresse IP alias pour l'interface n`.

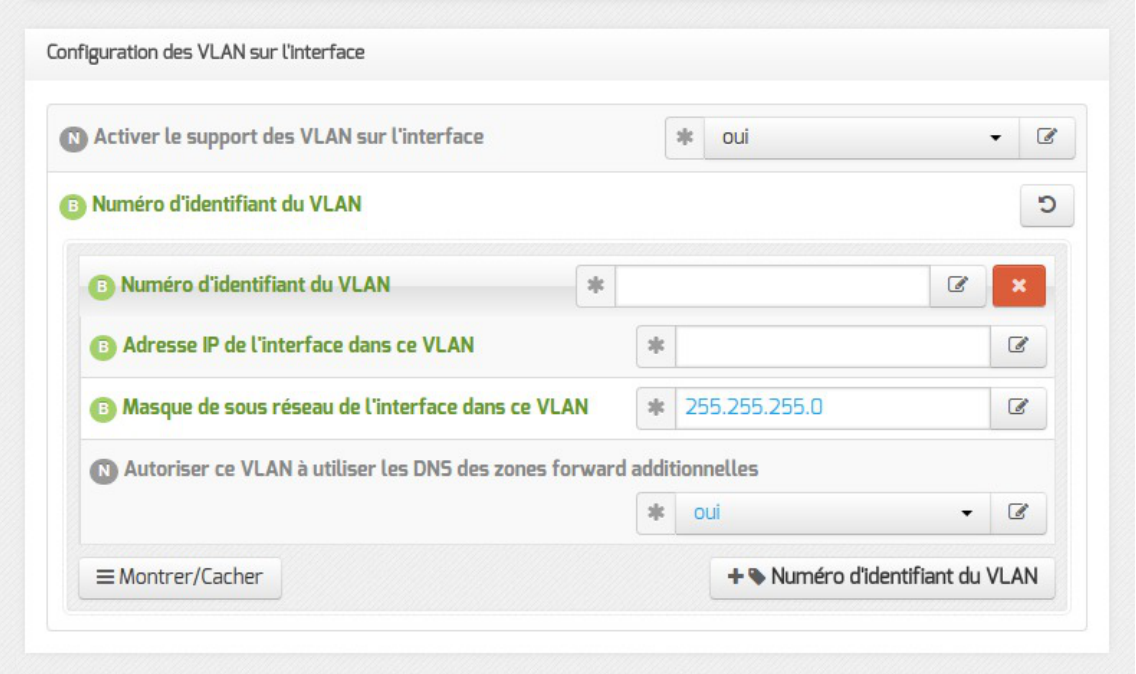
Si le support du RVP est activé une option supplémentaire est disponible :

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

Configuration des VLAN sur l'interface

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Il est possible de configurer des VLAN[p.734] (réseau local virtuel) sur une interface déterminée du module.



Pour cela, il faut activer le support des VLAN (`Activer le support des VLAN sur l'interface` à `oui`) puis ajouter un VLAN à l'aide du bouton `+ Numéro d'identifiant du VLAN` et configurer l'ensemble des paramètres obligatoires :

- le numéro du VLAN ;
- l'adresse IP de l'interface dans ce VLAN ;
- le masque de sous réseau de l'interface dans ce VLAN.

La variable `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`.

Il est possible d'ajouter d'autres VLAN sur l'interface en cliquant sur le bouton `+ Numéro d'identifiant du VLAN`.

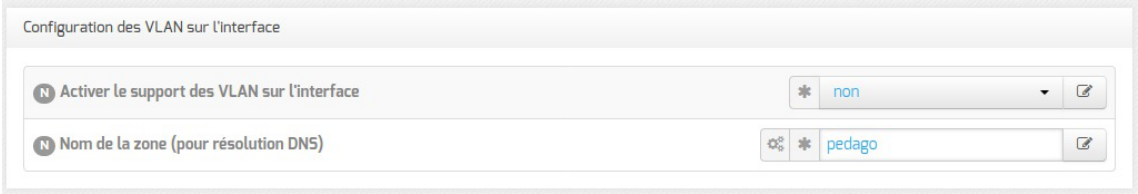
Si le support du RVP est activé une option supplémentaire est disponible :

- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



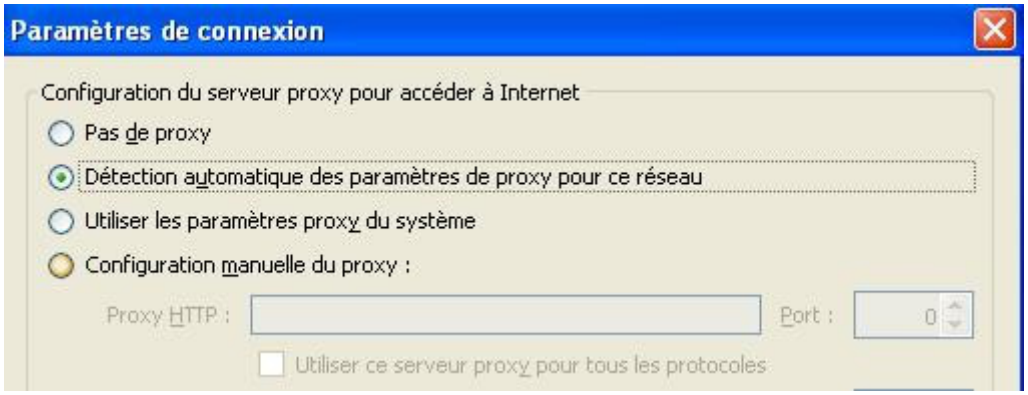
- `Nom de la zone (pour résolution DNS)` : entrée DNS correspondant à l'adresse IP de l'interface. Le nom (par défaut admin pour l'interface 1) doit être différent pour chacune des interfaces.

9. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.734] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

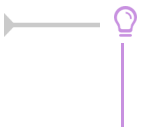
Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine_local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.



La détection automatique du proxy par les navigateurs peut notamment être imposée par GPO[p.713].

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.722] 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

environnement Amon / Scribe ou Amon / Horus il faut configurer correctement les deux modules.

Configuration sur le module Scribe

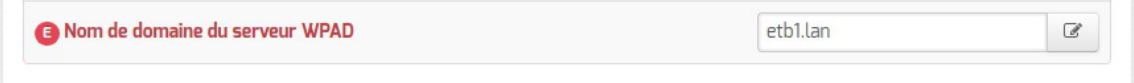
Le serveur DHCP doit être activé et correctement configuré sur le module Scribe (ou AmonEcole).

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 utilisée pour accéder au fichier WPAD tandis que pour des postes de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.



Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.



Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

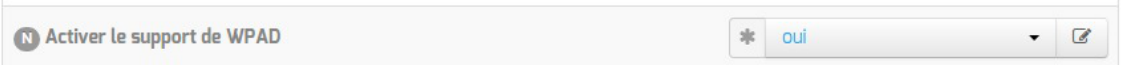
Configuration sur le module Amon

WPAD est mis à disposition sur les modules Amon et AmonEcole au travers du paquet `eole-wpad`.

Sur un module personnalisé, il n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

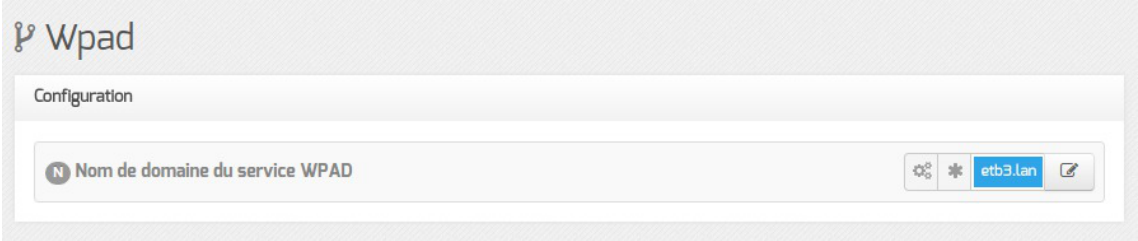
Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

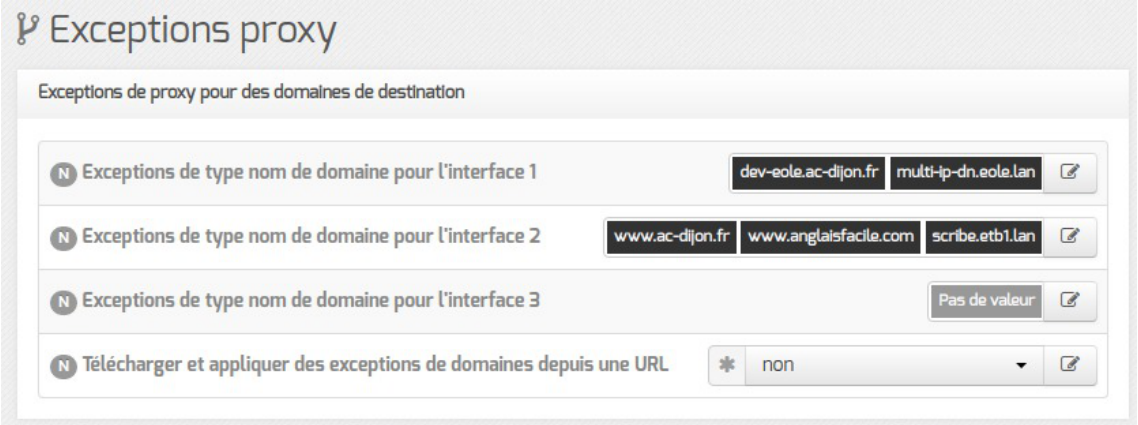
Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

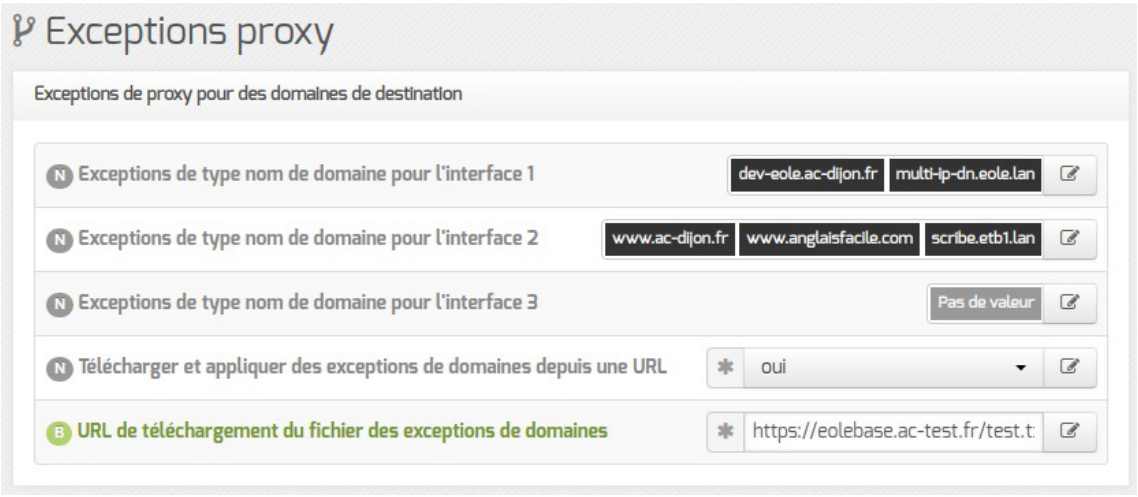
Exception de proxy pour des domaines de destination

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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



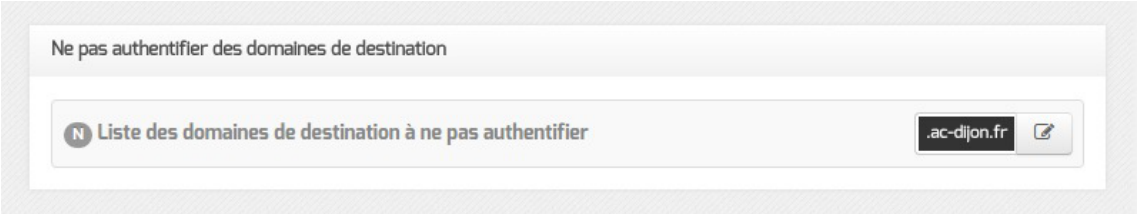
Il est également possible de fournir une liste de noms de domaine ou d'IP à inclure dans les exceptions au proxy depuis une URL, en activant la variable `Télécharger et appliquer des exceptions de domaine depuis une URL`.



Si vous utilisez une copie des modèles ERA fournis, il faudra l'adapter pour obtenir les règles supplémentaires

Exception au niveau de l'authentification des domaines de destination

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



Si WPAD est activés sur l'interface réseau, les utilisateurs utiliseront directement Squid pour accéder à ces sites.

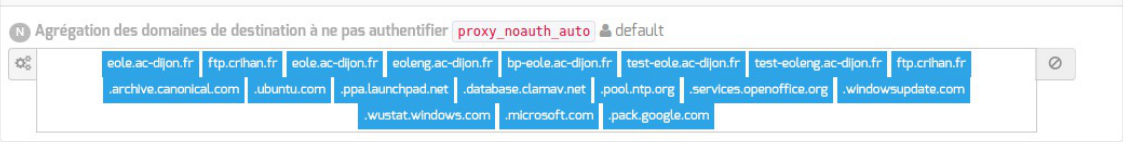
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

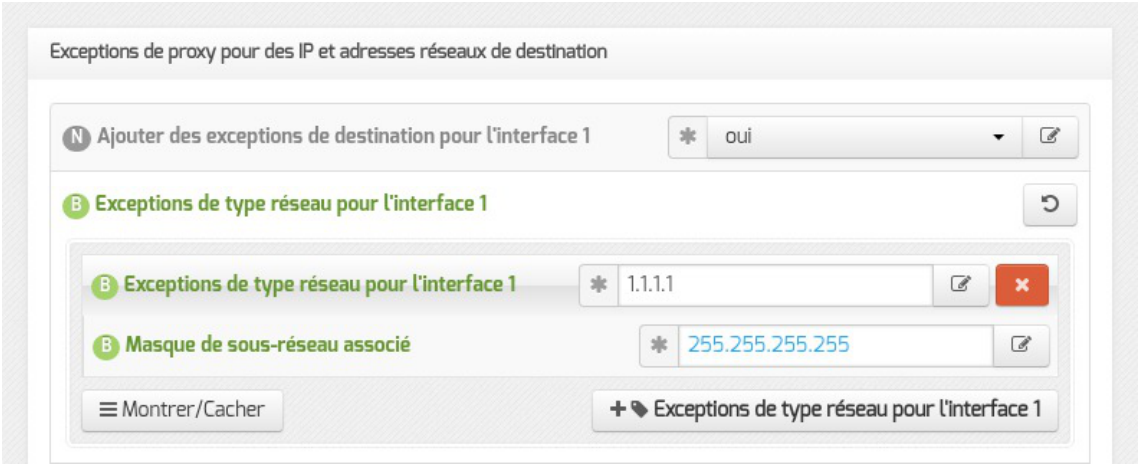
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



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

Exceptions de proxy pour des IP et adresses réseaux de destination

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.

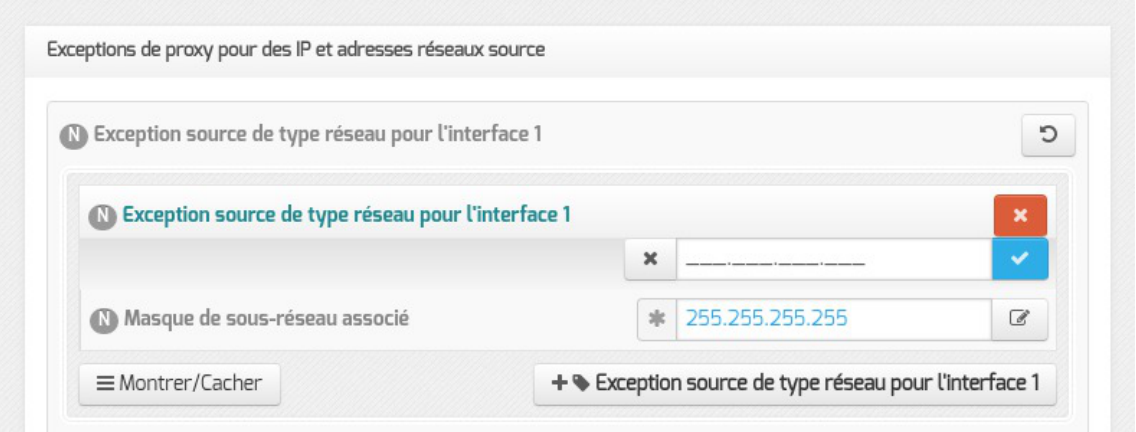


Le bouton `Exceptions de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.

Exceptions de proxy pour des IP et adresses réseaux source

Cette exception spécifique à ERA permet de déclarer une adresse IP ou une plage d'adresses IP **source** pour laquelle on ne passe pas par le proxy.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

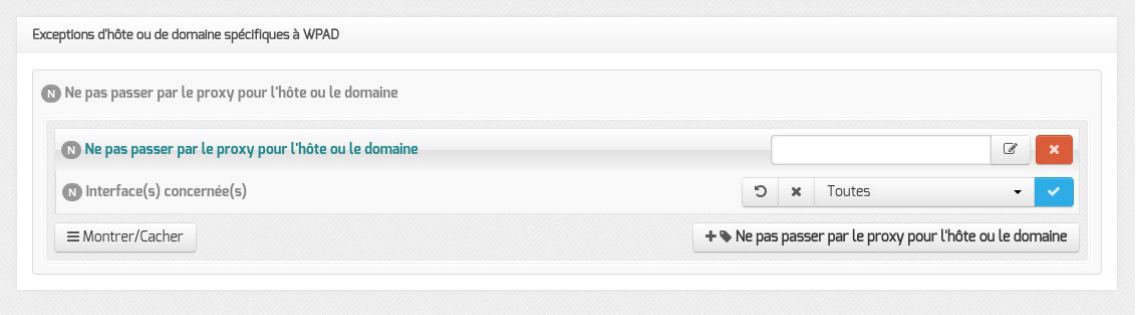


Le bouton `+ Exception source de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.

Cette fonctionnalité permet à une machine de contourner le proxy ce qui constitue un non respect des règles légales de sécurité. Elle peut servir pour effectuer des tests de proxy et d'exceptions de filtrage.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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

10. Paramétrage de l'authentification Squid pour le module Seth

Configuration de l'authentification KERBEROS si le proxy avec le module Seth en DMZ

Le module Amon doit pouvoir utiliser le service DNS du serveur Seth mais le service DNS du serveur Seth en DMZ ne peut pas interroger de DNS externe ce qui empêche notamment les machines de résoudre l'adresse du serveur NTP.

Pour contourner cette difficulté la déclaration du module Seth se fait en tant que Scribe DMZ sur le module Amon via l'interface de configuration du module.

Résolution DNS

Pour la résolution DNS il faut ajouter l'adresse IP du module Seth comme serveur DNS à l'adresse déjà déclarée, dans l'onglet `Général` → `Paramètres globaux` → `Adresse IP du serveur DNS`.



> L'ordre à une importance, l'adresse saisie en dernière peut être passée devant à l'aide du bouton .

Déclarer le module Seth dans la DMZ

Dans l'onglet `Firewall` il faut passer `Activer la gestion d'un Scribe dans la DMZ` à `oui` puis saisir le nom de machine du module Seth dans le champ `Nom du Scribe dans la DMZ (pour enregistrement DNS)` et saisir l'adresse IP du module Seth dans le champ `Adresse IP du Scribe dans la DMZ`.

Configuration de l'authentification KERBEROS

Dans l'onglet `Proxy authentifié`, passer le `Type d'authentification` à `NTLM/KERBEROS` puis saisir le nom de machine dans le champ `Nom du contrôleur de domaine KERBEROS`, le nom du domaine KERBEROS dans le champ `Nom du domaine KERBEROS (fqdn)` ainsi que le `Nom du domaine Windows` dans le champ du même nom. Enfin saisir l'adresse IP sur serveur Seth dans le champ `Adresse IP du contrôleur de domaine KERBEROS`.

> Les noms de domaine KERBEROS et Windows se retrouve dans l'interface de configuration du module Seth dans l'onglet `Active Directory` instancié en activant le mode Debug.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Application de la configuration

Pour que la configuration soit appliquée il faut exécuter la commande `reconfigure` sur le serveur Amon.

État du serveur Seth

La commande `diagnose` montre les services DNS et NTP valide. Il peut être nécessaire de reconfigurer le module Seth pour obtenir ce résultat.

Enregistrement du serveur au domaine

Il est nécessaire d'enregistrer le module Amon auprès du serveur de domaine.

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 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`.

11. Paramétrage de l'authentification Squid avec un serveur Windows

Configuration de l'authentification avec un serveur Windows sur la zone pédago

Le module Amon doit pouvoir utiliser le service DNS du serveur Windows mais il faut autoriser explicitement le serveur AD a accéder à des serveurs DNS.

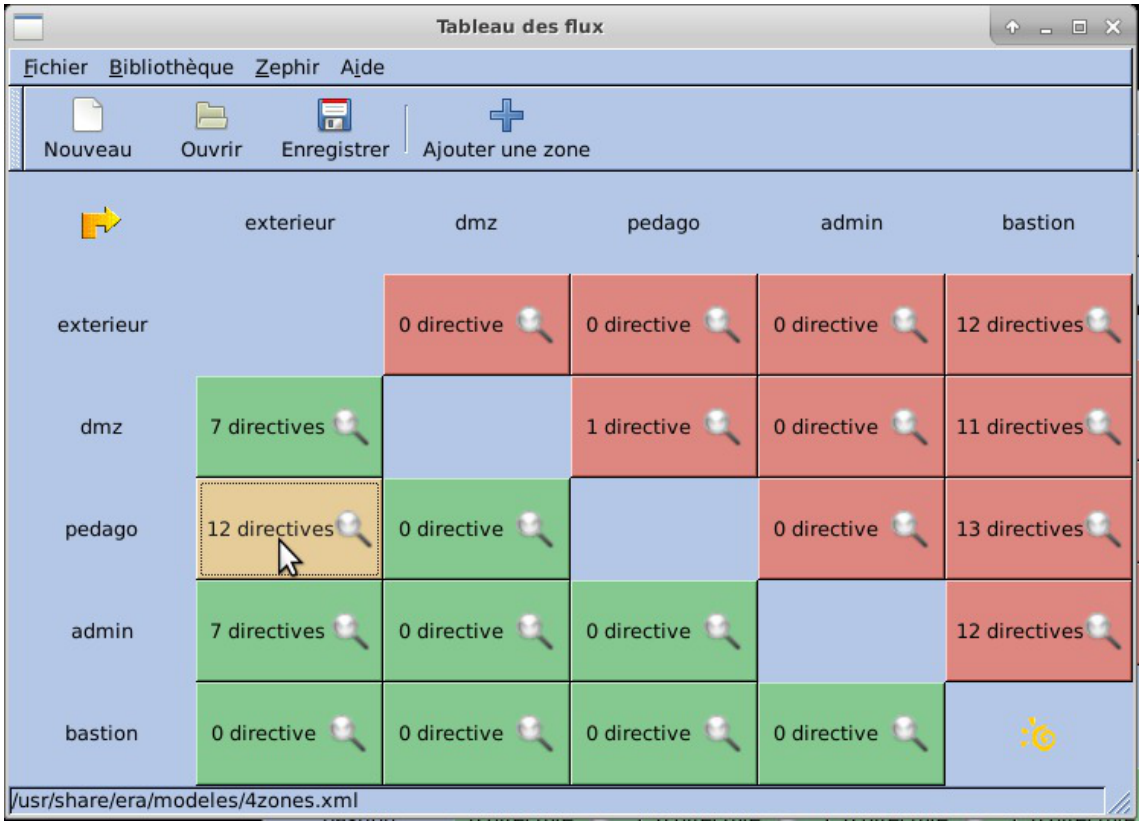
Résolution DNS

Se connecter sur le serveur Amon et éditer le modèle ERA afin d'autoriser les requêtes DNS depuis la zone pédago :

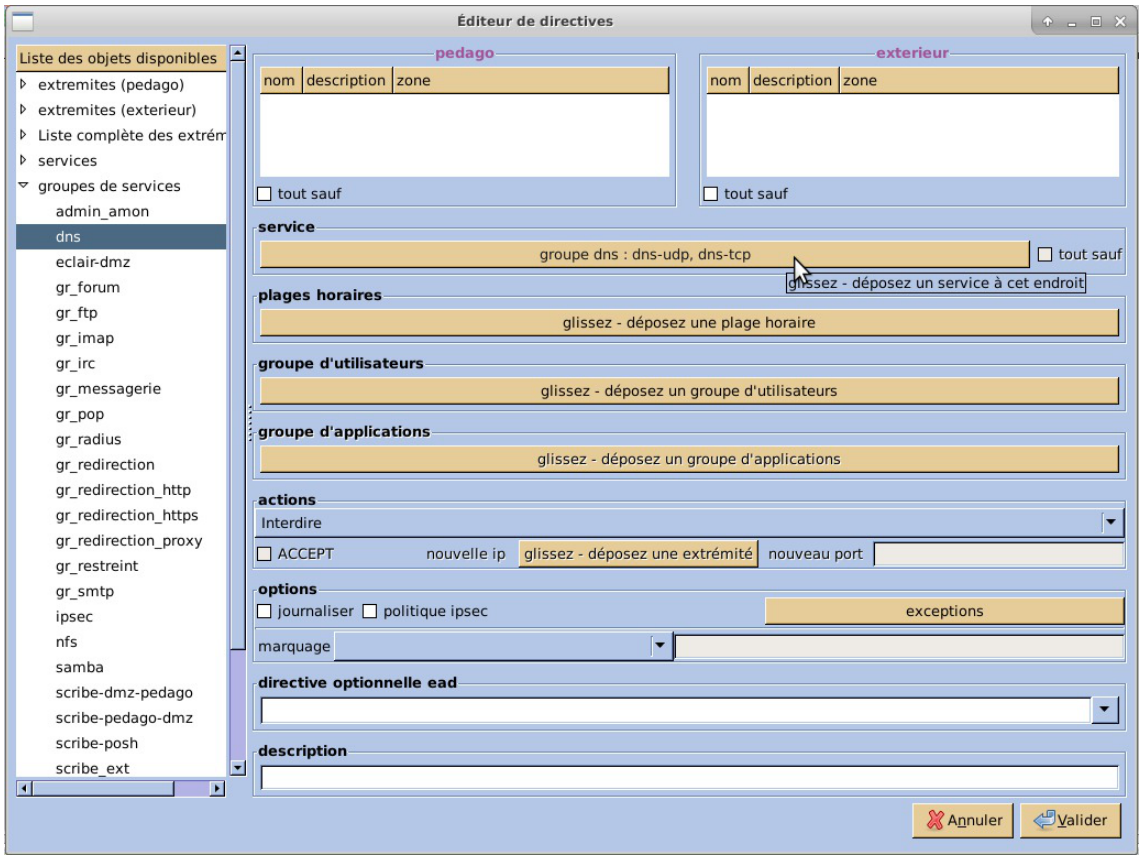
```
# era -f /usr/share/era/modeles/$(CreoleGet type_amon).xml
```

- cliquer sur la case verte : pedago → exterieur ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

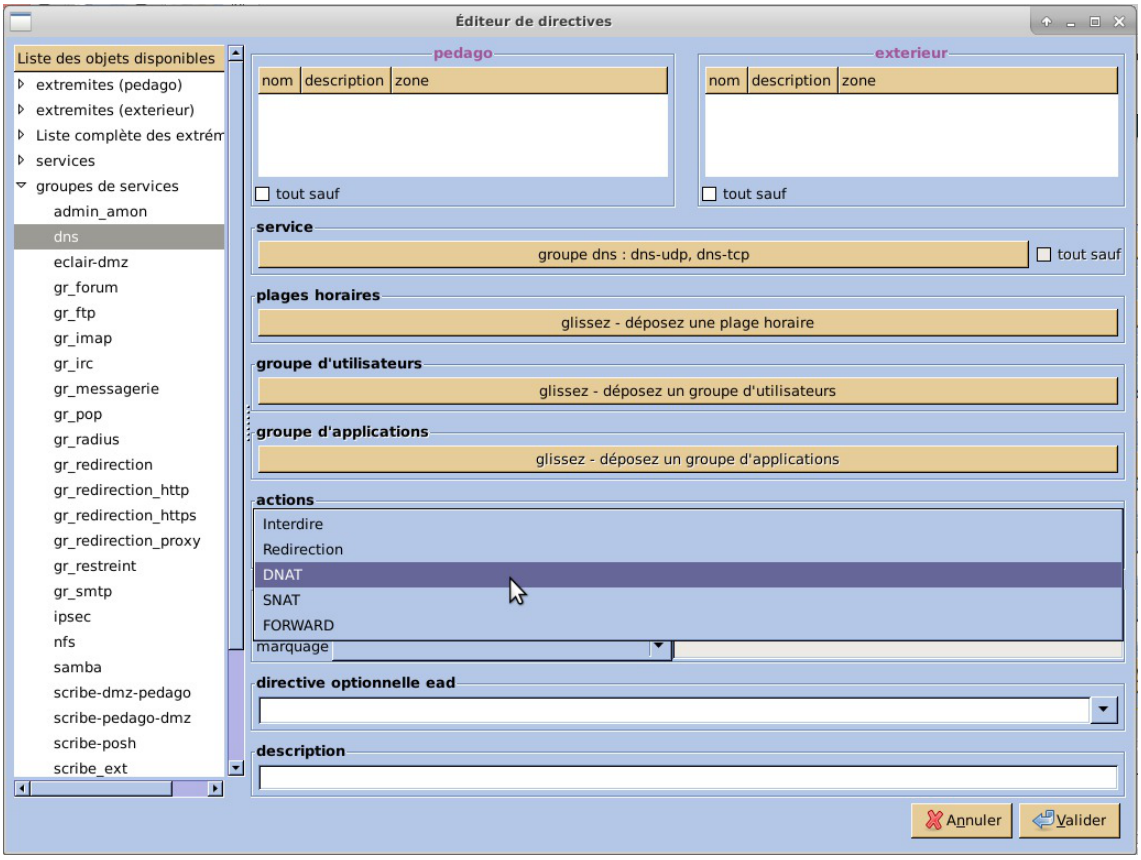


- dans la fenêtre s'affiche la liste des directives, cliquer sur le bouton `+ Ajouter` ;
- faire glisser `dns` depuis l'item `groupe de services` sur la partie de gauche la case beige "glissez - déposez un service" de la partie `Service` ;



- dans la partie Actions, sélectionner DNAT et cocher la case ☑ ACCEPT ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- cliquer sur le bouton `Valider` de l'éditeur de directive puis sur le bouton `Valider` de la fenêtre de confirmation ;
- quitter l'éditeur de directive ;
- quitter la liste des directives ;
- cliquer sur le bouton `Enregistrer` et Quitter.

Re-générer les règles ERA

Re-générer les règles ERA à l'aide de la commande :

```
# bastion regen
```

Modifier la configuration du module

Ouvrir l'interface de configuration du module.

Configuration de l'authentification Kerberos

Dans l'onglet `Proxy authentifié`, passer le `Type d'authentification` à `NTLM/KERBEROS` puis saisir le nom de machine dans le champ `Nom du contrôleur de domaine KERBEROS`, le nom du domaine KERBEROS dans le champ `Nom du domaine KERBEROS (fqdn)` ainsi que le Nom du domaine Windows dans le champ du même nom. Enfin saisir l'adresse IP sur serveur Seth dans le champ `Adresse IP du contrôleur de domaine KERBEROS`.

Les noms de domaine KERBEROS et Windows se retrouve dans l'interface de configuration du module Seth dans l'onglet `Active Directory` instancié en activant le mode Debug.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Application de la configuration

Pour que la configuration soit appliquée il faut exécuter la commande `reconfigure` sur le serveur Amon.

Enregistrement du serveur au domaine

Il est nécessaire d'enregistrer le module Amon auprès du serveur de domaine.

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 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`.

12. Mise en place de l'agrégation de liens Ethernet (bonding)

Activation de l'agrégation de liens Ethernet

L'activation de l'agrégation de liens Ethernet[p.702] s'effectue en déclarant au minimum deux interfaces réseau dans la variable experte `Nom de l'interface réseau` dans un onglet `Interface-n`.



L'utilisation de l'agrégation de liens Ethernet[p.702] nécessite de disposer d'un Commutateur réseau[p.706] compatible et configuré.

Pour configurer l'agrégation de liens Ethernet, il faut rafraîchir l'onglet (cliquer sur un autre onglet et revenir #21016 [https://dev-eole.ac-dijon.fr/issues/21016]).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Configuration de l'agrégation de liens Ethernet



Il est possible de choisir le mode d'agrégation en accord avec la configuration de votre Commutateur réseau[p.706] parmi :

- balance-rr ;
- active-backup ;
- balance-xor ;
- broadcast ;
- 802.3ad ;
- balance-tlb ;
- balance-alb.

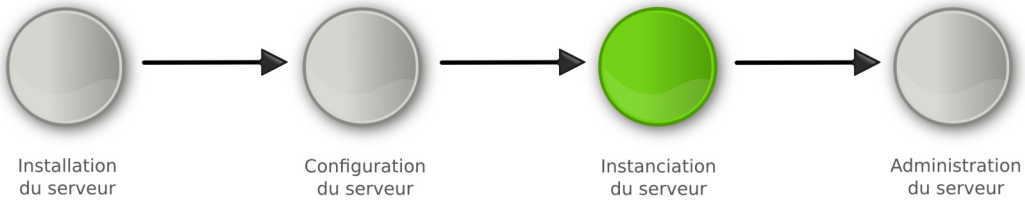
Les autres variables permettent d'adapter la sensibilité de la détection de la perte et du retour de lien.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 7

Instanciation du module

La troisième des quatre phases



Instanciation

- La **phase d'instanciation** s'effectue au moyen de la commande `instance` .
  L'instanciation permet de transférer les valeurs définies précédemment et des fichiers de configuration pré-remplis vers les fichiers cibles.
  À l'issue de cette phase, le serveur est utilisable en exploitation.
  Cette phase doit être complétée par un diagnostique complet du module à l'aide de la commande `diagnose -L` .

1. Principes de l'instanciation

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

Les templates[p.733] 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 patchs EOLE[p.726] ont étés créés pour personnaliser le serveur, ils seront pris en compte durant cette phase.

Voir aussi...

Personnalisation du serveur à l'aide de Creole [p.585]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

Mots de passe à l'installation

Lors de l'installation, les mots de passe des comptes `root` et `eole` sont générés aléatoirement selon les critères suivants :

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



Après installation, la connexion SSH par mot de passe pour l'utilisateur `root` est permise.

Cependant, le mot de passe généré aléatoirement de l'utilisateur `root` est affiché uniquement sur la console, il faut donc avoir un accès physique à la machine pour en prendre connaissance.

Mots de passe à l'instanciation

Lors de l'instanciation, la modification des mots de passe est demandée pour les comptes :

- 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- de l'utilisateur `Administrator` sur le module Seth avec le rôle de contrôleur de domaine principal.

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 ;
- un mot de passe commençant par une majuscule ou se terminant par un chiffre n'est pas considéré comme un mot de passe utilisant plusieurs classes de caractères ;
- ne pas utiliser le login comme partie du mot de passe.

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



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[p.705] donne une explication détaillée sur la stratégie des mots de passe.

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

2.2. Création d'un deuxième administrateur

À l'instance il est possible de créer un compte pour un nouvel administrateur.

```
Créer un nouvel administrateur eole2 ? [oui/non]
[non] : non
```


Des comptes administrateurs supplémentaires peuvent être créés en dehors de l'instance grâce à la commande `add_restricted_admin` .

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2.3. Jonction au domaine

À partir de la version EOLE 2.6.1, l'authentification NTLM/SMB nécessite l'enregistrement du module Amon/AmonEcole dans le domaine Samba. L'enregistrement au domaine est proposé lors de l'instanciation du module. Il n'est plus possible de configurer plusieurs contrôleurs de domaine.

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 ?
```

```
*** Redémarrage des services pour l'enregistrement au domaine ***
Stop Systemd service winbind in internet                                [  OK  ]
Restart Systemd service smbd in internet                                [  OK  ]
Restart Systemd service nmbd in internet                                [  OK  ]
Start Systemd service winbind in internet                               [  OK  ]

Entrer le nom de l'administrateur du contrôleur de domaine :
admin
Entrer le mot de passe de l'administrateur du contrôleur de domaine :
No realm has been specified! Do you really want to join an Active Directory server?
No realm has been specified! Do you really want to join an Active Directory server?
Using short domain name -- DOMPEDAGO
Joined 'AMONECOLE' to domain 'DOMPEDAGO'

*** Redémarrage des services pour confirmer l'enregistrement au domaine ***
Stop Systemd service winbind in internet                                [  OK  ]
Restart Systemd service smbd in internet                                [  OK  ]
Restart Systemd service nmbd in internet                                [  OK  ]
Start Systemd service winbind in internet                               [  OK  ]
L'intégration au domaine a réussi

```

Si la configuration de l'authentification 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`.

2.4. Mise à jour

À la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée.

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



Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

La mise à jour permet de maintenir votre serveur avec le niveau de fonctionnalité le plus récent et surtout

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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]
```

Voir aussi...

> Gestion des tâches planifiées eole-schedule [p.636]

2.5. Le redémarrage

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

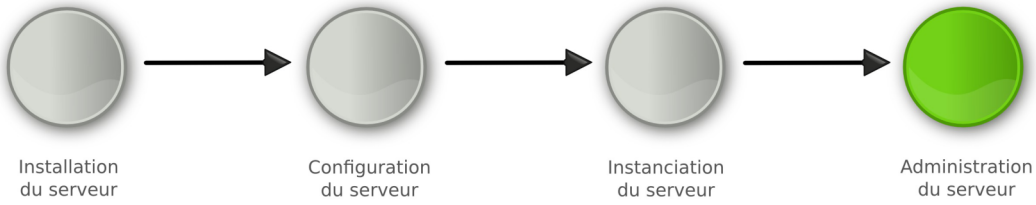
Si le noyau (kernel) a été mis à jour, le serveur doit redémarrer pour pouvoir l'utiliser. Dans ce cas, la question suivante apparaîtra :

```
Un redémarrage est nécessaire
Faut-il l'effectuer maintenant ? [oui/non]
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 8

Administration du module Amon

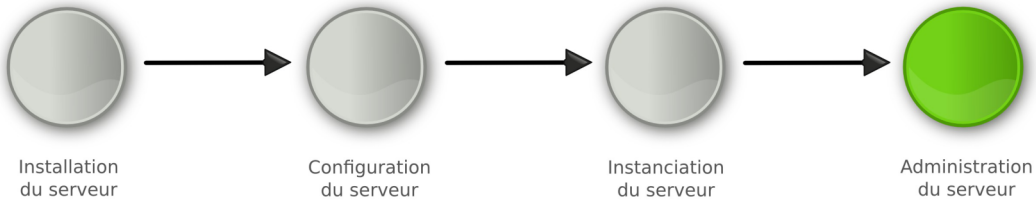


Administration

- 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



Administration

- 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.718]
- des outils périphériques = GNU [p.713]
- 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Racine de l'arbre

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

Arborescence 1er niveau

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

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

Fichiers et répertoires

Sous Unix, tout est fichier

Les différents types :

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

Adresse absolue / adresse relative

Un fichier ou un répertoire peut être défini :

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

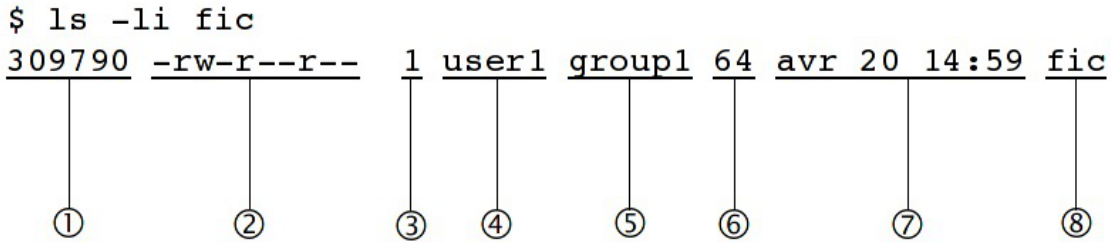
Droits essentiels :

- lecture
- écriture
- exécution

Autres droits :

- sticky bit
- setuid et setgid bits

Description d'un fichier



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `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** (e*X*ecute/exécution) respectivement pour le propriétaire (**u**), le groupe (**g**) et les autres utilisateurs (**o**). Les codes u, g et o (u comme user, g comme group et o comme others) sont utilisés par les commandes UNIX qui permettent d'attribuer les droits et l'appartenance des fichiers.

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

Droits Spécifiques

SUID Bit

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

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

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

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

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

SGUID Bit

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

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

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

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

Sticky Bit

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

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

Exemple : le répertoire /tmp

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

Listes de contrôle d'accès

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

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

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

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


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les droits étendus apparaissent de la façon suivante :

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

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

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

Par exemple :

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

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 raccroché à `init`. Ainsi donc, à l'instar des fichiers, les processus sont organisés en arbre.

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

Etat d'un processus

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

- **Actif** : le processus utilise le processeur, et est donc en train de réaliser des actions pour lequel il a été conçu.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- **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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- modifier la configuration : `upsrw 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

arguments disponibles.

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

Exemple :

- `cp [options] fichier chemin`
  `Options GNU (forme courte) : [-abdfilprsuvxPR]`

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

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

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

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

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

Description

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

Fichiers

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

Voir aussi

(ou "See also")

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

Exemple :

- `VOIR AUSSI`
  `passwd(1), login(1), group(5), shadow(5).`

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

Environnement

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

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 prochaine mot : `w` ;
- se déplacer au début de deux mots : `2w` ;
- revenir au début du mot précédent : `b` ;
- se déplacer à la fin du prochain mot : `e` ;
- se déplacer à la prochaine phrase : `)` ;
- revenir à la phrase précédente : `(` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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` .

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.731] (Secure Shell) et un protocole de communication sécurisé. Il permet différentes actions comme l'authentification à distance, l'exécution de commande à distance ou le transfert de fichier.

Le protocole est chiffré par un mécanisme d'échange de clés de chiffrement effectué au début de la connexion.

Le transfert de fichier d'une machine à une autre se fait par un protocole proche de FTP[p.712]. 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le client SSH est installé par défaut sur la plupart des distributions. Si ce n'est pas le cas, il faut installer un paquet dont le nom est généralement "openssh-client".

Une fois installé, il est possible d'ouvrir une session à distance de la manière suivante :

```
ssh utilisateur@ip_serveur
```

Si vous ne spécifiez pas de nom d'utilisateur, c'est l'utilisateur courant de votre session GNU/Linux qui sera utilisé.

Pour lancer des applications graphiques, il faudra le préciser dans la commande ssh en rajoutant l'option -X :

`ssh -X utilisateur@ip_serveur`.

A la première connexion, le message suivant apparaît :

```
Warning: Permanently added 'xxxxx' (RSA) to the list of known hosts.
```

Cela signifie qu'on ne s'est jamais connecté sur cette station et qu'un identifiant est ajouté à la liste des hôtes connus.

Il peut arriver que le certificat du serveur change (par exemple en cas de réinstallation).

Le message suivant apparaîtra :

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
65:6d:9d:c0:78:f7:60:bf:13:86:59:16:53:07:3b:a4.
Please contact your system administrator.
Add correct host key in /home/xxx/.ssh/known_hosts to get rid of this message.
Offending key in /home/xxx/.ssh/known_hosts:12
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
X11 forwarding is disabled to avoid man-in-the-middle attacks. Permission denied (publickey,password).
```

Ce message nous apprend plusieurs choses :

- le serveur ssh a une clef différente de celle de notre dernier passage ;
- le fichier comprenant les hôtes connus est `/home/xxx/.ssh/known_hosts` ;
- l'identifiant de l'hôte est spécifié à la ligne 12 (Offending key in /home/xxx/.ssh/known_hosts:12).

Si vous êtes sûr que l'hôte est le bon, il vous suffira de supprimer la ligne 12 du fichier known_hosts et de relancer une connexion.

Il faudra spécifier le mot de passe de l'utilisateur pour se connecter.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 :

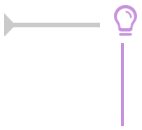
```
scp utilisateur@ip_serveur:/repertoire/source/nom_du_fichier /repertoire/de/destination/
```

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.733] et SSH[p.731] 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.

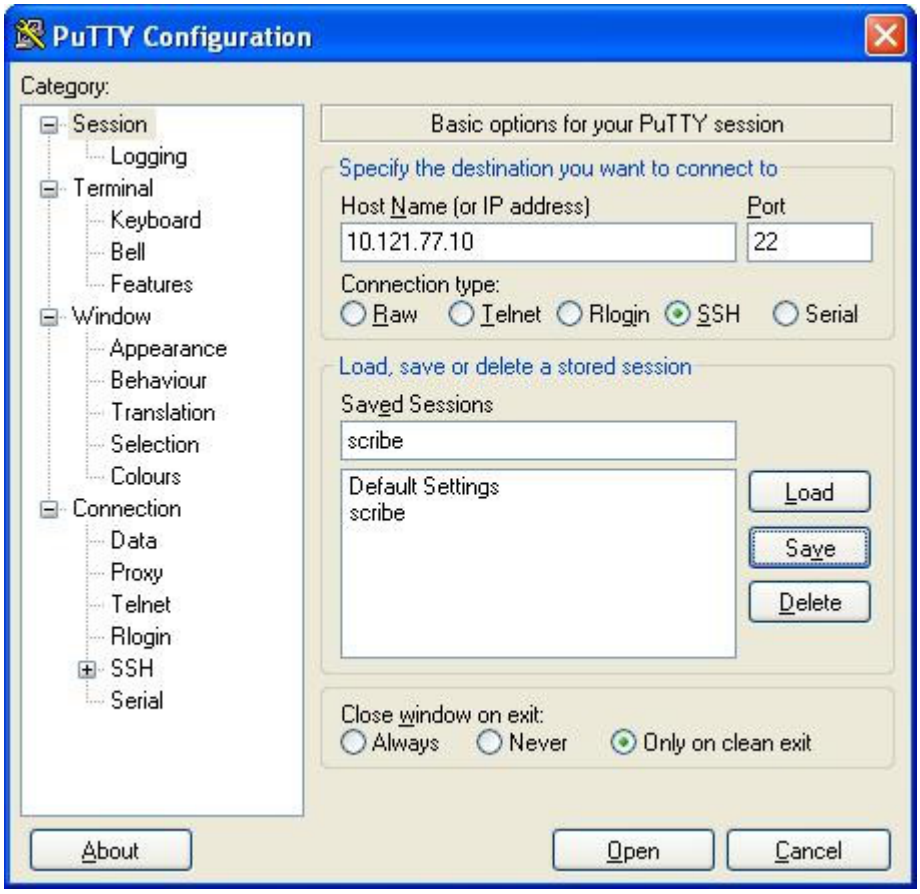
La connexion avec Putty au serveur se fait en utilisant le protocole SSH.

Sur le module Scribe, Putty est pré-installé dans le répertoire personnel d'*admin* (`U:\client\putty.exe`).

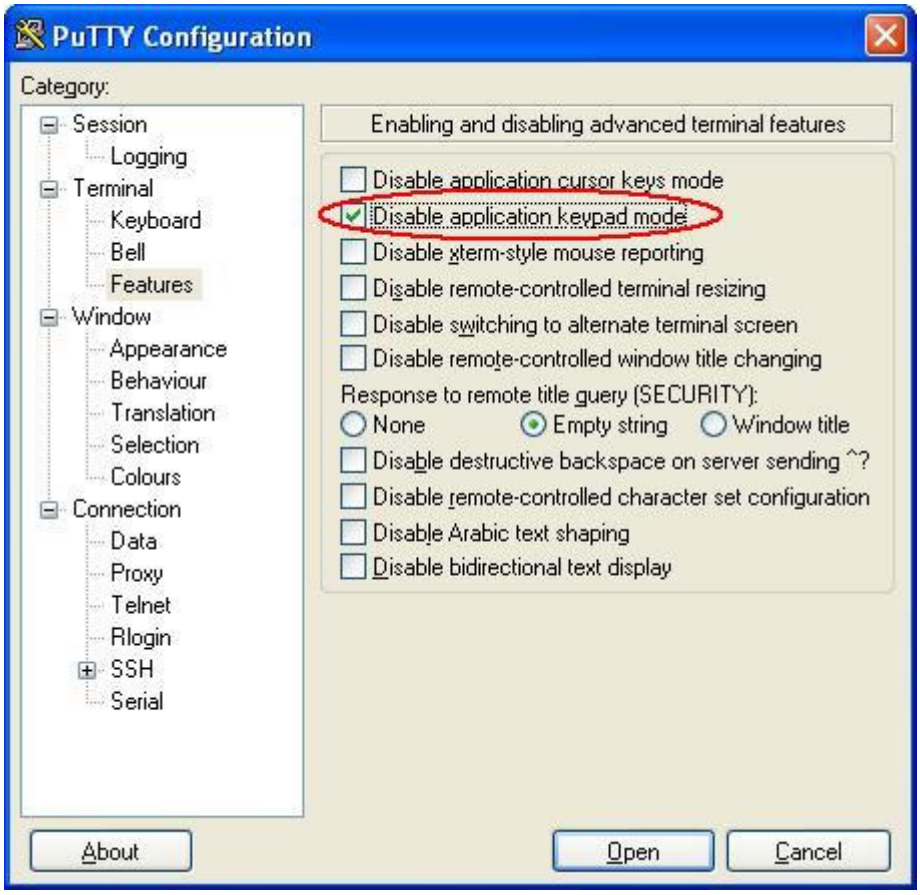
Configuration pour les serveurs EOLE

Pour obtenir un meilleur environnement de travail, la configuration par défaut de Putty doit être modifiée.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

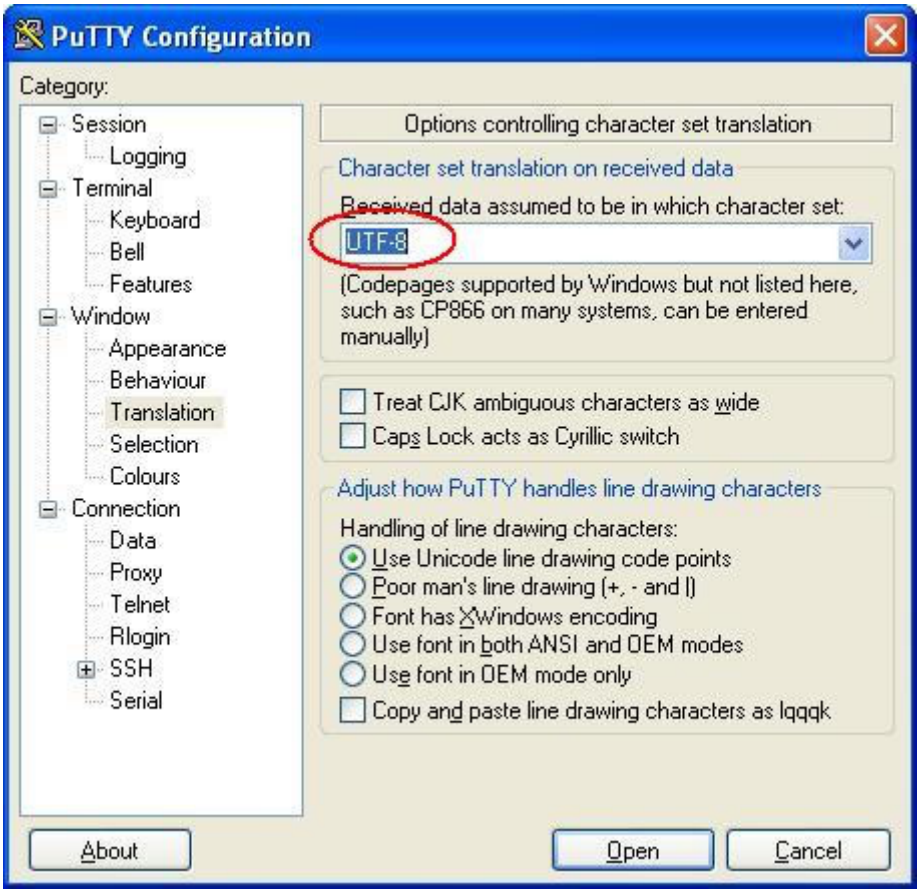


Fenêtre principale

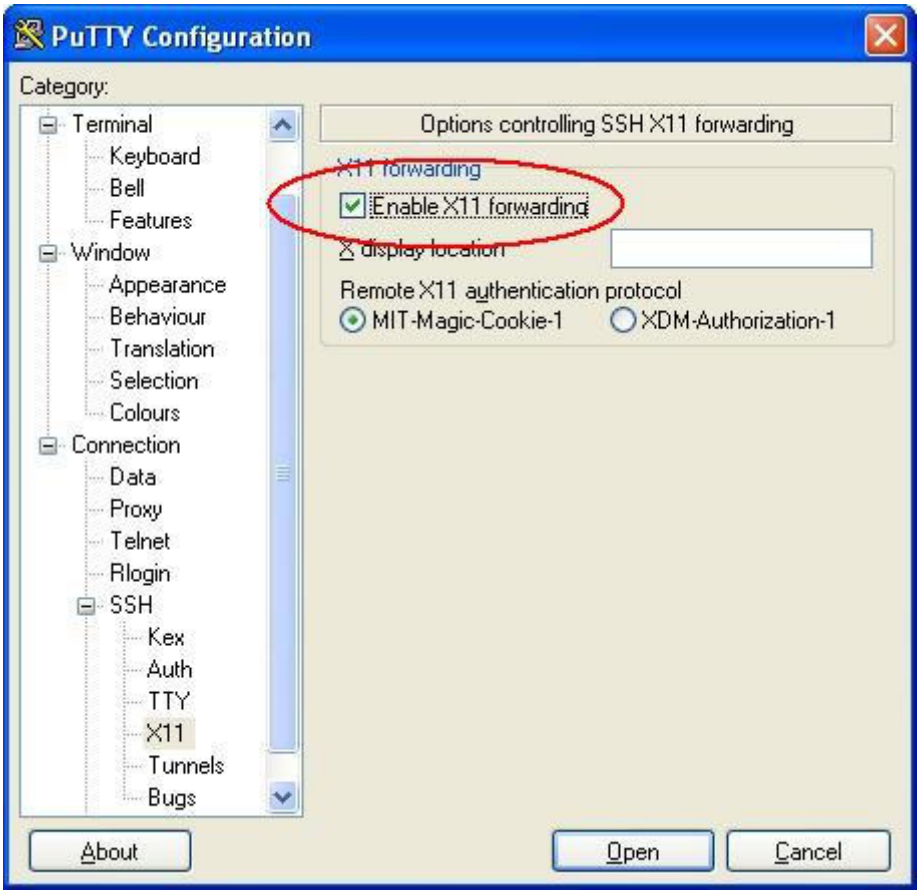


Permettre au pavé numérique de fonctionner correctement (dans "vim" par ex.)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Permettre aux accents de s'afficher normalement



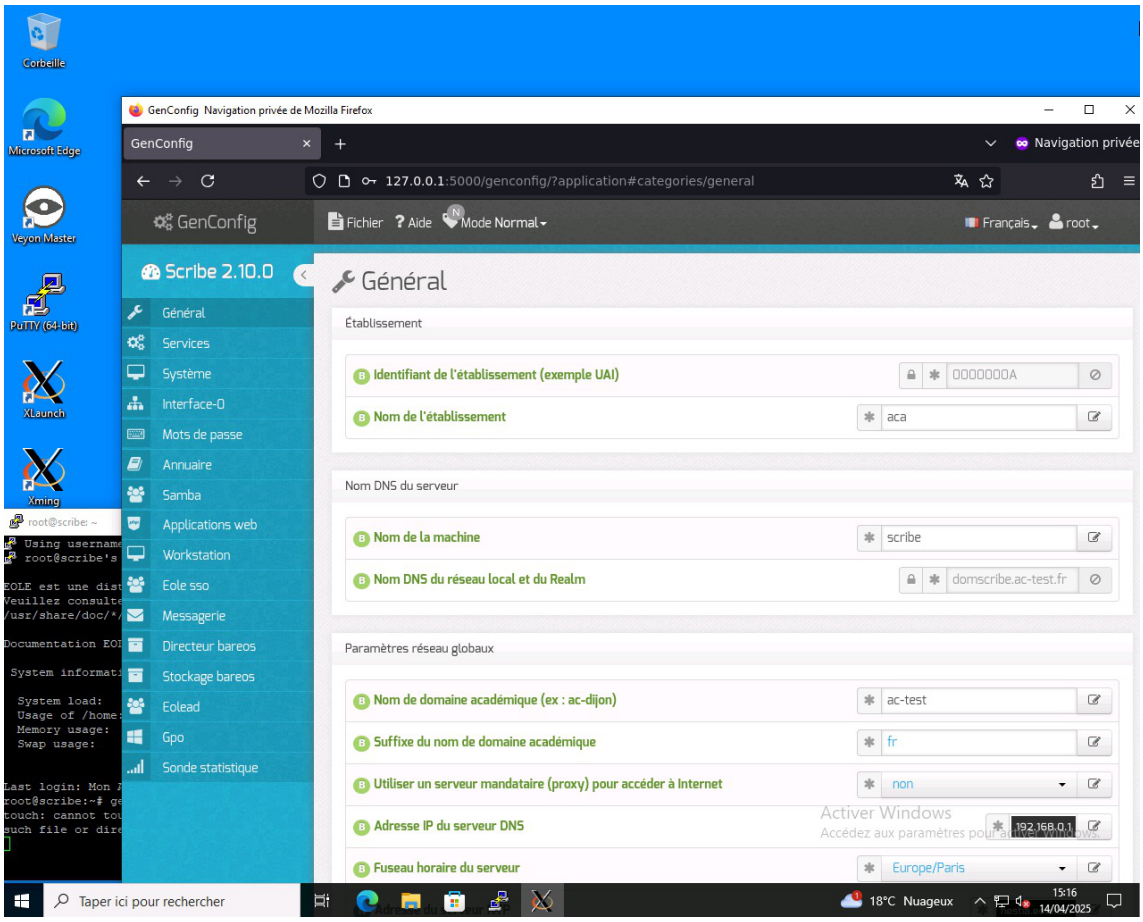
Pouvoir lancer des applications graphique du serveur depuis la station (Ex. "gen_config")

La dernière capture montre comment autoriser la redirection des applications graphiques vers votre poste.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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,

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.716] 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 sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

S'il existe une différence entre `config.eol` et `config.eol.bak` c'est que la configuration du serveur a été modifiée mais qu'elle n'a pas encore été 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.730] 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 ;
- recréé le compte `admin` s'il n'a pas été trouvé (modules Scribe et Horus) ;
- copie, patch[p.726] 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.710], `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 inexistants ;
- lance des commandes spécifiques à l'instanciation ;
- copie, patch et renseigne les templates ;
- (re)lance les services ;
- contrôle la version du noyau en fonctionnement et demande un redémarrage si ce n'est pas la dernière version (reboot automatique si mise à jour par EAD).



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.

Des comptes d'administration supplémentaires peuvent être ajoutés en dehors de la procédure d'instance grâce à la commande `add_restricted_admin`.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.



Depuis la version EOLE 2.6, il n'est plus possible d'accéder à l'EAD à l'aide de l'adresse IP du serveur, il faut impérativement utiliser un nom de domaine et que celui-ci soit présent dans le certificat SSL.

Cette restriction est notamment due au durcissement du support du protocole HTTPS[p.714] par les navigateurs.

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, Seth, ...) 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.



Certificats SSL

Pour avoir accès à l'EAD, il faut impérativement que le nom de domaine soit présent dans le certificat SSL.

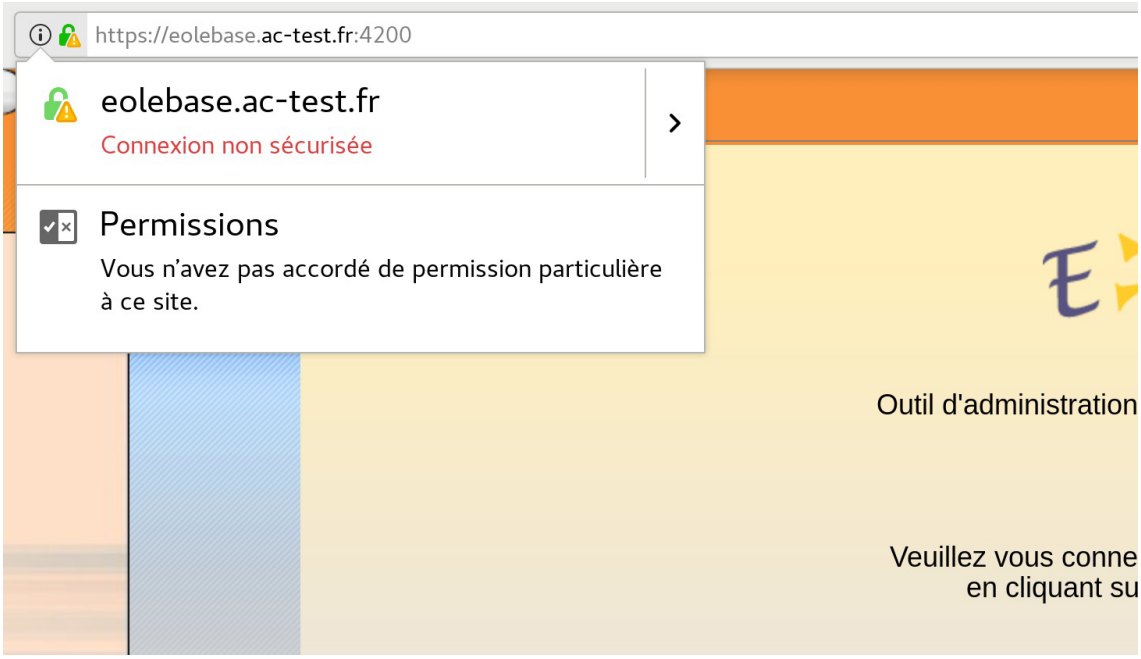
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

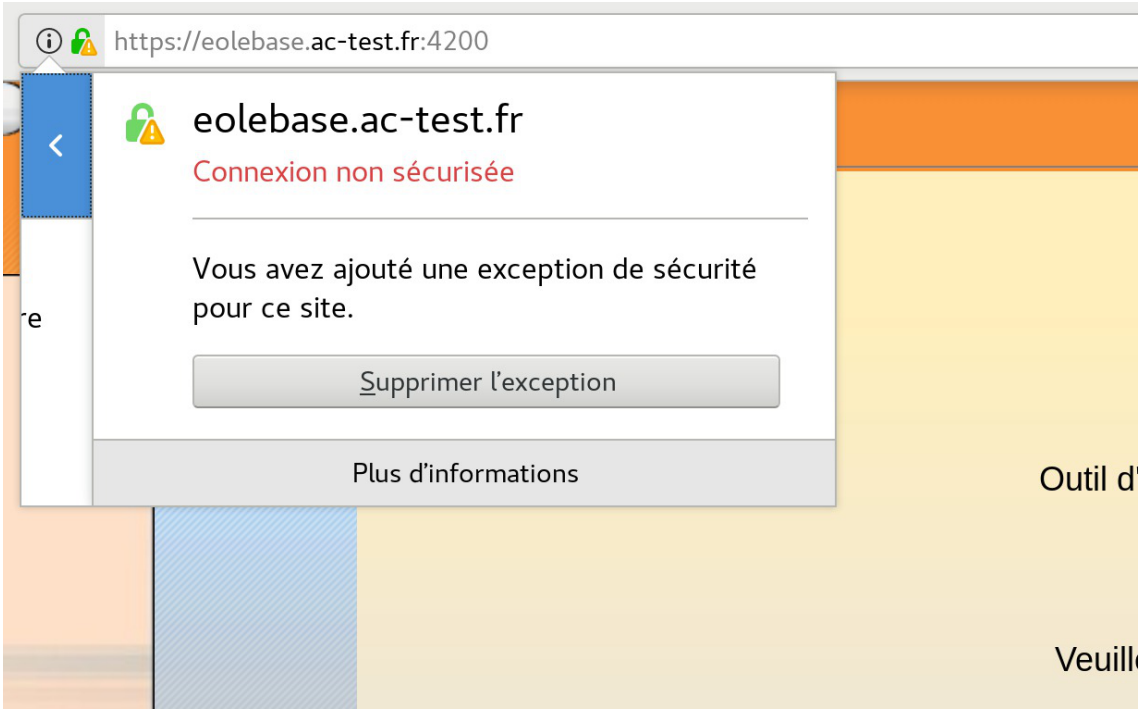
Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

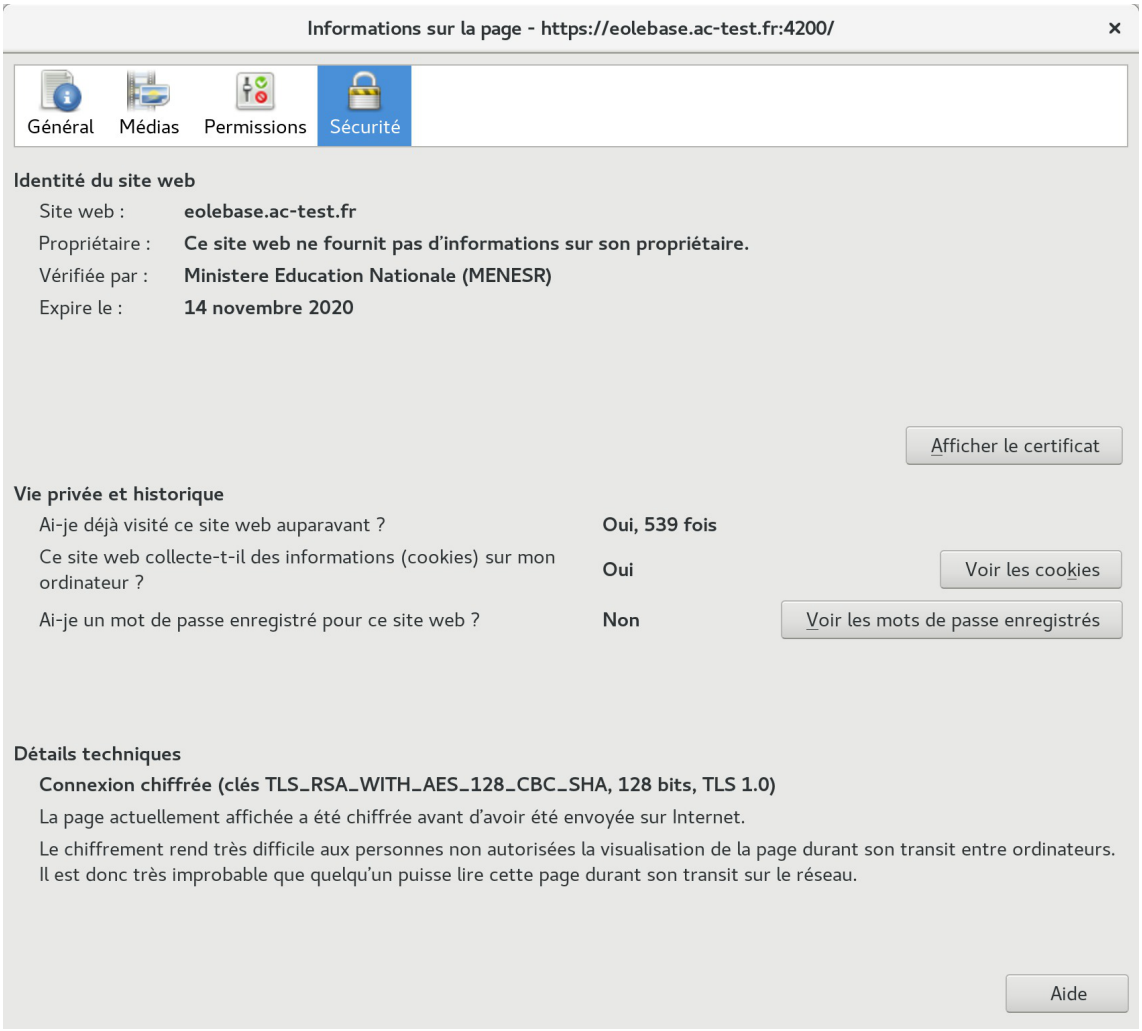


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion



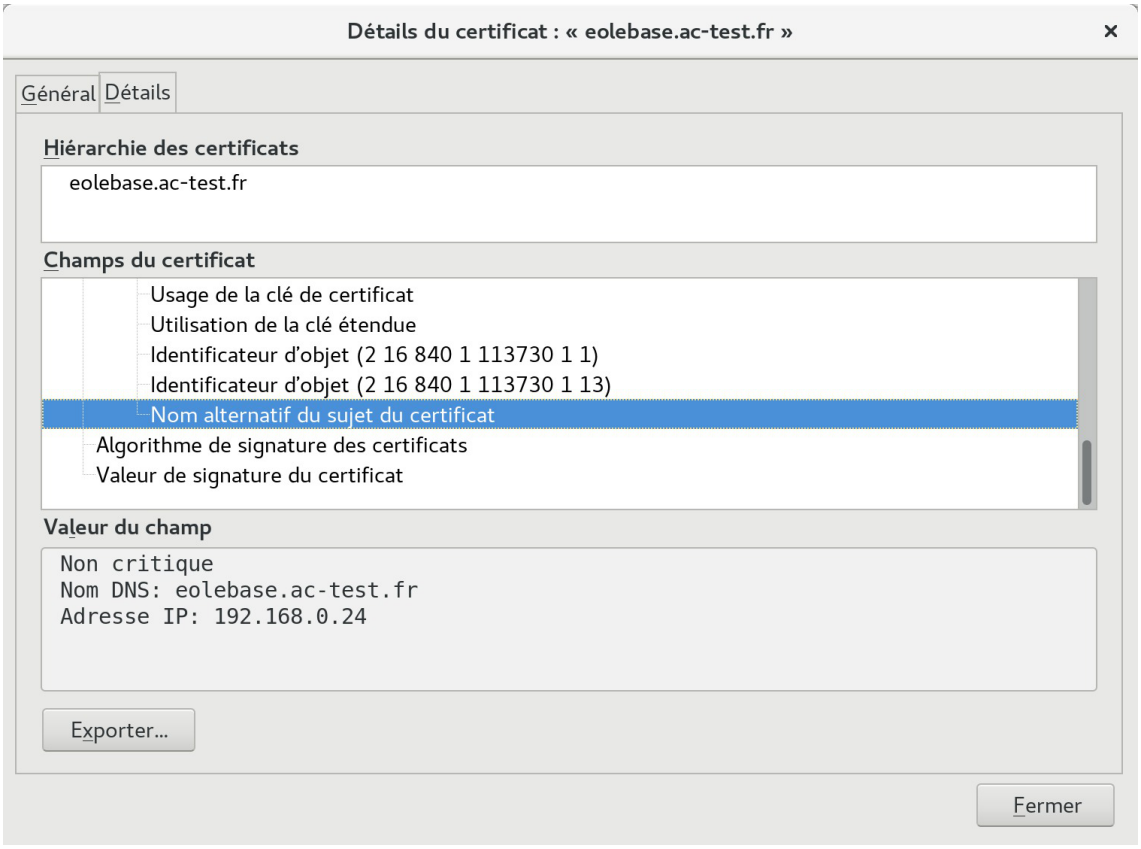
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



- Il est possible que des noms alternatifs soient renseignés dans le certificat. Pour les retrouver, cliquer sur le bouton `Afficher le certificat`, puis sur l'onglet `Détails` et sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Attention, même si la bonne adresse IP apparaît dans le certificat, elle ne sera pas prise en compte.

Si le nom de domaine n'apparaît pas et que le certificat est de type autosigné, il faut le rajouter dans l'onglet `Certificats ssl` de l'interface de configuration du module en mode expert.

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom d'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.

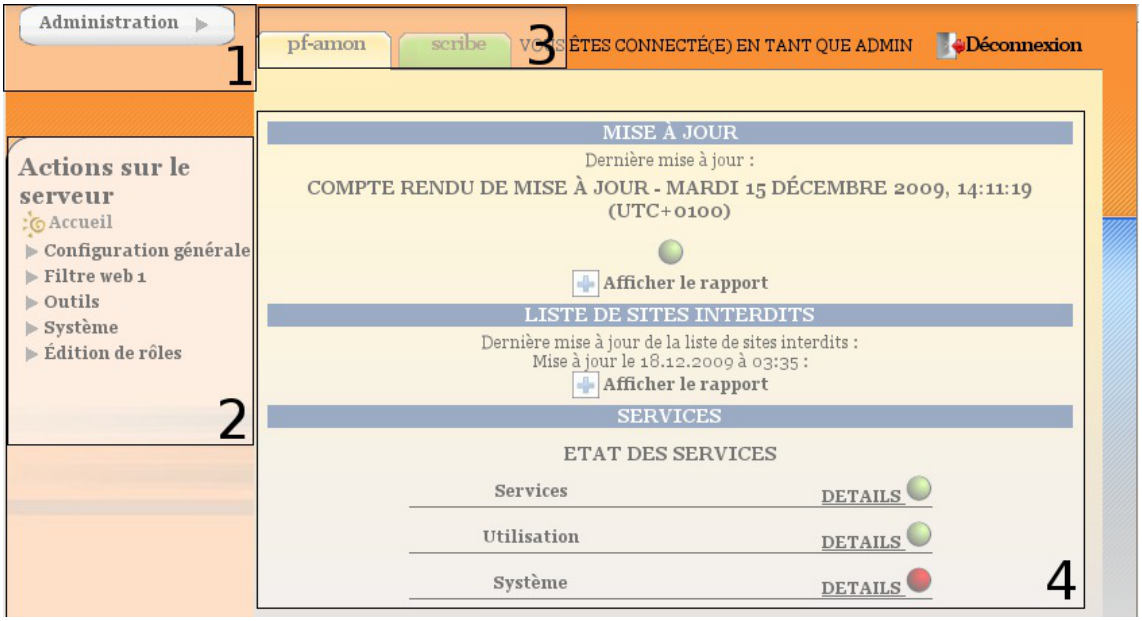
Après changement des paramètres il est nécessaire de supprimer le certificat puis d'exécuter la reconfiguration du module :

```
rm -f /etc/ssl/certs/eole.crt
reconfigure
```

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les agents Zéphir peuvent être consultés directement en utilisant l'adresse : `http://<adresse module>:8090`

Voir aussi...

Surveillance de l'état du serveur [p.398]

1.4.3. 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.

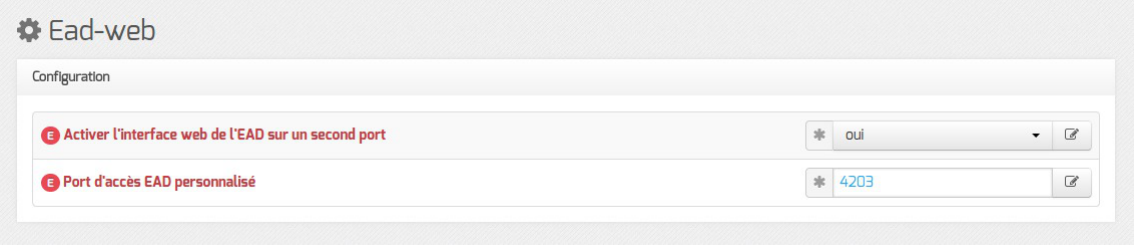
Avantages

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`.



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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.709] : `ead_scribe`.

Voir aussi...

- Onglet Ead-web : EAD et proxy inverse [p.275]
- Onglet Reverse proxy : Configuration du proxy inverse [p.167]

1.4.4. 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.

Depuis la version EOLE 2.6, il n'est plus possible d'accéder à l'EAD à l'aide de l'adresse IP du serveur, il faut impérativement utiliser un nom de domaine et que celui-ci soit présent dans le certificat SSL.

Cette restriction est notamment due au durcissement du support du protocole HTTPS [p.714] par les navigateurs.

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.

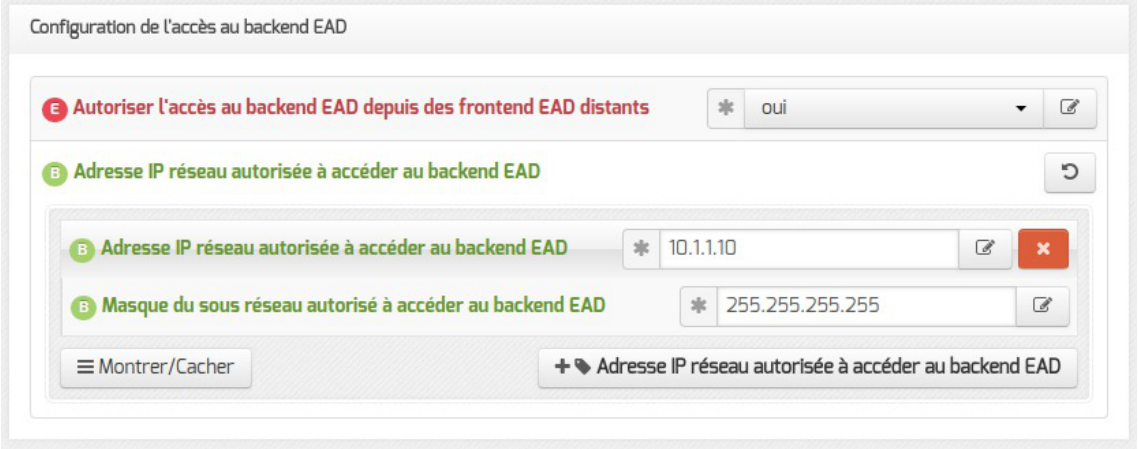
Il est ensuite possible de gérer les accès ainsi que les actions autorisées par utilisateur ou par groupe.

Ajout de serveur

Pour permettre à un frontend EAD de se connecter à un serveur de commandes EAD distant, il faut, sur

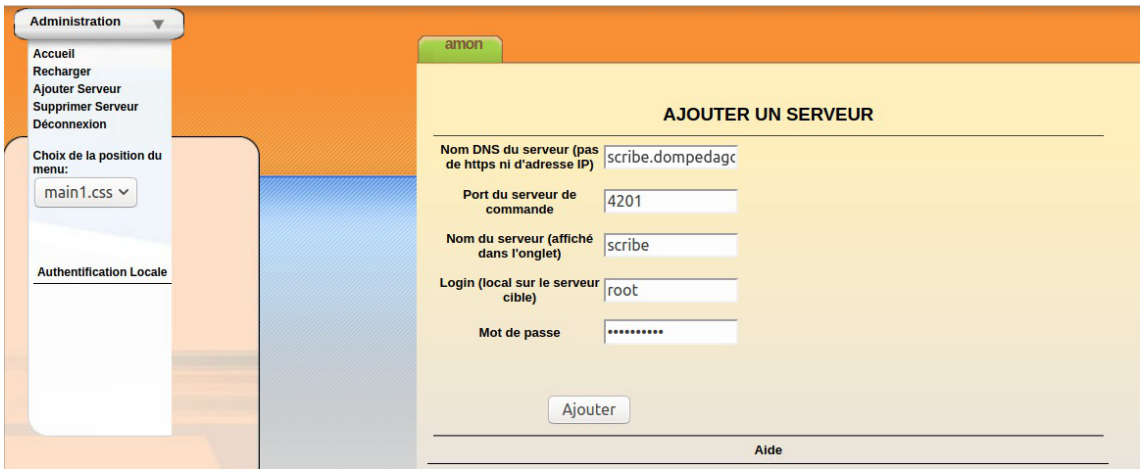
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

le module distant, l'autoriser explicitement pour chaque interface. Cela peut s'effectuer en mode expert dans l'interface de configuration du module, dans l'onglet `Interface-n`.



Dans la gondole d'administration de l'EAD, cliquer sur `Ajouter serveur` et renseigner :

- le nom DNS 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).



Depuis la version EOLE 2.6, si le certificat du serveur à ajouter n'est pas signé par une autorité de certification[p.704] connue du serveur hébergeant le frontend EAD, il sera nécessaire de copier sa CA sur ce dernier.

L'exemple suivant décrit la copie et l'intégration de la CA d'un module Scribe sur un module Amon :

```
root@amon:~# scp root@scribe:/etc/ssl/certs/ca_local.crt
/usr/local/share/ca-certificates/
root@amon:~# update-ca-certificates
```

Le compte `root` peut être utilisé à la place du compte `eole` pour toutes les manipulations présentées ici.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`

```
[1]
url = https://127.0.0.1
port = 4201
comment = amon
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Si nécessaire, il est possible de réinitialiser ces fichiers à l'aide des commandes suivantes :

```
1 echo '[keys]' > /usr/share/ead2/backend/config/frontend_keys.ini
2 echo '' > /usr/share/ead2/frontend/config/servers.ini
3 reconfigure
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.4.5. 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 classées dans 3 catégories : Système, Services et Utilisation.

1.4.5.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.720] 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.708].

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
```

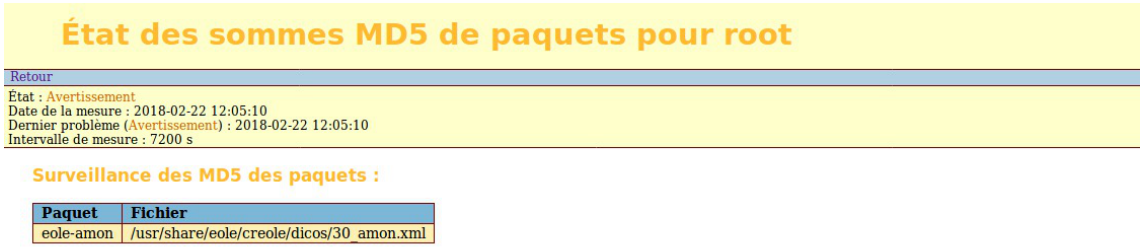

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
Container: root
===============

Filename: /var/log/eole-debsums/report.log
Last update: 2018-02-22 11:09:15

eole-amon:
    /usr/share/eole/creole/dicos/30_amon.xml

Ignored by eole
---------------

```

Un agent[p.702] de surveillance Zéphir permet de surveiller les sommes MD5 des paquets.



Il permet également de consulter la liste des fichiers signalés comme modifiés.



Exceptions

Il est possible d'ajouter des listes de fichiers à ignorer dans le résultat debsums en les plaçant dans le répertoire : `/etc/eole/debsums-ignore.d` (exemple : `/etc/eole/debsums-ignore.d/academie.conf`).

Les fichiers modifiés par EOLE sont listés dans `/usr/share/eole/debsums/eole-ignores`.

1.4.5.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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- État des démons bacula

Enfin d'autres agents sont propres à un module en particulier :

- État des tunnels

1.4.5.d. Utilisation

Quelques agents sont fournis de base et sont commun à tous les modules :

- Mise à jour
- Validité des certificats

D'autres agents sont disponibles suite à l'activation du service sur le serveur par l'intermédiaire de l'interface de configuration du module :

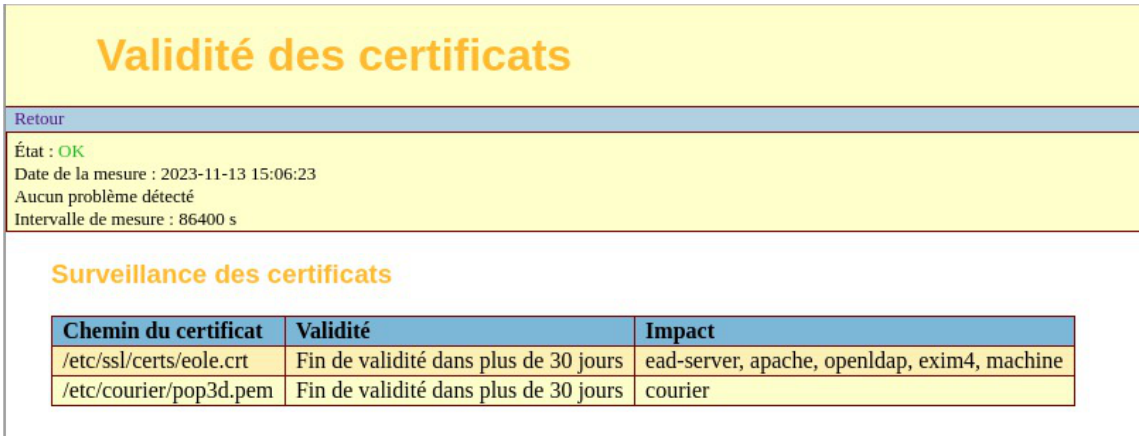
- Sauvegarde

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

Validité des certificats

L'agent `localcert` permet de surveiller la validé des certificats locaux utilisés par les différents services du module EOLE.



1.4.6. Authentification locale et SSO

Dans l'EAD, il existe deux systèmes d'authentification :

- l'authentification unique (SSO[p.731]) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 utilisé conjointement avec l'authentification SSO.

Pour vous authentifier localement, dans la gondole d'administration :

- cliquer sur `authentification locale` ;
- cliquer sur le nom de votre serveur.

Vous accédez alors au formulaire d'authentification locale.

Si le serveur SSO n'est pas activé, vous arriverez sur ce même formulaire en cliquant sur l'onglet.



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

(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.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

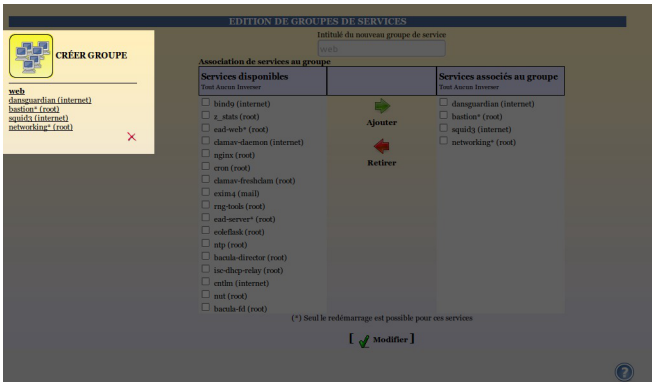


Création d'un groupe de services (1)



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

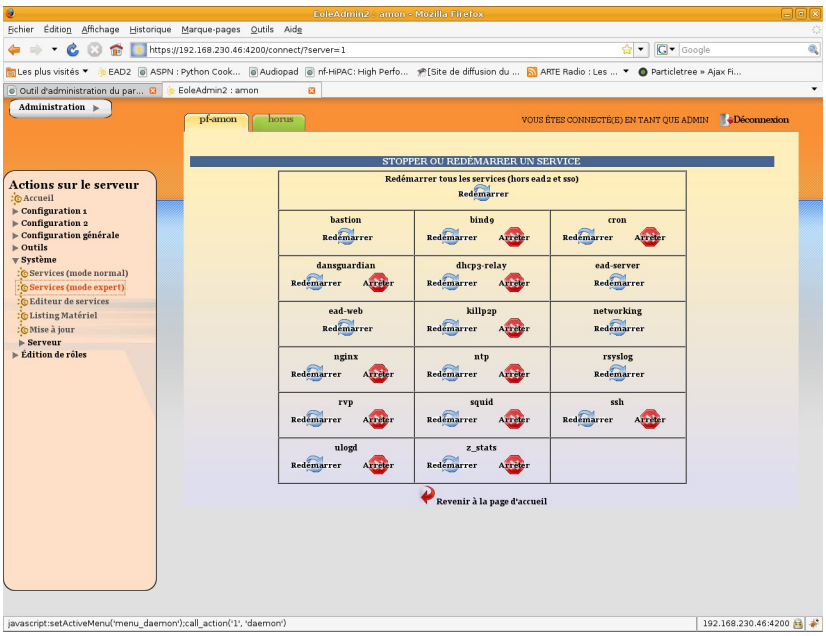
Complément technique

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).

Sur un serveur en mode conteneur[p.707], certains services peuvent être listés plusieurs fois en fonction de leur emplacement.

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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

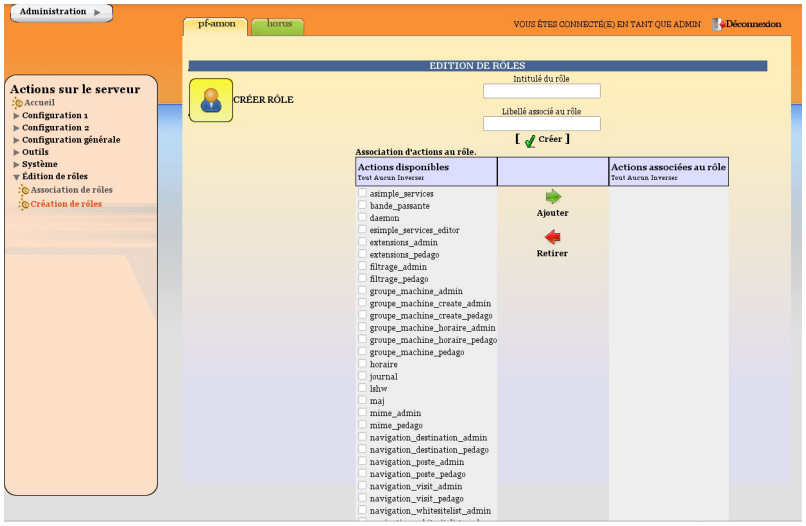
La fenêtre d'édition des rôles

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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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_admi**n (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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- **gestion_group_create** : action de création de groupe ;
- **gestion_group_modify** : action de modification de groupe ;
- **gestion_group_suppr** : action de suppression de groupe.

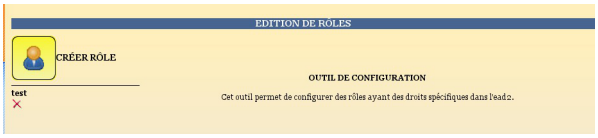
- Autres actions
  - **gestion_account_suppr** : action de suppression forcée de compte ;
  - **extraction_aaf** : action pour l'extraction AAF ;
  - **bareos** : action programmation de sauvegarde ;
  - **bareos_config** : action de configuration de Bareos pour la sauvegarde ;
  - **scripts_admin** : 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.715] 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

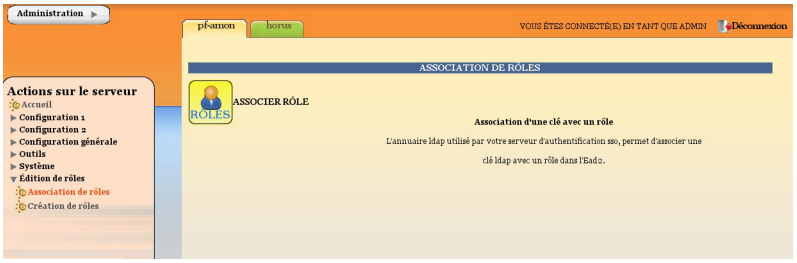
Création d'association via l'EAD

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Authentification locale :

- le login de l'utilisateur.

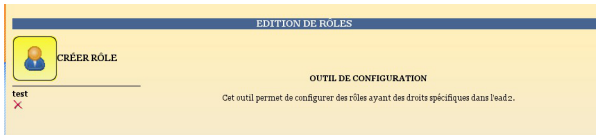
Authentification SSO :

- 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 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) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

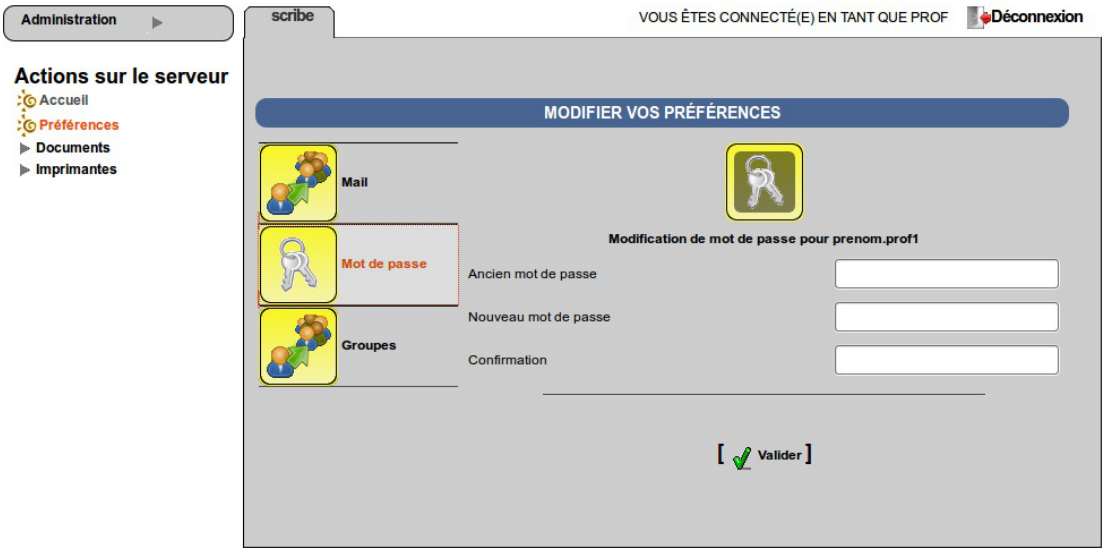
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



l'EAD pour un professeur

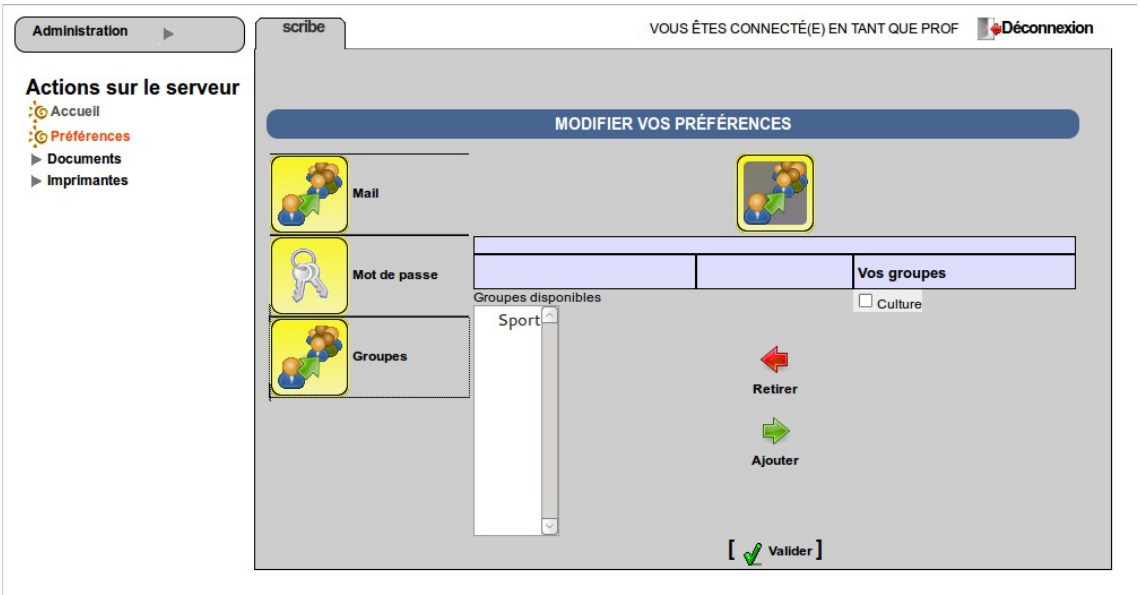
L'item *Préférences* permet à un utilisateur de :

- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

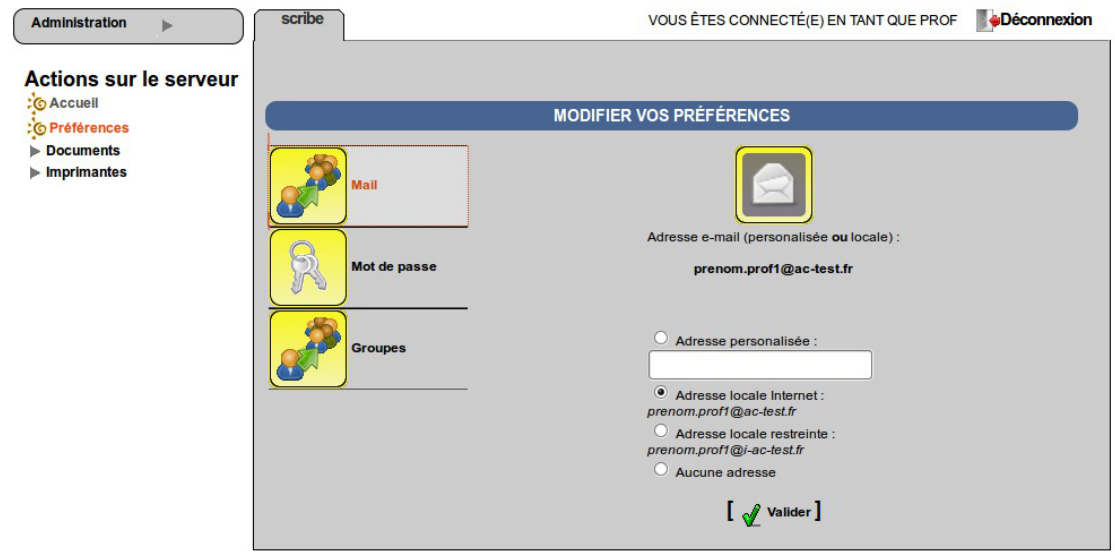
- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

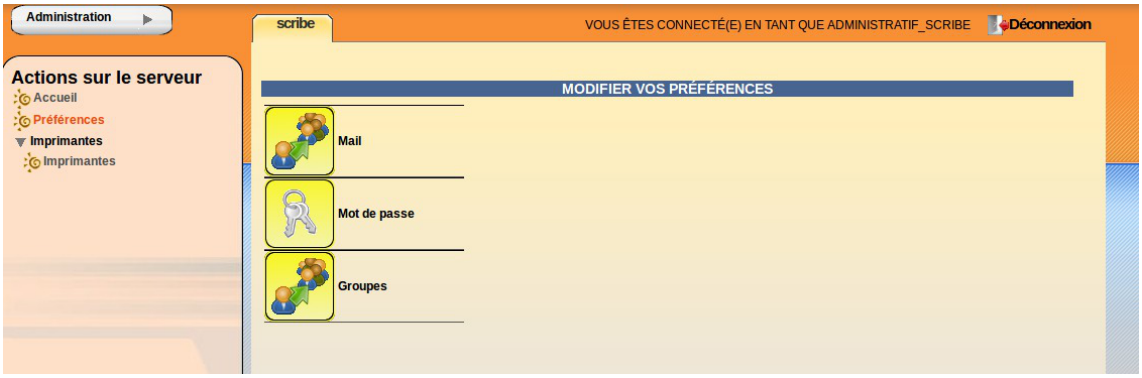
Un professeur peut être responsable de plusieurs classes.

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.

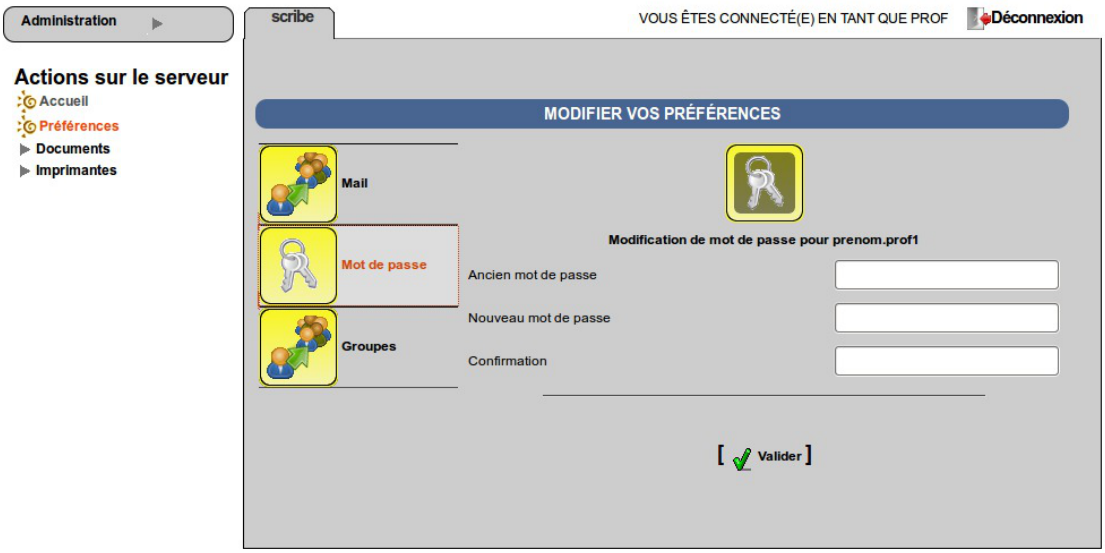
Accès "Administratif du Scribe"

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 :

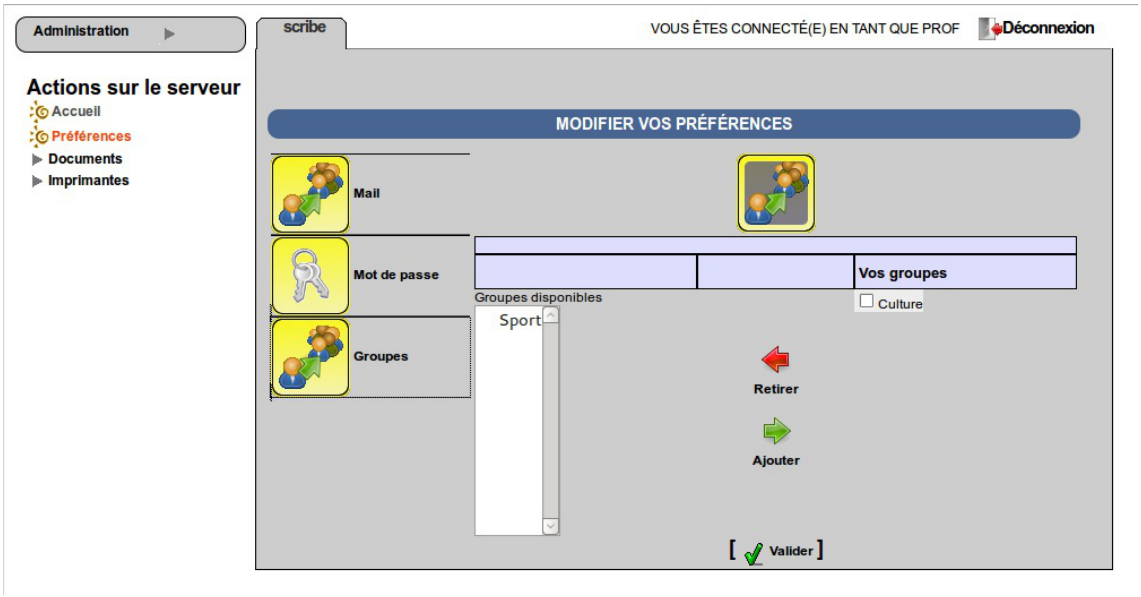
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

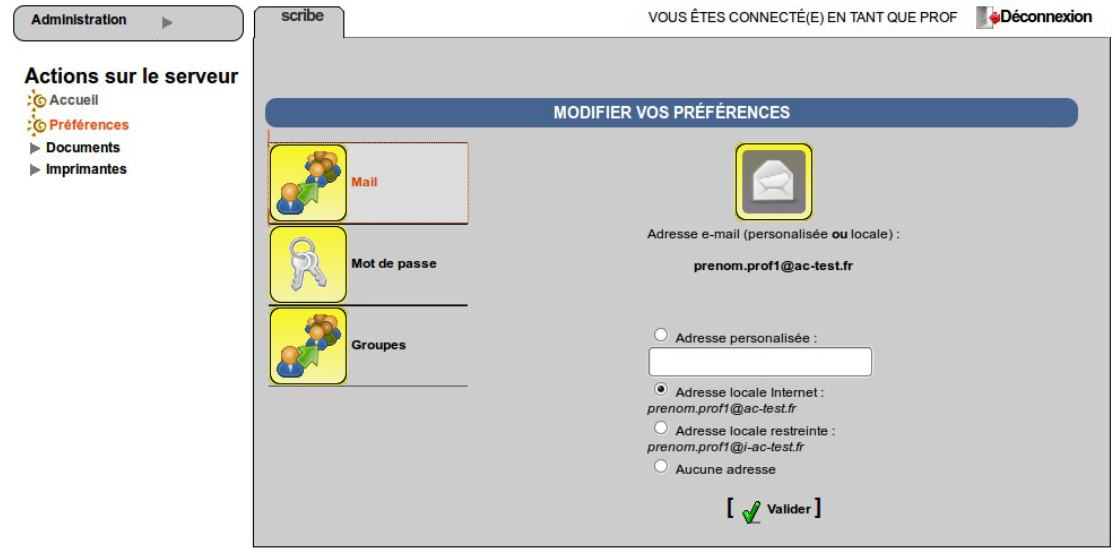
- s'inscrire/se désinscrire d'un groupe ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.e. 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.) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

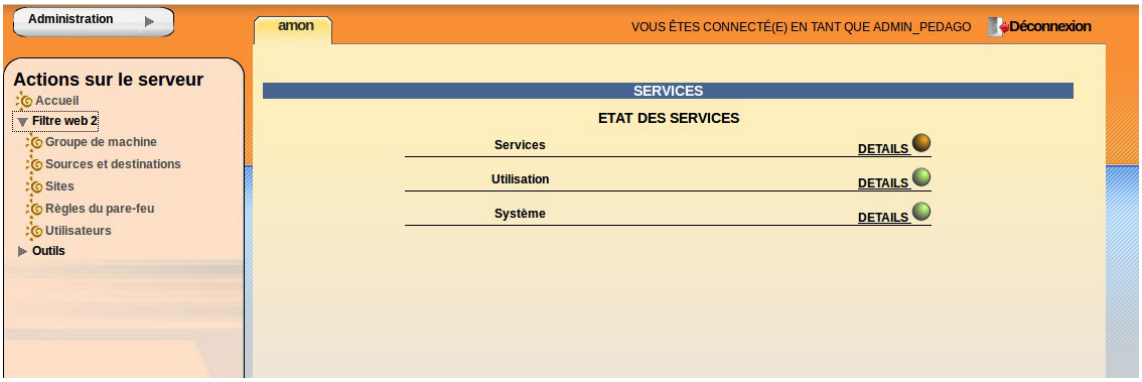
Fonctionnalités Amon

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.f. Les rôles sur le module AmonEcole

L'EAD est accessible :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.

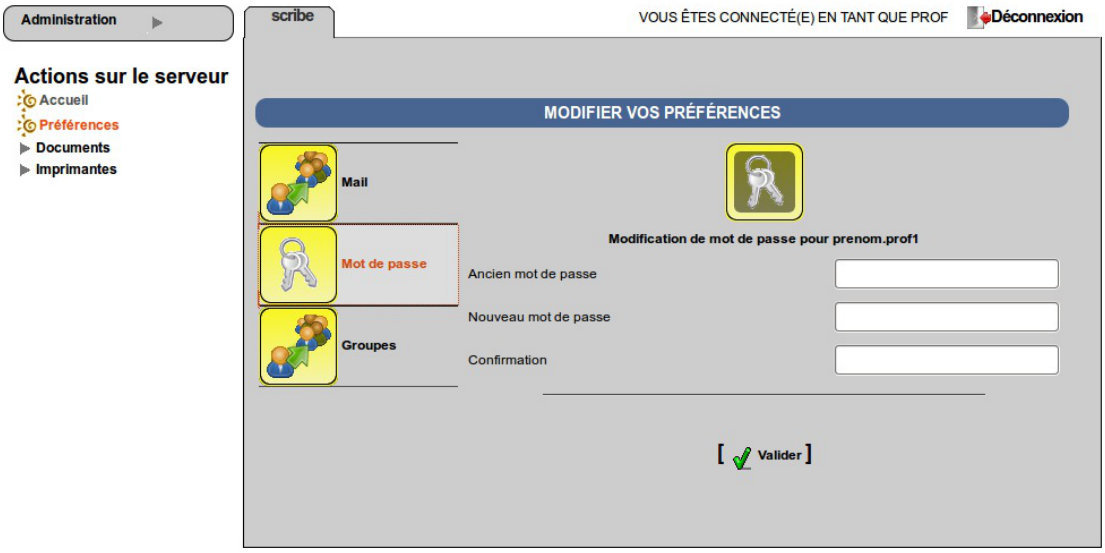


l'EAD pour un professeur

L'item *Préférences* permet à un utilisateur de :

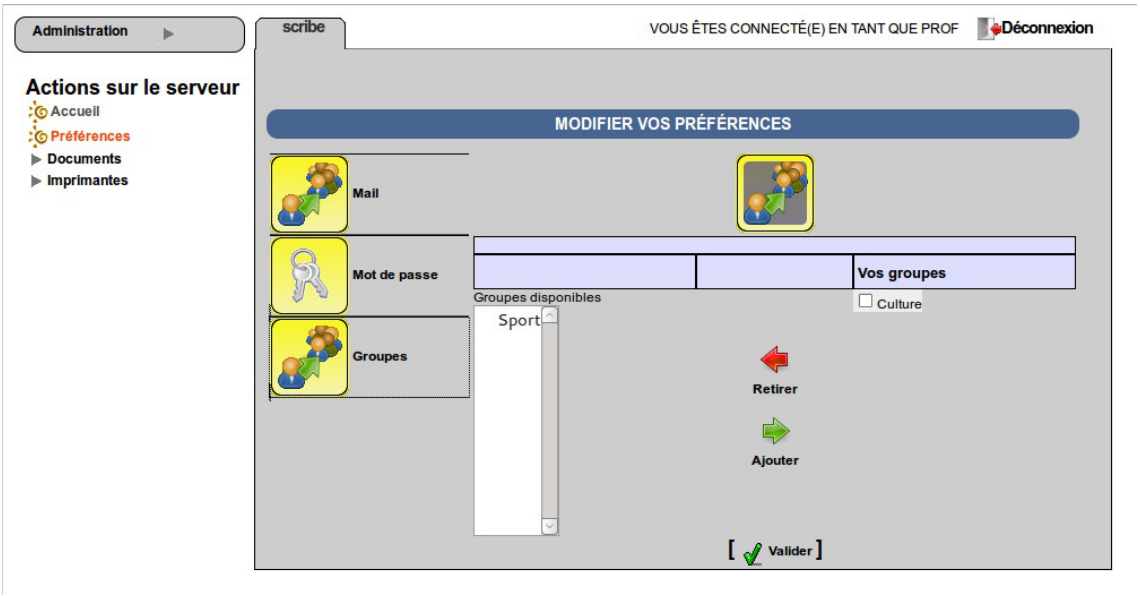
- modifier son mot de passe ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



EAD vue enseignant avec thème Envole, changement de mot de passe

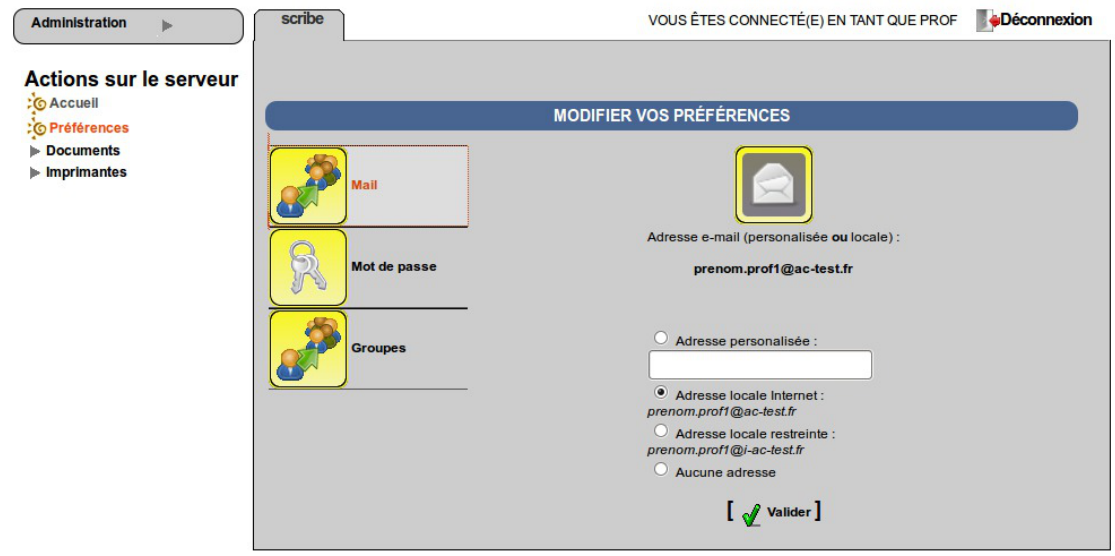
- s'inscrire/se désinscrire d'un groupe ;



EAD vue enseignant avec thème Envole, gestion des groupes

- renseigner/modifier son adresse mail.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



EAD vue enseignant avec thème Envole, changement d'adresse électronique

L'adresse de courrier électronique est renseignée dans l'annuaire, elle est utilisée, par exemple, par les listes de diffusion.

Accès "responsable de classe"

Un professeur peut être défini *responsable de classe* par l'administrateur. Il obtient alors quelques actions lui permettant d'administrer les classes dont il est responsable. Cela permet à l'administrateur de déléguer certaines actions comme :

- la **ré-initialisation du mot de passe d'un élève** ;
- l'**appartenance d'un élève à un groupe** ;
- la **création d'un groupe** ;
- etc.

Les fonctions disponibles :

- préférences personnelles ;
- distribution de devoirs ;
- gestion des imprimantes (CUPS) ;
- création de groupe ;
- ajout/modification/suppression des élèves dans la/les classe(s) dont il est responsable ;
- édition groupée sur les membres de la/les classe(s) dont il est responsable.



l'EAD pour un responsable de classe

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

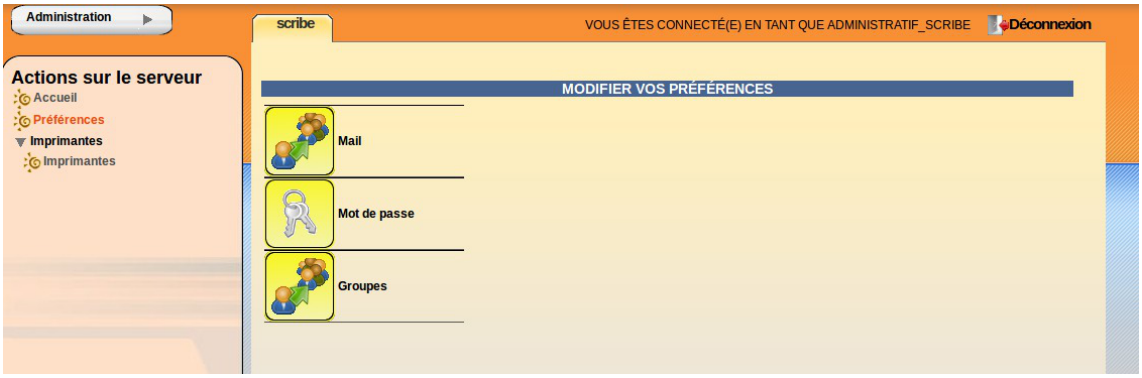
Un professeur peut être responsable de plusieurs classes.

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.

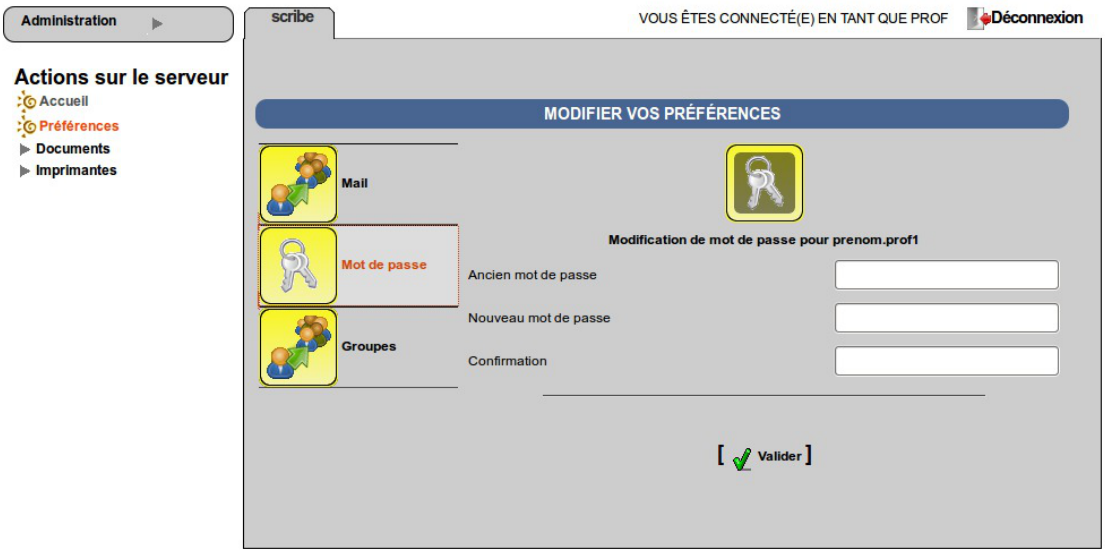
Accès "Administratif du Scribe"

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 :

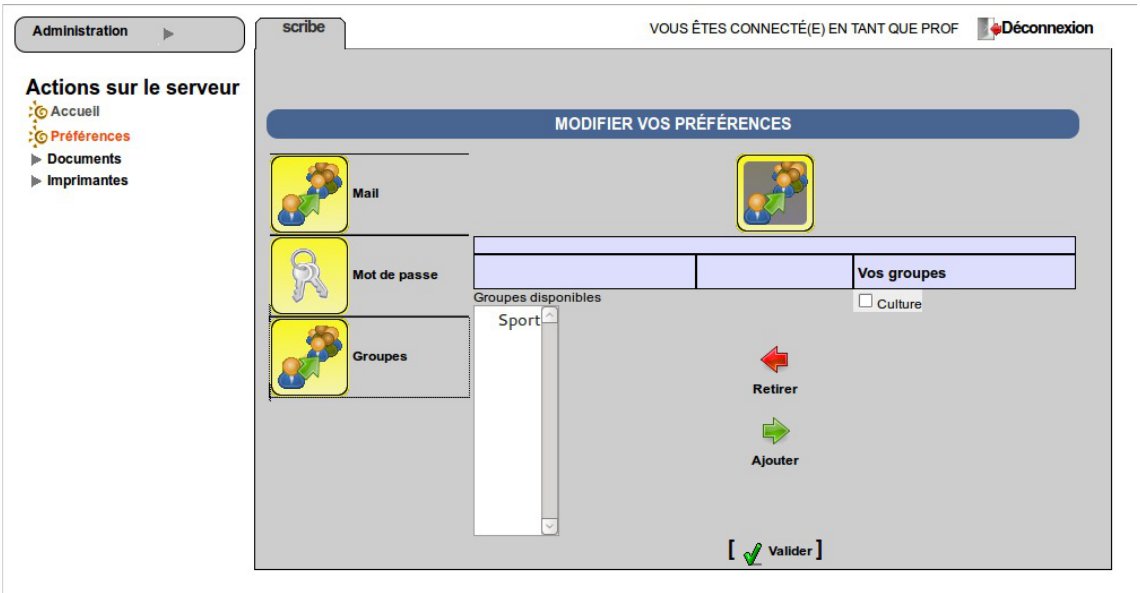
- modifier son mot de passe ;



EAD vue enseignant avec thème Envole, changement de mot de passe

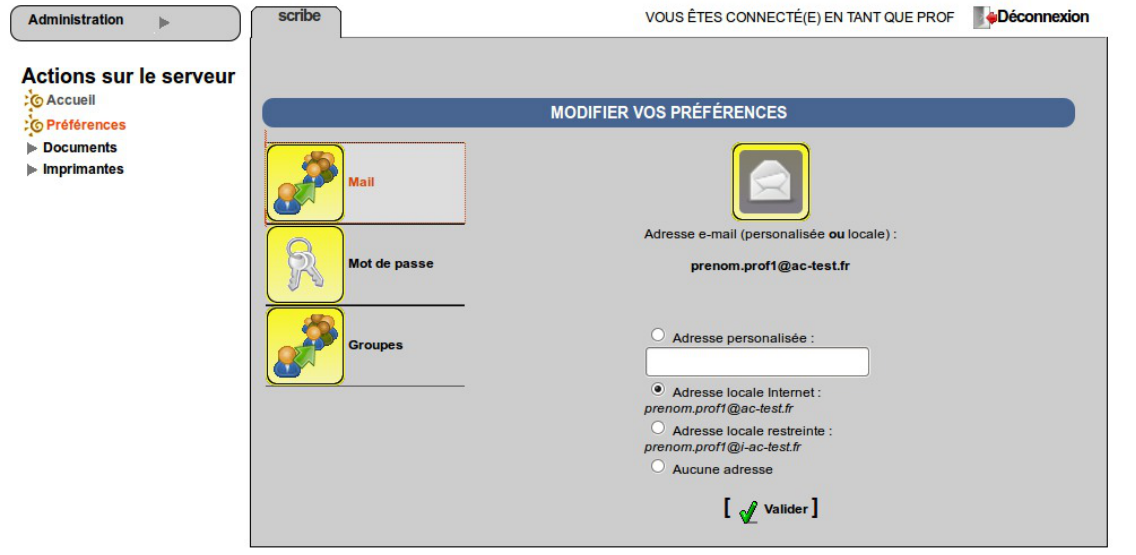
- s'inscrire/se désinscrire d'un groupe ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 "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) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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

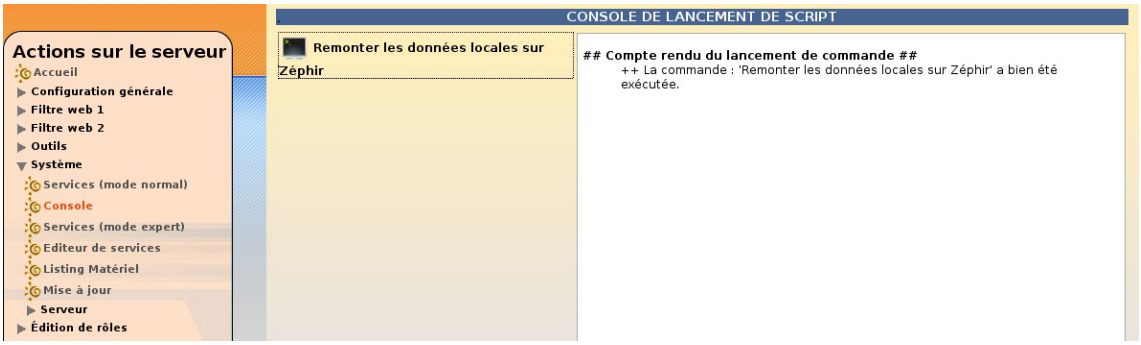
L'EAD du module Amon, dans son mode le plus complet, présente les fonctionnalités suivantes :

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Remontée des données locales sur Zéphir par la console EAD

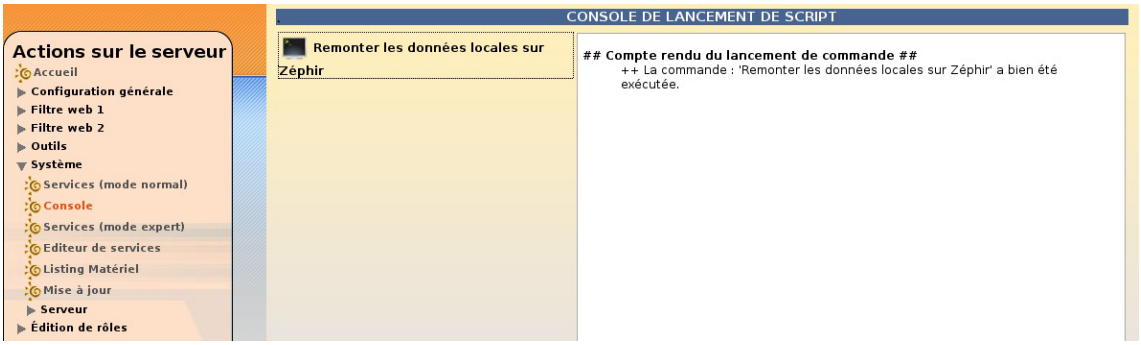
Seul le script Remonter les données locales sur Zéphir est fourni par défaut.



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"
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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 réussi un message s'affiche :

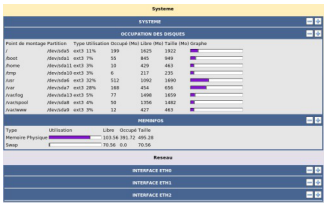
```
++ La commande : 'Occupation disque' a bien été exécutée.
```

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.718] 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.

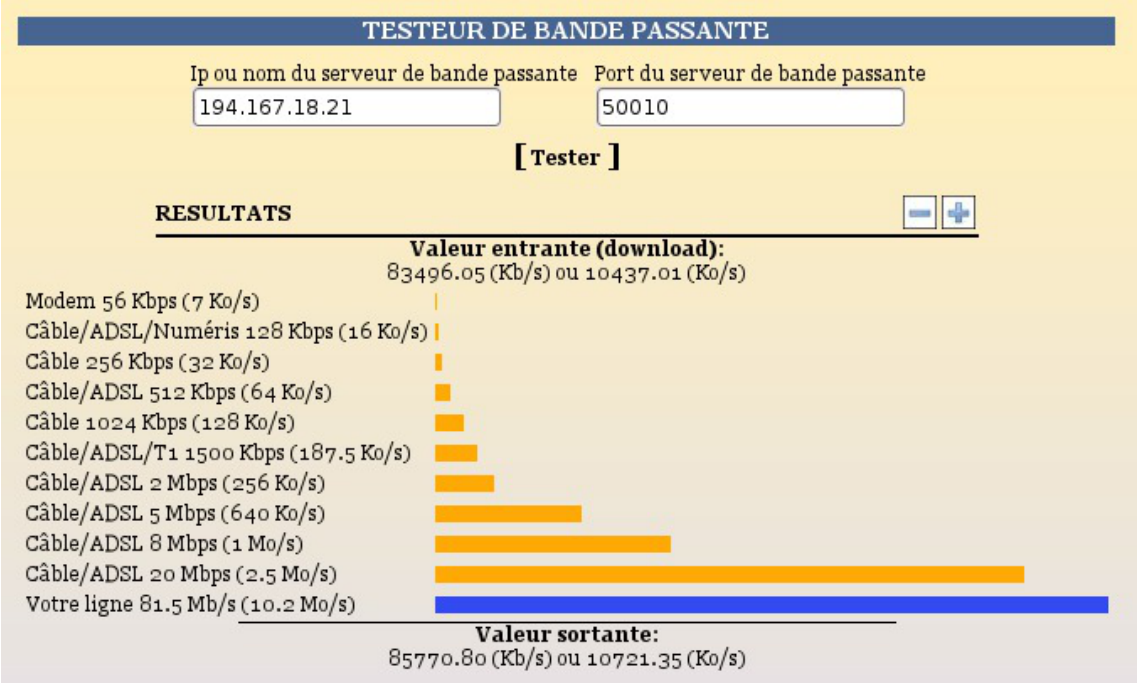
Sur EOLE 2.9, les interfaces VLAN ne sont plus affichées par l'outil `lshw` et n'apparaissent

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> donc plus dans l'interface.

1.4.13. Bande passante

Le menu `Outils/Bande passante` permet de tester la bande passante dont dispose le serveur.



Testeur de bande passante

1.4.14. Résoudre des dysfonctionnements liés à l'EAD

Services et journaux

Les fichiers journaux associés aux services EAD sont les suivants :

- `/var/log/rsyslog/local/ead-server/ead-server.info.log`
- `/var/log/rsyslog/local/ead-web/ead-web.info.log`

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation des fichiers journaux n'apportent pas d'informations pertinentes, le service peut être exécuté manuellement à l'aide des commandes suivantes :

```
service ead-server stop
cd /tmp
export PYTHONPATH=/usr/share
twistd3 -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, le service peut être exécuté manuellement à l'aide des commandes suivantes :

```
service ead-web stop
cd /tmp
export PYTHONPATH=/usr/share
twistd3 -noy /usr/share/ead2/frontend/frontend.tac
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

Certificats SSL

Pour avoir accès à l'EAD, il faut impérativement que le nom de domaine soit présent dans le certificat SSL.

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

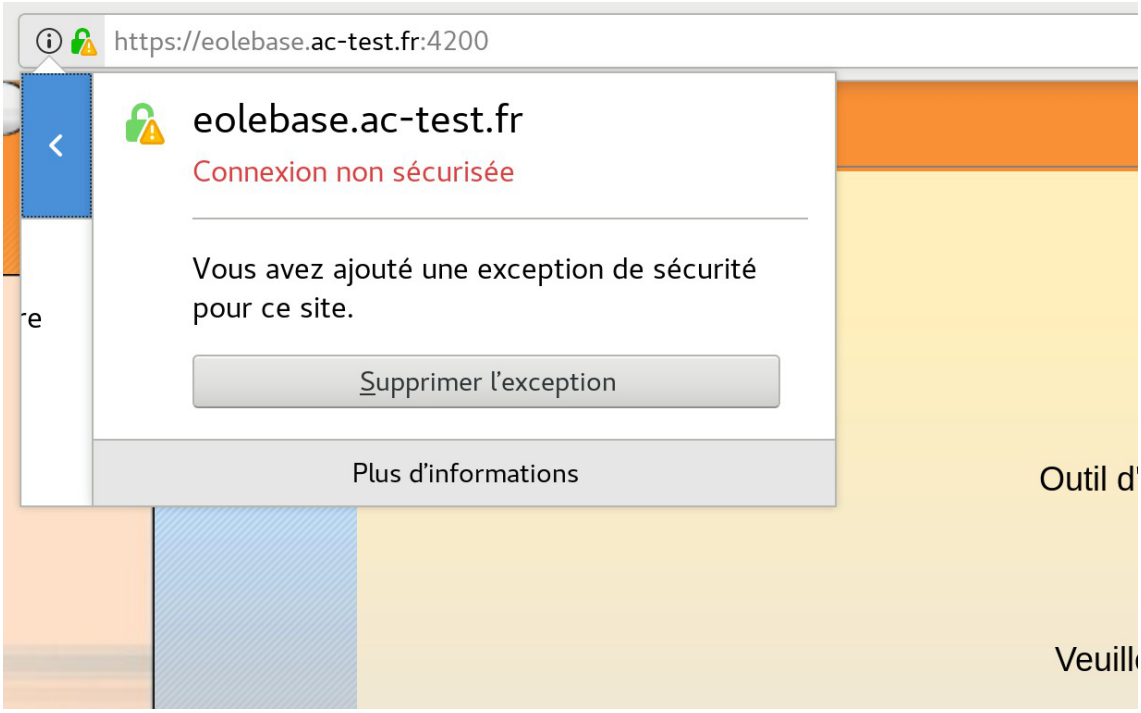
Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

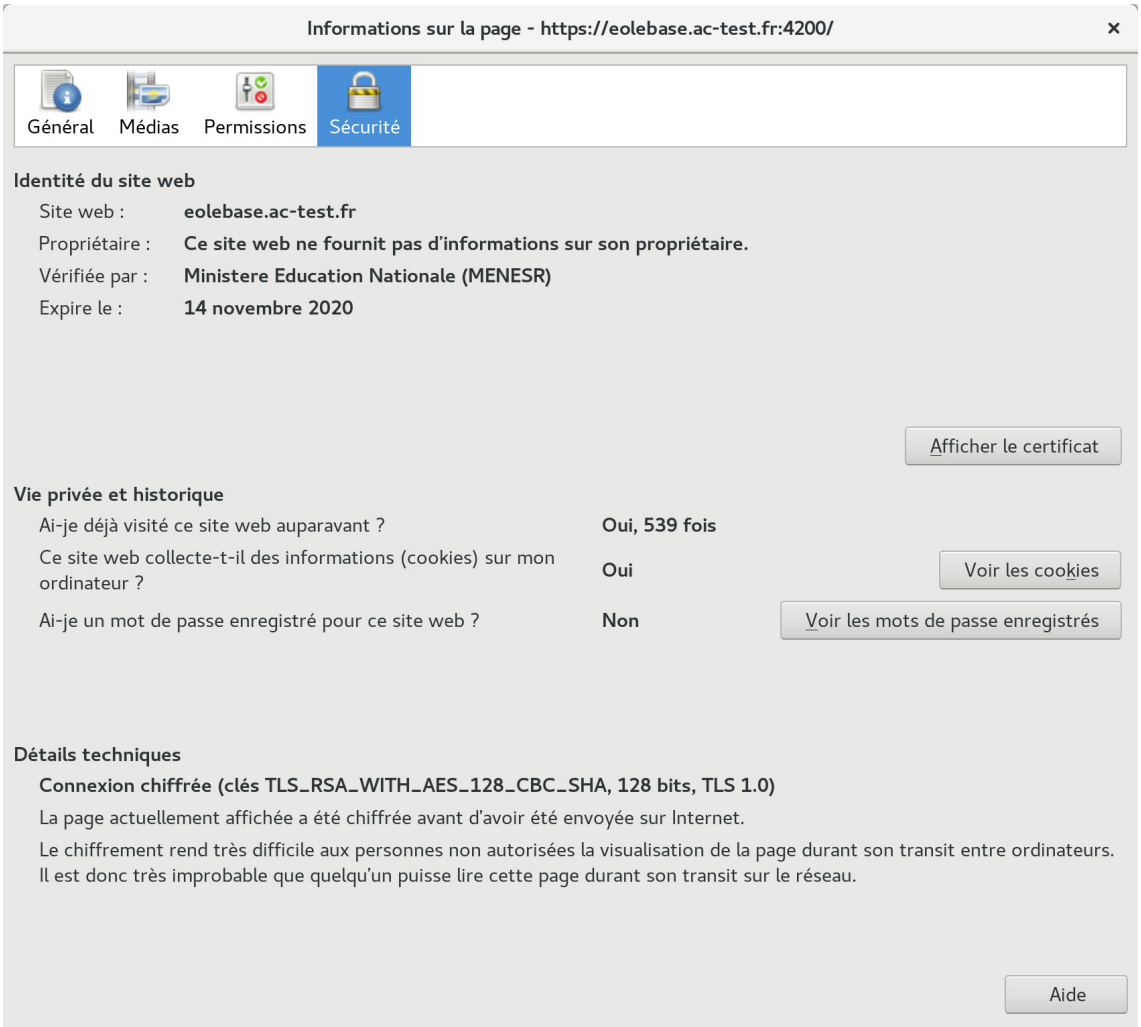


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



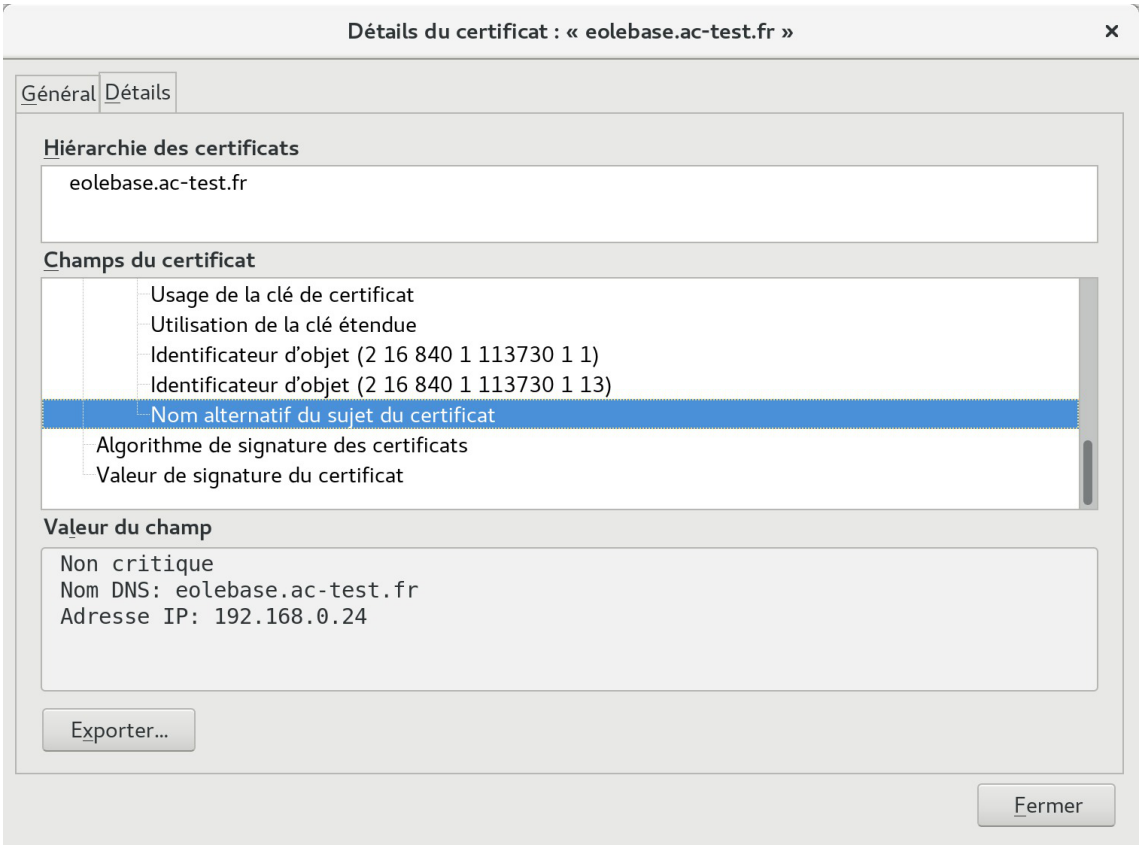
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- Il est possible que des noms alternatifs soient renseignés dans le certificat. Pour les retrouver, cliquer sur le bouton `Afficher le certificat`, puis sur l'onglet `Détails` et

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.



Attention, même si la bonne adresse IP apparaît dans le certificat, elle ne sera pas prise en compte.

Si le nom de domaine n'apparaît pas et que le certificat est de type autosigné, il faut le rajouter dans l'onglet `Certificats ssl` de l'interface de configuration du module en mode expert.

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom d'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 puis d'exécuter la reconfiguration du module :

```
rm -f /etc/ssl/certs/eole.crt
reconfigure
```

Clés d'enregistrement

Les interfaces associées au serveur de commandes local sont enregistrées dans le fichier `/usr/share/ead2/backend/config/frontend_keys.ini`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
[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`

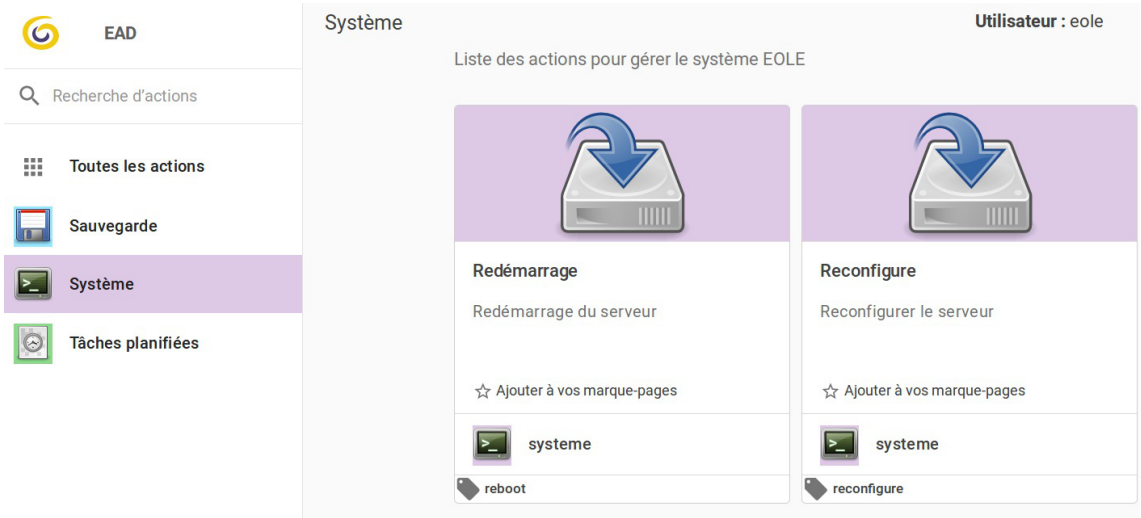
```
[1]
url = https://127.0.0.1
port = 4201
comment = amon
key = 157b551f55359d92d20e412e83f87f9ea2e47ab3
```

Si nécessaire, il est possible de réinitialiser ces fichiers à l'aide des commandes suivantes :

```
1 echo '[keys]' > /usr/share/ead2/backend/config/frontend_keys.ini
2 echo '' > /usr/share/ead2/frontend/config/servers.ini
3 reconfigure
```

1.5. L'interface d'administration EAD 3

EOLE offre une nouvelle interface simplifiée de gestion du serveur : l'interface d'administration EAD 3.



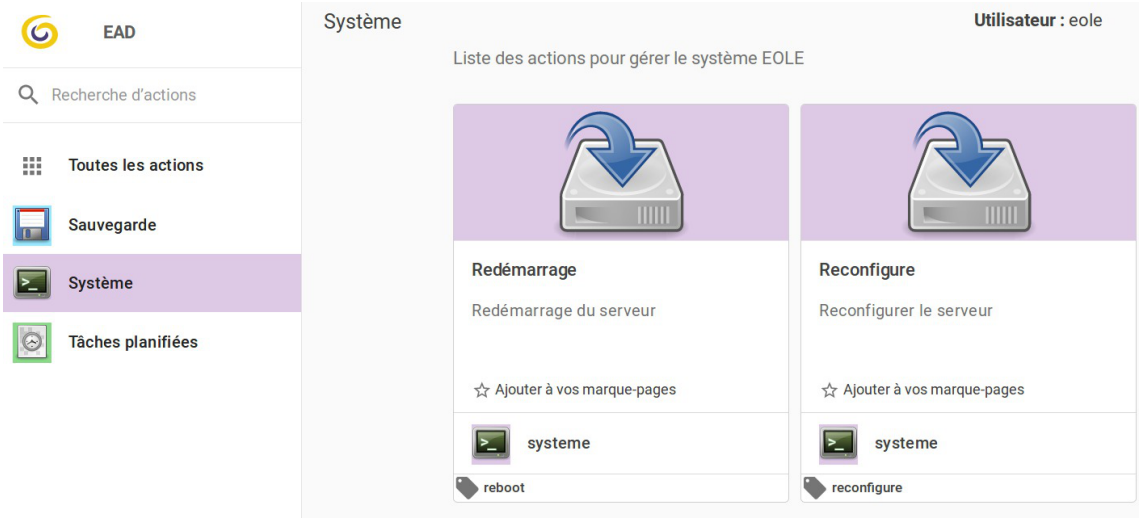
Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

L'EAD 3 est préinstallé sur les modules mais n'est pas activé.

1.5.1. Présentation

EOLE offre une nouvelle interface simplifiée de gestion du serveur : l'interface d'administration EAD 3.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Cette interface propose un ensemble d'actions utilisables par une personne peu habituée au système Unix.

L'EAD 3 est préinstallé sur les modules mais n'est pas activé.

1.5.2. Installation et configuration

Activation

L'EAD3 est préinstallé sur les modules mais n'est pas activé.

L'activation s'effectue dans l'onglet `Services` de l'interface de configuration du module en mode expert.



Pour que l'activation soit effective il faut reconfigurer le module.

Pour activer l'EAD3 en ligne de commande :

```
# CreoleSet activer_ead3 oui
```

Son activation nécessite la reconfiguration du serveur :

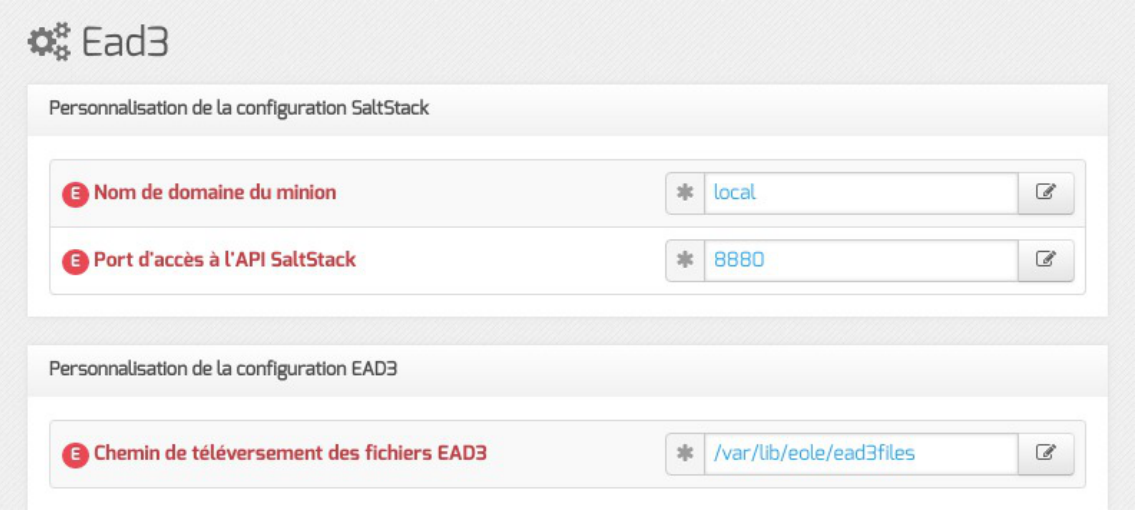
```
# reconfigure
```

Configuration

L'onglet `Ead3` est uniquement disponible après avoir passé `Activer l'interface d'administration du module (EAD3)` à `oui` dans l'onglet `Services`.

Il permet de personnaliser la configuration Saltstack[p.729] de l'EAD3.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Le port d'écoute par défaut de l'API Saltstack est 8880.

Le choix du chemin de téléversement des fichiers EAD3 est par défaut `/var/lib/eole/ead3files`.

1.5.3. L'application web

Pour accéder à l'application EAD3 il faut utiliser l'URL suivante : https://<serveur>/ead/

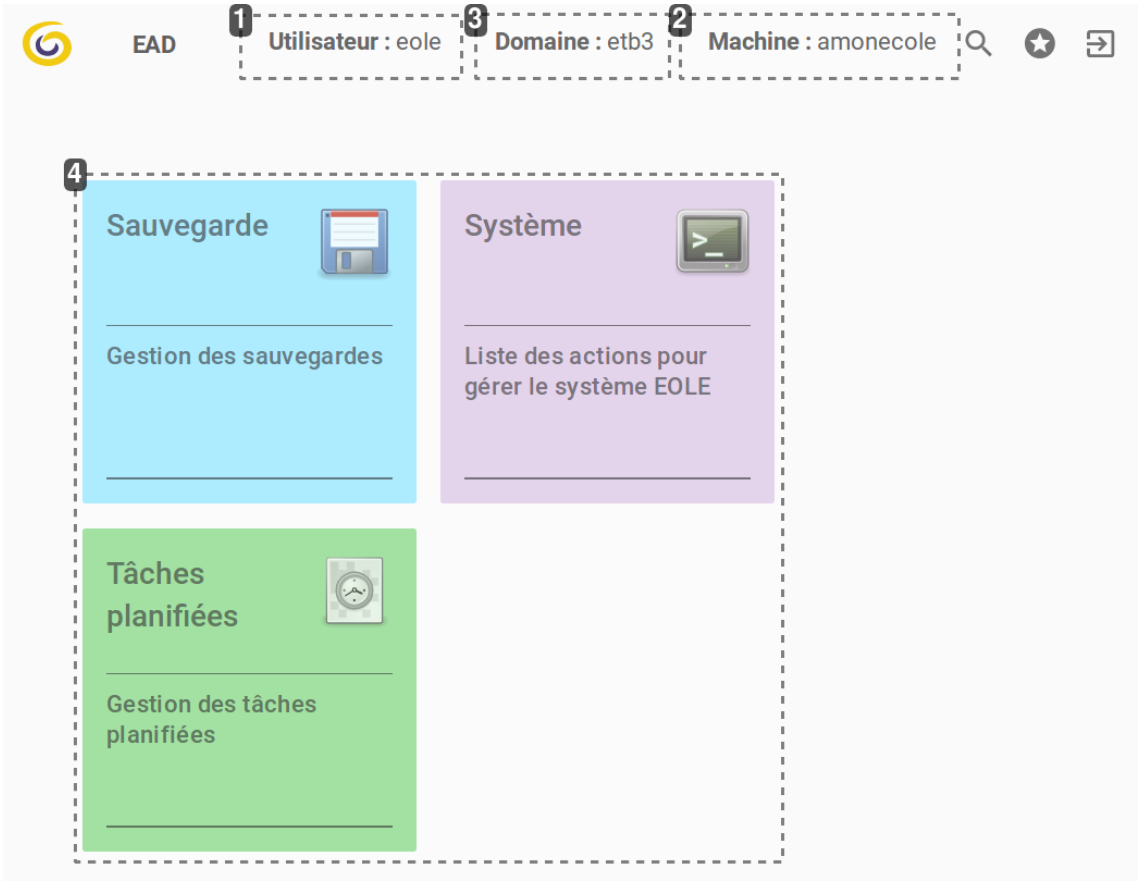
Une mire d'authentification apparaît. Saisir le compte et la clé secrète associée.

Pour le moment l'authentification est réalisée avec PAM[p.725], vous pouvez par exemple utiliser le compte `eole` et le mot de passe défini à l'instanciation du module ou créer un autre compte.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

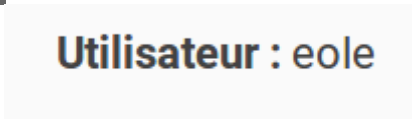


Description des éléments de la page principale



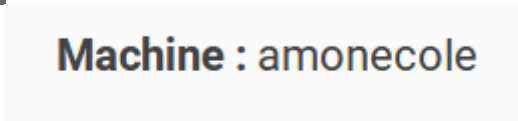
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1



Compte connecté

2



Nom de machine du serveur que l'application administre.

3



Nom de domaine du serveur que l'application administre.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

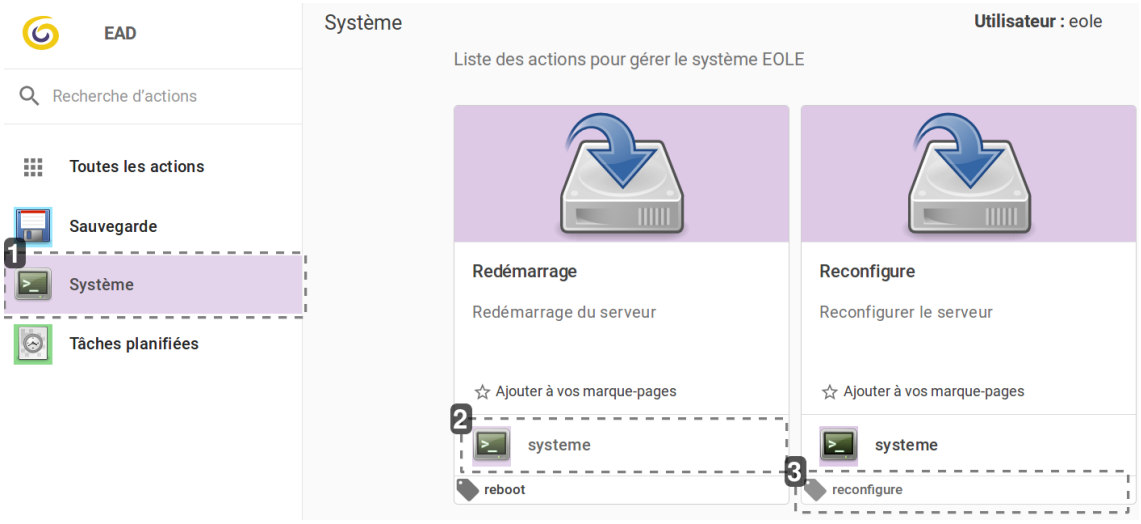
4



Catégories d'actions (exemple : sauvegarde, système…)

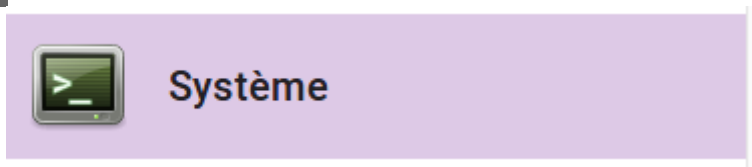
Cliquer sur une catégorie particulière permet d'afficher une vue propre à la catégorie.

Description de la vue par catégorie



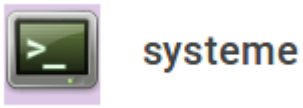
création : Mars 2022 Version : révision : Avril 2022
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1



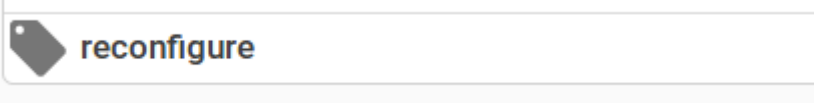
La catégorie choisie est en surbrillance.

2



Chaque action appartient à une catégorie.

3



Les étiquettes ne sont pas liées à une catégorie, elles déterminent un ensemble d'actions.

1.5.4. Généralités sur les actions

Une action est une fonctionnalité de l'EAD3 permettant de réaliser un ou plusieurs traitements sur un ou plusieurs serveurs cibles.

Une action est construite à partir de deux éléments :

- un fichier XML Creole[p.708] permettant de décrire l'action et de définir les variables et/ou les configurations nécessaires pour construire l'interface web ;
- un fichier de recette SaltStack[p.729] (nommé States) permettant d'effectuer l'action demandée sur les serveurs cibles.

Ces fichiers sont stockés sur le serveur dans le répertoire `/usr/share/eole/creole/extra/`.

Un sous-répertoire correspond à une action et son nom est le nom de l'action.

Par exemple, l'action *majreport* est définie à la création du répertoire enfant `/usr/share/eole/creole/extra/majreport/` qui contient le XML Creole, et éventuellement une recette SaltStack.

Si une recette SaltStack est associée à l'action, elle doit obligatoirement être placée dans le répertoire enfant `sls/` de l'action.

```
root@scribe:~# tree /usr/share/eole/creole/extra/backuponce
/usr/share/eole/creole/extra/backuponce
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
├── 00_action.xml
└── sls
    └── eole
        └── init.sls

2 directories, 2 files
root@scribe:~#
```

Dans les dossiers `sls` des actions déjà existantes, un sous-dossier `eole` est présent. Il contient les recettes SaltStack fournies par EOLE.

Plusieurs recettes SaltStack successives peuvent être appelées. Un fichier `init.sls` permet d'inclure toutes les recettes à appliquer dans un ordre spécifique.

Pour personnaliser le comportement d'une action existante il faut placer les recettes SaltStack directement dans le répertoire parent.

Par exemple pour surcharger le comportement des recettes EOLE de l'action *majonce* il faut placer les recettes personnalisées dans `/usr/share/eole/creole/extra/majonce/sls/`.

Les fichiers personnalisés des recettes SaltStack peuvent être templatisés avec Jinja2[p.716].

Dans ce cas, l'accès aux variables Creole se fait via les pillars[p.729].

Si l'on souhaite accéder à la variable Creole *hour* de la famille *mise_a_jour* de l'action *majonce*, il faut écrire dans la recette : *pillar['majonce.mise_a_jour.hour']*.

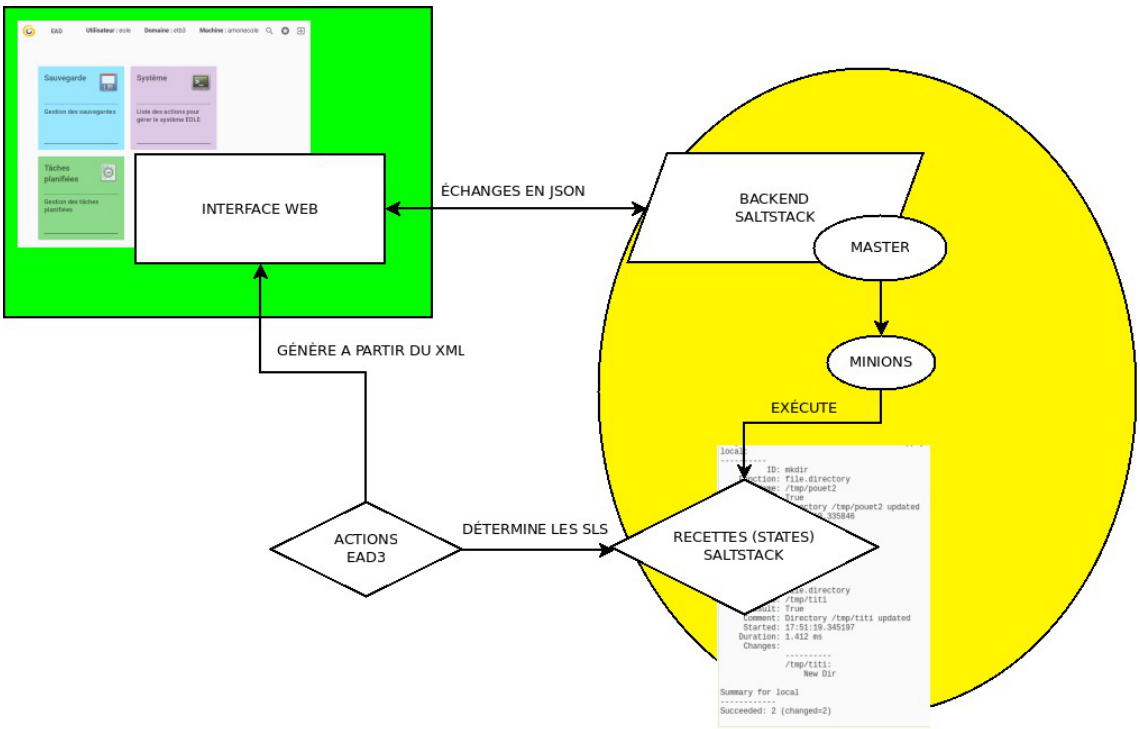


Diagramme de fonctionnement

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
<creole>
    <family_action name="Catégorie contenant une ou plusieurs actions">
        <action type="reader"
            title="Nom appraissant dans l'interface web"
            description="Description de l'action apparaissant dans
l'interface web"
            image="icons/edit-find.svg">
            <profile>ead_admin</profile>
            <ewtapp>ead</ewtapp>
            <tag>étiquette1</tag>
            <tag>étiquette2</tag>
        </action>
    </family_action>

    <variables>
        <family name="options">
            <variable name="filename" type="filename">
        </family>
    </variables>
</creole>

```

Balises et variables qui permettent de définir l'interface pour une action de type formulaire :

- *<family_action>* : Cette balise est obligatoire, elle permet de définir la catégorie qui contient l'action (si on veut ranger l'action à créer dans une catégorie existante, il suffit de renseigner le nom de la catégorie, si on veut créer une nouvelle catégorie, il suffit de mettre un nouveau nom) ;
- *<action>* : Cette balise est obligatoire, elle définit l'action d'une manière générique ;

  type : Le type de l'action, exemple *reader* pour une action d'affichage, *form* pour une action de type formulaire, *custom* pour une action personnalisée ;

  title : Intitulé de l'action ;

  descriptif : Courte description de l'action ;

  image : Les icônes disponibles sont dans le répertoire : `/usr/share/ewt/static/images/icons/` ;
- <family name="options"><variable name="filename" type="filename"> : Permettent de définir les variables Creole nécessaires au bon fonctionnement de l'action ;
- *<ewtapp>* : Applications dans lesquelles l'action doit apparaître (une balise par application), ici seulement l'EAD ;
- *<profile>* : L'action n'est accessible que pour le profil *ead_admin* ou un profil équivalent ou supérieur ;
- *<tag>* : Permet de déclarer une ou plusieurs étiquettes dans l'interface EAD.

Il est possible, comme dans n'importe quel XML Creole, de mettre en place des contrôles et des conditions sur les variables déclarées.

1.5.5. Créer une nouvelle action

Pour créer une nouvelle action il est possible de prendre modèle sur une action existante :

```
# cp -R /usr/share/eole/creole/extra/majreport/00_action.xml
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`/usr/share/eole/creole/extra/test/00_action.xml`

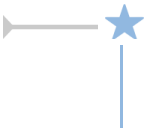
À gauche la copie de l'action de droite

```
<creole>
<creole>
    <family_action name="Test"
     <family_action name="Mise à jour"
                   description="Test"
                    description="Gestion de la mise à jour"
                   color="#0000dd"
                    color="#fca474"
                   image="icons/mail-attachment.svg">
                    image="icons/applications-internet.svg">
    <action type="reader"
     <action type="reader"
           title="Test de lecture"
            title="Rapport de mise à jour"
           description="Afficher le contenu d'un fichier"
            description="Afficher le journal de la dernière mise à jour"
           image="icons/face-angel.svg">
            image="icons/edit-find.svg">
           <profile>ead_admin</profile>
            <profile>ead_admin</profile>
           <ewtapp>ead</ewtapp>
            <ewtapp>ead</ewtapp>
           <tag>lecture</tag>
            <tag>log</tag>
           <tag>fichier</tag>
            <tag>maj</tag>
           <tag>test</tag>
            <tag>maj-auto</tag>
       </action>
            <tag>mise à jour</tag>
    </family_action>
         </action>
    <variables>
     </family_action>
        <family name="options"
     <variables>
                description="Contenu du fichier  ">
         <family name="options"
            <variable name="filename" type="filename">
                 description="Dernière mise à jour">
                <value>/usr/share/eole/creole/extra/test/00_action.xml
</value>             <variable name="filename" type="filename">
            </variable>
                 <value>/var/lib/eole/reports/rapport-maj.log</value>
            <variable name="language" type="string">
             </variable>
                <value>prolog</value>
             <variable name="language" type="string">
            </variable>
                 <value>prolog</value>
        </family>
              </variable>
    </variables>
         </family>
    <constraints>
     </variables>
    </constraints>
     <constraints>
    <help/>
     </constraints>
</creole>
     <help/>

</creole>
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour que la nouvelle action soit prise en compte il faut reconfigurer le serveur à l'aide de la commande `reconfigure` ou appliquer les commandes suivantes :

```
# /usr/share/eole/postservice/00-actions reconfigure
# CreoleCat -t ext_auth.conf
# service salt-api restart
```



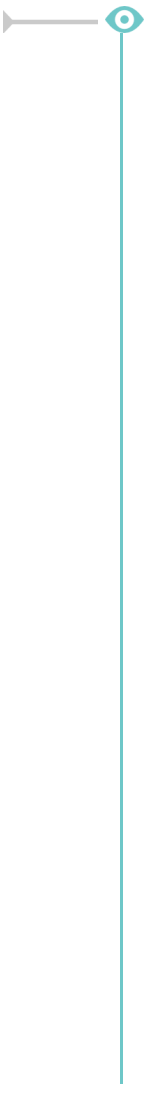
Dans un cas comme dans l'autre il est préférable de se déconnecter et se reconnecter à l'EAD.

Pour supprimer une action :

```
# rm -r /usr/share/eole/creole/extra/test/
# reconfigure
```

1.5.6. Type d'actions

1.5.6.a. Les actions d'affichage



```
<creole>
    <family_action name="Tâches planifiées">
        <action type="reader"
        title="Rapport de mise à jour"
        description="Visualisation du fichier de log de MajAuto"
        image="icons/edit-find.svg">
        <profile>ead_admin</profile>
        <ewtapp>ead</ewtapp>
        <tag>log</tag>
        <tag>maj</tag>
        <tag>maj-auto</tag>
        <tag>mise à jour</tag>
        </action>
    </family_action>

    <variables>
        <family name="options">
        <variable name="filename" type="filename">
        <value>/var/lib/eole/reports/rapport-maj.log</value>
        </variable>
        <variable name="language" type="string">
        <value>prolog</value>
        </variable>
        </family>
    </variables>

<constraints>
</constraints>

<help/>

</creole>
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
33
```

Balises et variables qui permettent de définir l'interface pour une action de type affichage :

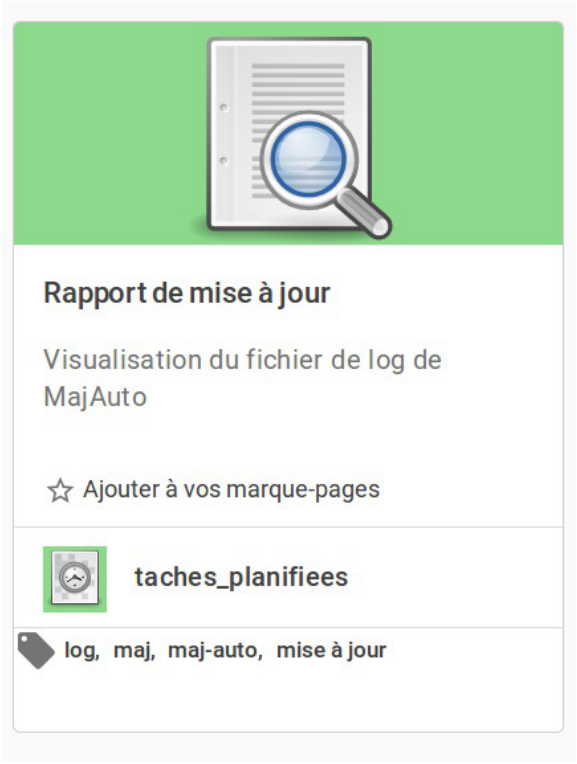
- *<family_action>* et *<action>* : permettent de définir l'action d'une manière générique ;

Des variables Creole sont définies dans la rubrique *familly* et sont utiles pour le fonctionnement de l'action :

- la variable *filename* contient le nom long du fichier à afficher ;
- la variable *language* est optionnelle, elle contient le mode de coloration syntaxique utilisé pour afficher le fichier en couleur.

Ces variables sont des variables Creole chargée en mémoire vives, si on veut qu'elles soient enregistrées il faut renseigner l'attribut *save=True* et elles leurs nouvelles valeurs seront stockées dans un `config.eol` (qui n'est pas le `/etc/config.eol` principal de Creole).

L'action d'affichage est de type *filename* et est préexistante. Elle ne nécessite aucune recette SaltStack particulière. Donc seul le fichier XML Creole est présent.



L'action Rapport de mise à jour

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Rapport de mise à jour

1.5.6.b. Les actions de type formulaire

Les actions de type formulaire sont des actions qui ont besoin de paramètres pour pouvoir être lancées.

Dans ce cas, il faut faire apparaître un formulaire pour renseigner les variables nécessaires au fonctionnement de l'action.

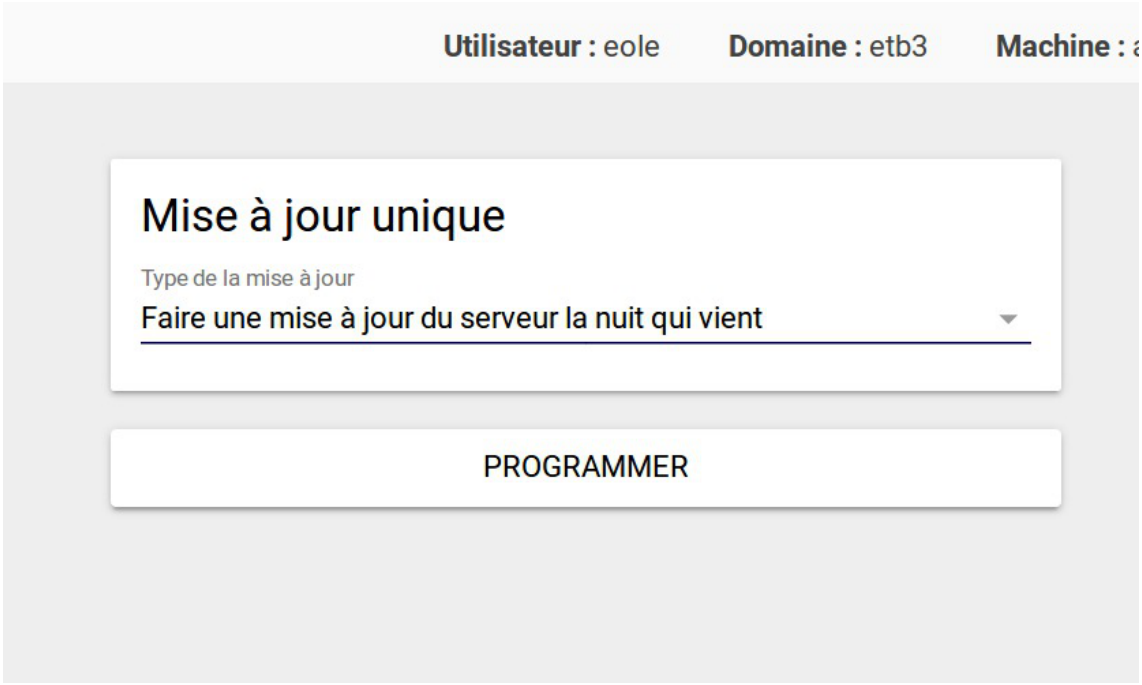
Ce formulaire est généré automatiquement à partir de la définition de variables dans le XML Creole.

```
<variables>
    <family name='Mise à jour'>
    <variable description="Type de la mise à jour" type="string" name="typemaj">
    <value>Faire une mise à jour du serveur la nuit qui vient</value>
    </variable>
    <variable description="Choisir les options de mise à jour" type="string" name="majoption">
    <value>Mise à jour, reconfigure et redémarrage du serveur</value>
    </variable>
    <variable description="Heure" name='hour' type='number'/>
    <variable description="Minute" name='minute' type='number'/>
    <variable description="Jour" name='day' type='date'/>
    </family>
</variables>

```

La définition de variables de type *string* ou de type *number* va générer un formulaire dans l'espace réservé à afficher l'action (widget).

- *<input>Programmer</input>*
  permet de définir un bouton de validation
- *<variable description="Type de la mise à jour" type="string" name="typemaj">*
  <value>Faire une mise à jour du serveur la nuit qui vient</value>
  </variable>
  fait apparaître une liste déroulante avec un item

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



1.5.7. Compléments techniques

Relancer l'EAD3

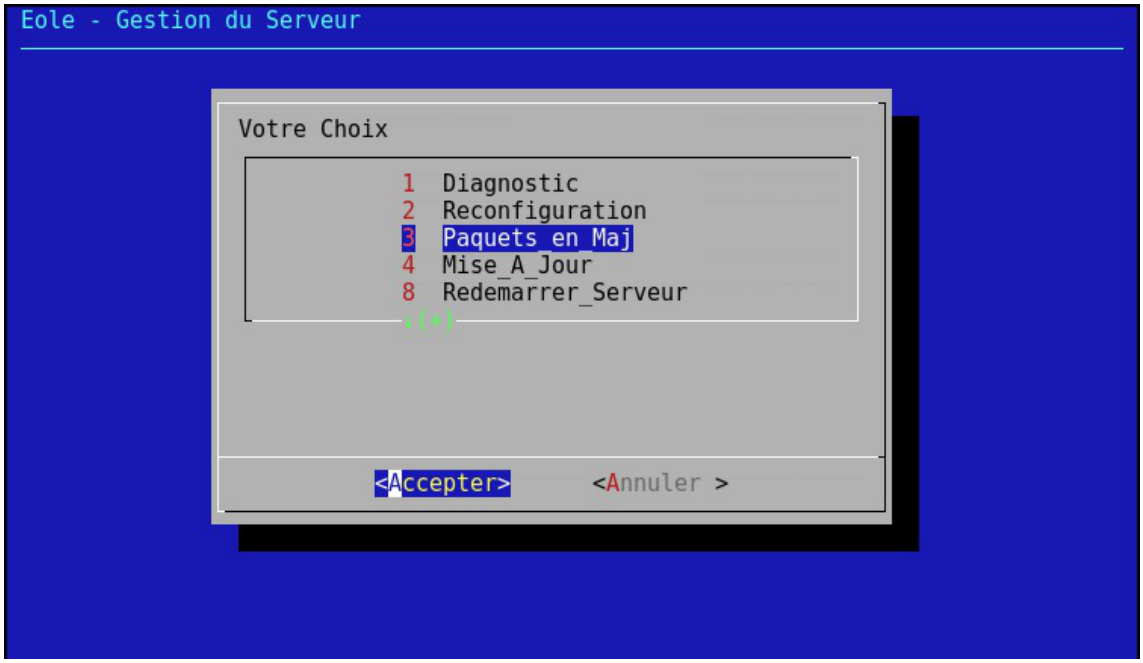
```
root@scribe:~# service salt-api status
● salt-api.service - The Salt API
   Loaded: loaded (/lib/systemd/system/salt-api.service; enabled; vendor preset:
enabled)
   Active: active (running) since mer. 2017-03-01 11:31:49 CET; 4min 22s ago
 Main PID: 9193 (salt-api)
   CGroup: /system.slice/salt-api.service
           ├─9193 /usr/bin/python /usr/bin/salt-api
           └─9614 /usr/bin/python /usr/bin/salt-api

mars 01 11:31:48 scribe systemd[1]: Starting The Salt API...
mars 01 11:31:49 scribe systemd[1]: Started The Salt API.
root@scribe:~#
```

1.6. 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ... créés à l'instance, et pour les administrateurs à droits restreints qui peuvent être créés avec la commande `add_restricted_admin` en dehors de la procédure d'instance.

1.7. 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 continuelles 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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`.

1.7.1. 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.

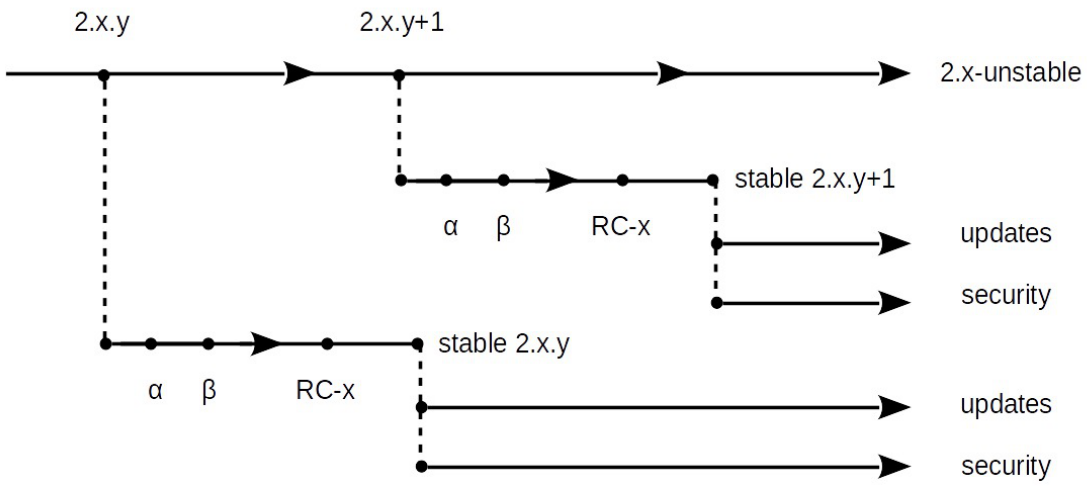
Par défaut une mise à jour hebdomadaire est configurée automatiquement à la fin de l'instanciation du module. Ce comportement est paramétrable et désactivable.

Depuis EOLE 2.6, il n'existe 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 (2.6.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.734] 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 (2.6.x). Chaque version d'EOLE bénéficie des dépôts :

- Security : paquets fixant un problème de sécurité ;
- Updates : paquets fixant des dysfonctionnement 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

La publication des paquets fait 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://pcll.ac-dijon.fr/eole/ ;
- envoi d'un message sur les principales listes de diffusion du projet : https://pcll.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/Journaux290 pour EOLE 2.9.0).

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 par la mise à jour hebdomadaire.

Mise à jour candidate annoncée

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

La publication des paquets fait 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://pcll.ac-dijon.fr/eole/ ;
- envoi d'un message sur les principales listes de diffusion du projet : https://pcll.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/Journaux290 pour EOLE 2.9.0).

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/Journaux280 pour EOLE 2.8.0).

Les paquets en version candidate non annoncés sont disponibles à tout moment uniquement dans les dépôts de test.

Ils s'installent à l'aide de la commande : `Maj-Auto -C -S test-eole.ac-dijon.fr`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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-2.8-unstable` pour EOLE 2.8) 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.661]

1.7.2. Les procédures de mise à jour

Les procédures manuelles de mise à jour des modules EOLE sont accessible de quatre manières :

- EAD[p.710] ;
- 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.

Proxy et mise à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

1.7.2.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.



Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

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.

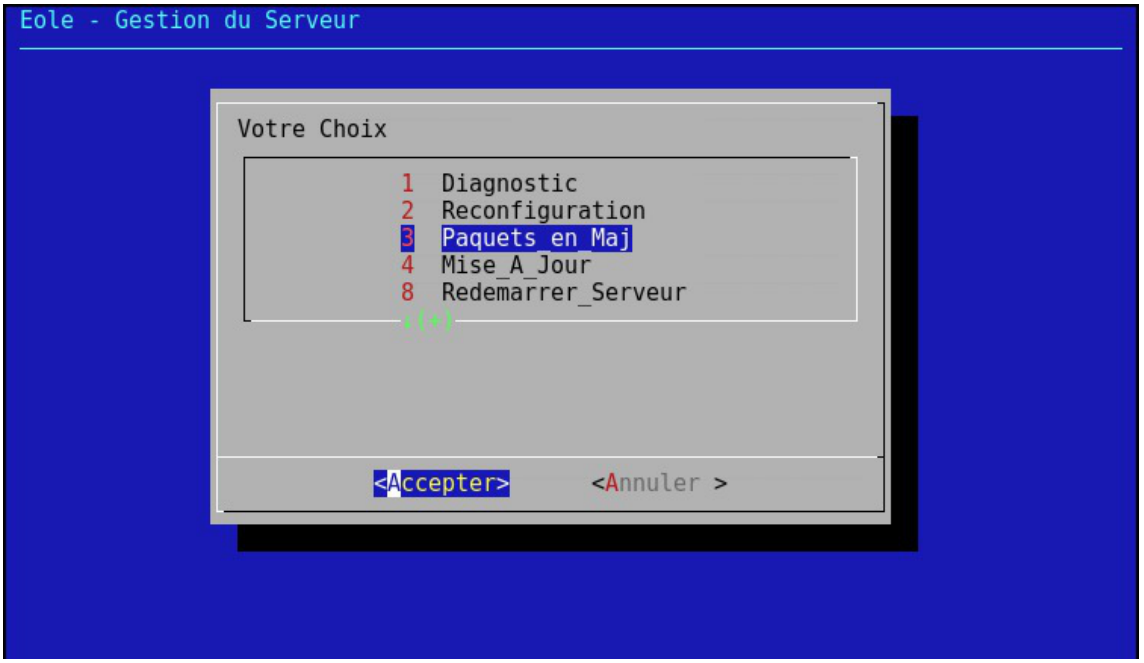
Si un redémarrage est nécessaire, celui-ci est effectué automatiquement dès la fin de la reconfiguration.

1.7.2.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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'interface semi-graphique : manage-eole

Par défaut, elle est proposée à la connexion pour les utilisateurs `eole`, `eole2`, ... créés à l'instance, et pour les administrateurs à droits restreints qui peuvent être créés avec la commande `add_restricted_admin` en dehors de la procédure d'instance.

1.7.2.c. Mise à jour

À la fin de la phase d'instanciation, la mise à jour automatique hebdomadaire est activée.

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



Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

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]
```

Voir aussi...

Gestion des tâches planifiées eole-schedule [p.636]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.7.2.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.

Suppression des commandes Maj-Cd et Query-Cd

Le mode d'installation des modules a évolué pour adopter la procédure d'Ubuntu.

Le CD-ROM d'installation ne contient plus les paquets spécifiques aux modules EOLE et ne peut plus servir de medium pour l'installation et la mise à jour.

Il n'est, par ailleurs, pas prévu de fournir des CD-ROM contenant les paquets d'une version donnée.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les commandes `Maj-Cd` et `Query-Cd` ne sont donc plus proposées.

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.710].

Options spécifiques aux scripts Maj-Auto et Query-Auto

- -C : force la mise à jour en version candidate pour tous les dépôts par défaut ou pour le (ex : -C envole) ou les dépôts spécifiés (ex : -C eole envole) ;
- -D : force la mise à jour des paquets en développement pour tous les dépôts par défaut ou pour le (ex : -D envole) ou les dépôts spécifiés (ex : -D eole envole) ;
- -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 au script Maj-Auto

- -n : exécuter en mode simulation (*dry run*) équivaut à utiliser les commandes `Query-Auto`.
- -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
```

Dépôts additionnels

Il est possible de spécifier un dépôt particulier via l'onglet `Dépôt tiers` de l'interface de configuration du module en mode expert.

Ce dépôt sera pris en compte à chaque exécution de la commande `Maj-Auto` et lors des mises à jour automatiques du serveur.

Voir aussi...

Les dépôts EOLE [p.661]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Reconfiguration [p.386]

Installation manuelle de paquets [p.458]

Onglet Dépôt tiers [p.240]

1.7.3. Ajout de dépôts supplémentaires

Les outils `Query-Auto` et `Maj-Auto` 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
```


L'ajout de dépôts supplémentaires est proposé dans l'interface de configuration du module, en mode expert, dans l'onglet `Dépôt tiers`.

Voir aussi...

Onglet Dépôt tiers [p.240]

1.7.4. Désactivation temporaire des mises à jour



Désactiver les mises à jour met en danger votre système. Il n'est pas recommandé de désactiver les mises à jour sauf dans certains cas et ce de manière temporaire.

Malgré les nombreux tests et la période d'incubation des paquets, il arrive parfois qu'un paquet ait un comportement inattendu, il est alors possible et souhaitable de ne pas déstabiliser l'ensemble du parc de machines. Reporter temporairement les mises à jour est l'une des solutions.

La désactivation des mises à jour peut s'effectuer de plusieurs façon :

- désactiver la mise à jour hebdomadaire dans l'EAD ;
- désactiver la mise à jour hebdomadaire avec Creole et eole-schedule ;
- personnaliser la fréquence de la mise à jour dans l'interface de configuration du module, onglet `Schedule` ;
- interdire les mises à jour du serveur dans le serveur Zéphir.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Voir aussi...

- Mise à jour depuis l'EAD [p.402]
- Gestion des tâches planifiées eole-schedule [p.636]
- Onglet Schedule [p.242]
- Les actions Zéphir sur les serveurs

1.8. 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.704] 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.704] et permet de gérer les paquets et leurs mises à jour.

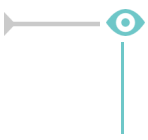
L'usage de la commande `apt-eole` en lieu et place de la commande `apt-get` est recommandée pour l'installation des paquets EOLE.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.707] proposés par EOLE.

Voir aussi...

Choisir le mode du module

Les mises à jour en ligne de commande [p.455]

1.9. Les administrateurs locaux à droits restreints

À l'instance, au moins un compte local d'administrateur à droits restreints est créés.

Ce type de compte est notamment utilisé pour accéder à l'interface d'administration EAD3.

Trois commandes sont proposées pour gérer ces comptes locaux.

list_restricted_admins

La commande list_restricted_admins retourne tous les comptes locaux appartenant au groupe adm et disposant de l'interface semi-graphique comme shell de connexion.

add_restricted_admin

La commande add_restricted_admin permet de créer un compte local appartenant aux groupes adm et mail et disposant de l'interface semi-graphique comme shell de connexion.

À la différence de la procédure de création de comptes locaux supplémentaires à l'instance, le nom n'est pas contraint à eole suffixé d'un numéro.

del_restricted_admin

La commande del_restricted_admin permet de supprimer un compte local appartenant au groupe adm et disposant de l'interface semi-graphique comme shell de connexion.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.10. Passage d'une version d'EOLE à une autre



Maj-Release

Le passage d'une version mineure à une autre (exemple de 2.8.0 à 2.8.1) est manuel et volontaire.
Il s'effectue par l'intermédiaire de la commande `Maj-Release`.
Il s'apparente à une grosse mise à jour car il n'implique pas de changement de la version d'Ubuntu utilisée en tant que base du module EOLE.

Consulter le manuel de la commande pour voir toutes les options :

```
# man Maj-Release
```

Upgrade-Auto

Le passage d'une version majeure à la suivante (exemple de 2.8.1 à 2.9.0) est manuel et volontaire.
Il s'effectue par l'intermédiaire de la commande `Upgrade-Auto`.

Consulter le manuel de la commande pour voir toutes les options :

```
# man Upgrade-Auto
```

1.11. Passage d'une version RC à une version stable

Avant d'être publiée en version RC, la distribution Linux EOLE subit de nombreux tests.
Aussi, elle ne contient plus aucun changement qui ne peuvent être résolus 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 s'effectue avec la commande `Maj-Auto`.

Les versions RC portent un numéro, il signifie uniquement qu'une image ISO a été

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> re-générée, un nombre conséquent de paquets ont été recompilés et cela évite une trop grosse mise à jour.

2. Fonctionnalités de l'EAD3 sur le module Amon

2.1. Fonctionnalités de l'EAD3 communes à tous les modules

2.1.1. Action de stockage de fichiers pour les actions EAD3

Gérer les fichiers



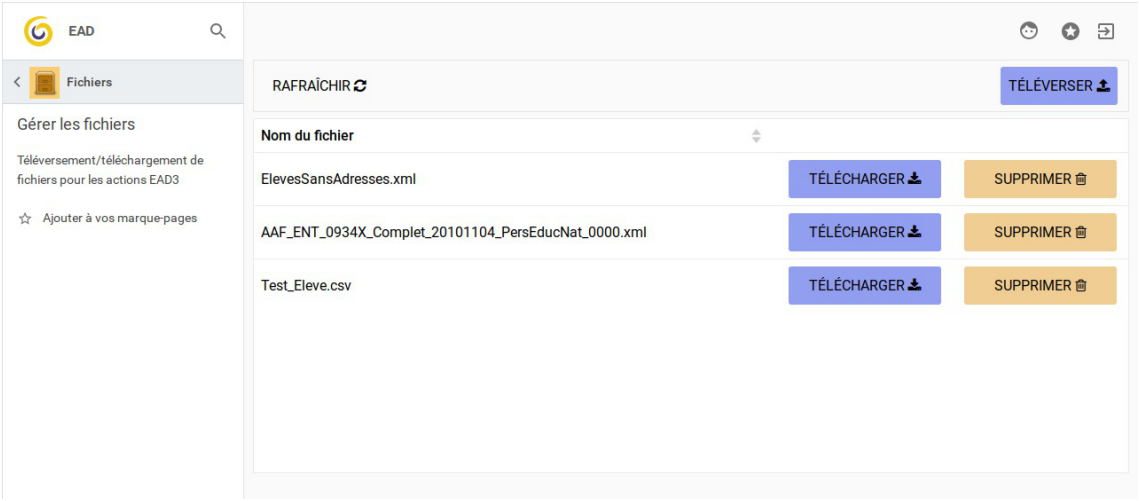
Cette action permet de téléverser des fichiers dans l'EAD3 dans le but d'être utilisés dans d'autres actions.

Elle permet également d'accéder à des fichiers créés par des actions lorsque ceux-ci sont trop lourds pour être affichés par l'action dédiée.

Téléverser des fichiers

Seuls les fichiers aux formats XML, CSV, TAR.GZ et ZIP sont autorisés.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



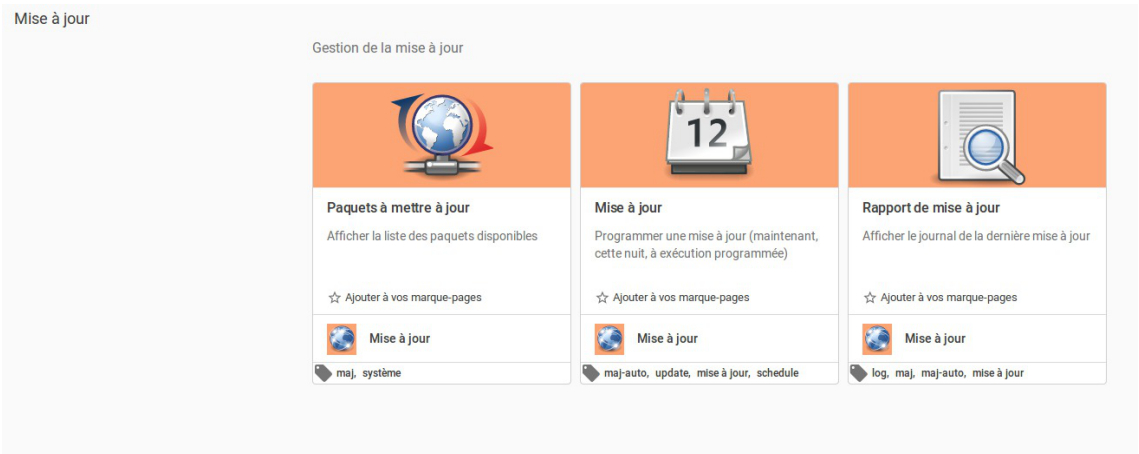
Par défaut les fichiers téléversés sont stockés dans le répertoire `/var/lib/eole/ead3files/`.

Ce chemin peut, si besoin, être modifié dans l'interface de configuration du module dans l'onglet `Ead3` en mode expert.

Le téléversement d'un fichier portant le même nom écrase celui déjà présent sur le serveur.

La liste des extensions autorisées est définie dans le template[p.733] : `ead3fileserver.conf`.

2.1.2. Action de mise à jour

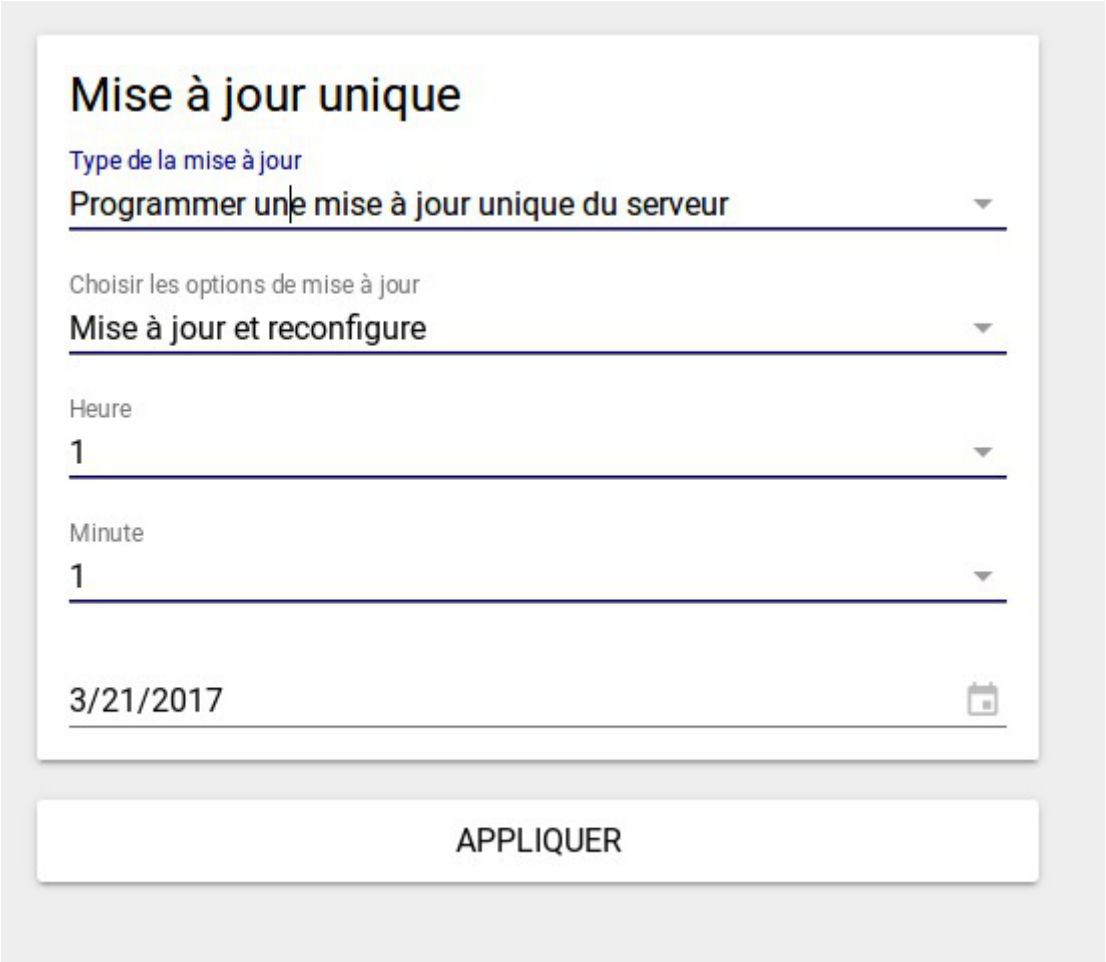


Trois actions sont disponibles.

- Paquets à mettre à jour ;
- Mise à jour ;
- Rapport de mise à jour.

La mise à jour unique

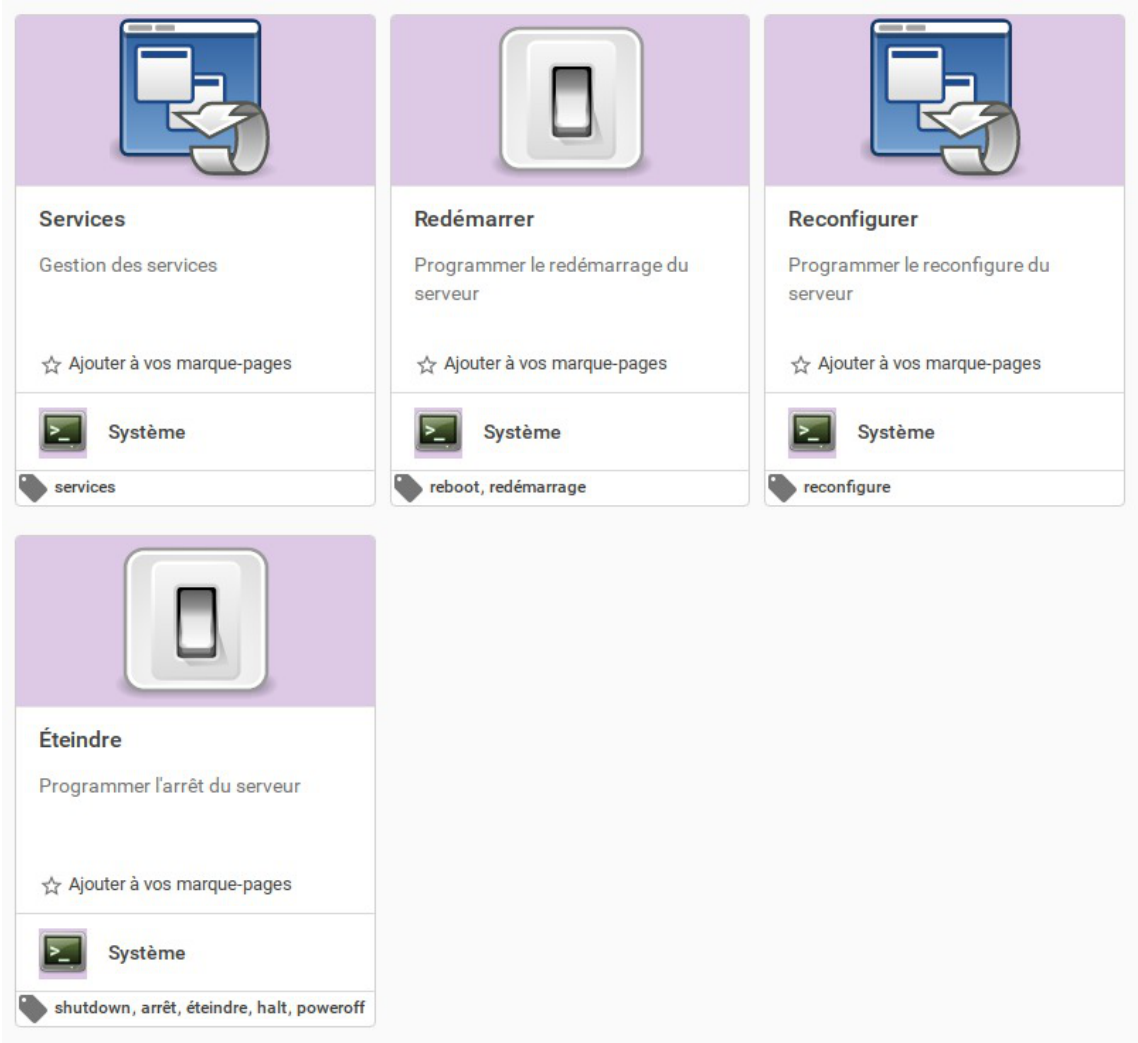
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



La mise à jour peut-être effectuée immédiatement, ou dans la nuit qui suit, ou bien à encore à une date précise.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2.1.3. Action système



Quatre actions sont disponibles :

- Services
- Redémarrer
- Reconfigurer
- Éteindre

Services

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



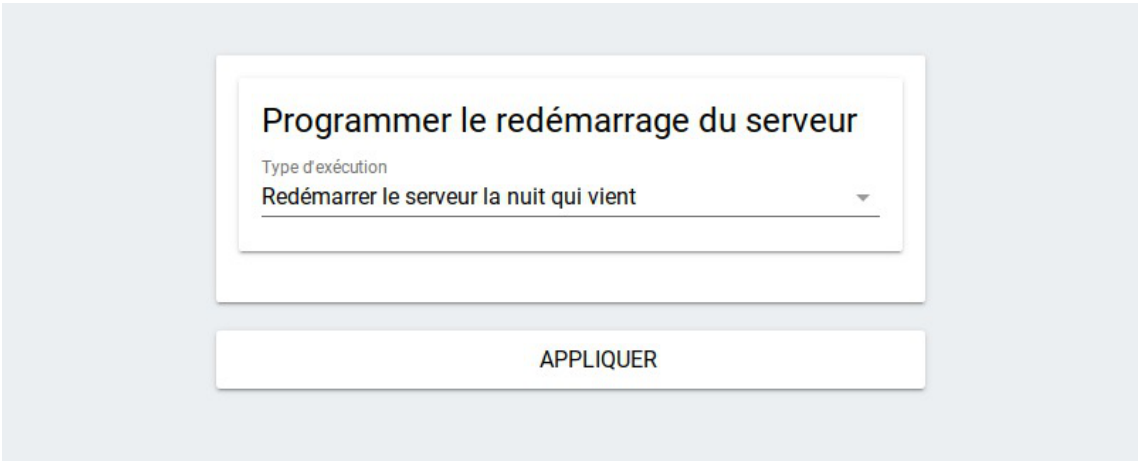
L'action Services liste les services du système et permet de les redémarrer ou des les arrêter immédiatement.

L'état actuel des services listés n'est pas affiché.

Sur un serveur en mode conteneur[p.707], certains services peuvent être listés plusieurs fois en fonction de leur emplacement.

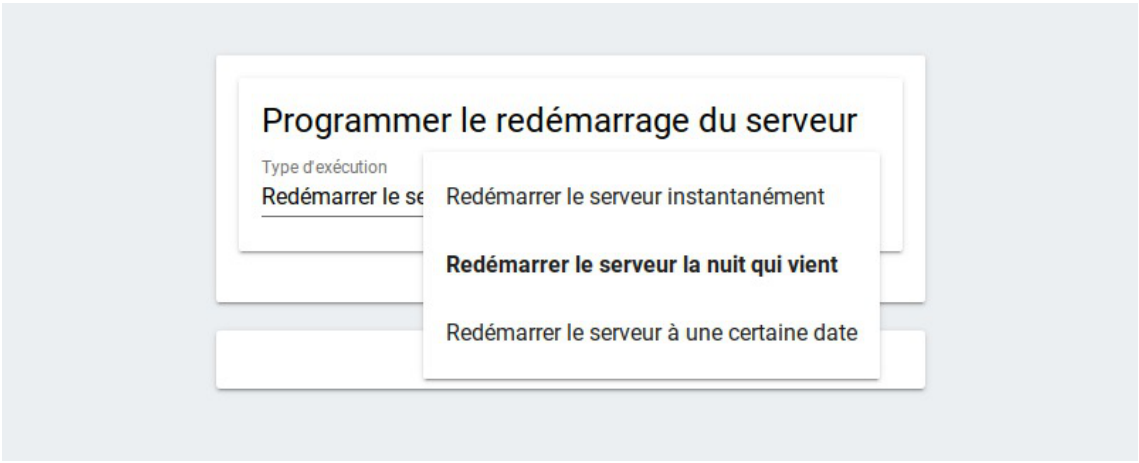
Redémarrer

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'action Redémarrer permet de programmer le redémarrage du serveur selon trois options de programmation :

- immédiatement ;
- la nuit suivante ;
- à une date et une heure données.

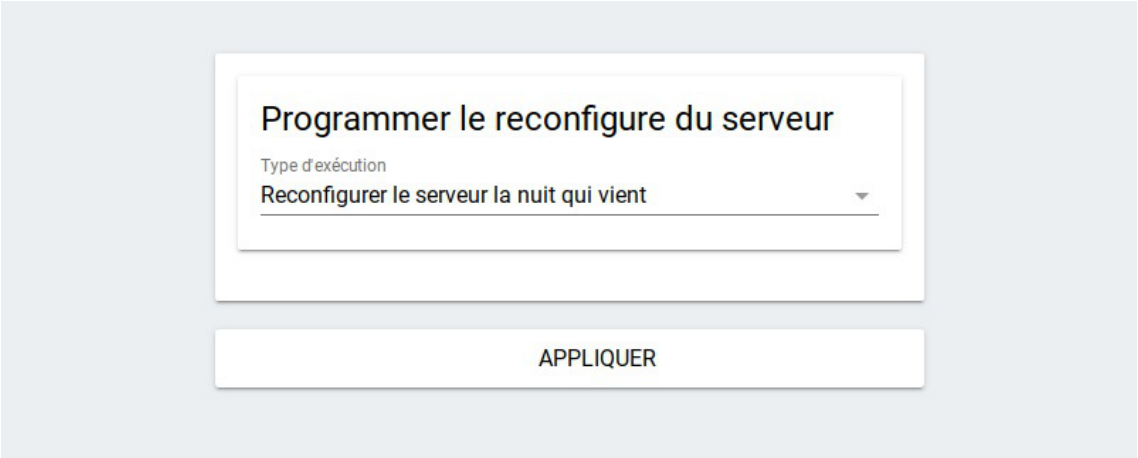


L'option permettant de préciser une date et un horaire de redémarrage nécessite de renseigner l'heure sous forme heure et minute et la date.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



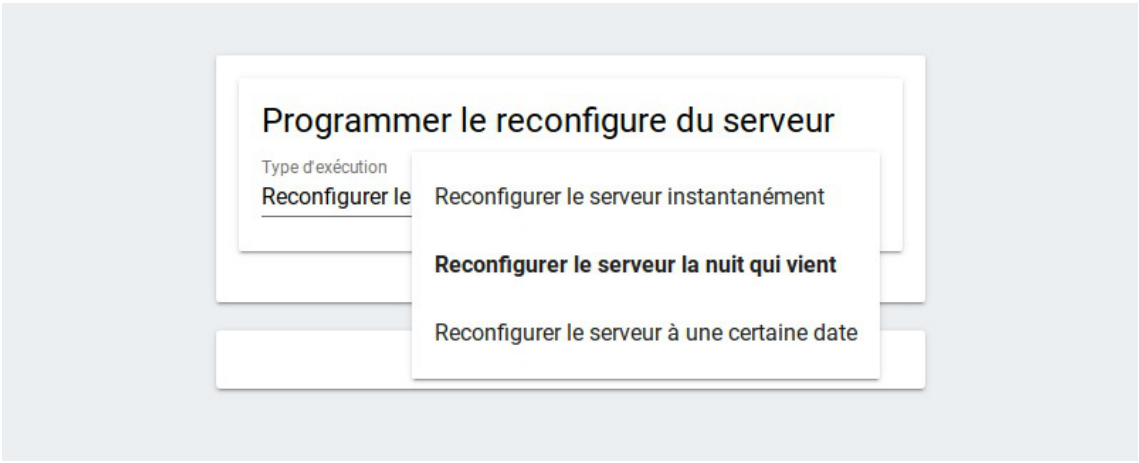
Reconfigurer



L'action Reconfigurer permet de programmer le reconfigure (cf. Reconfiguration) [p.386] du serveur selon trois options de programmation :

- immédiatement ;
- la nuit suivante ;
- à une date et une heure données.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

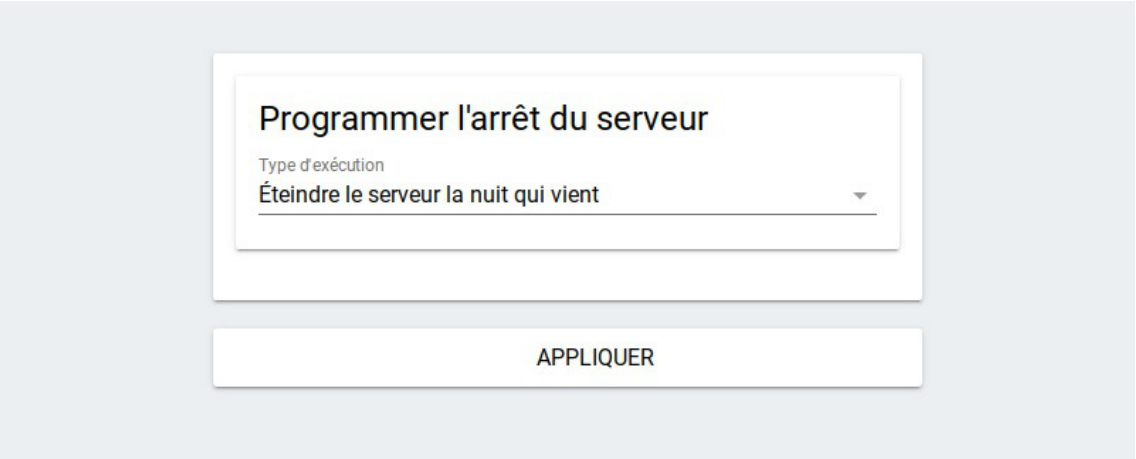


L'option permettant de préciser une date et un horaire de reconfigure nécessite de renseigner l'heure sous forme heure et minute et la date.



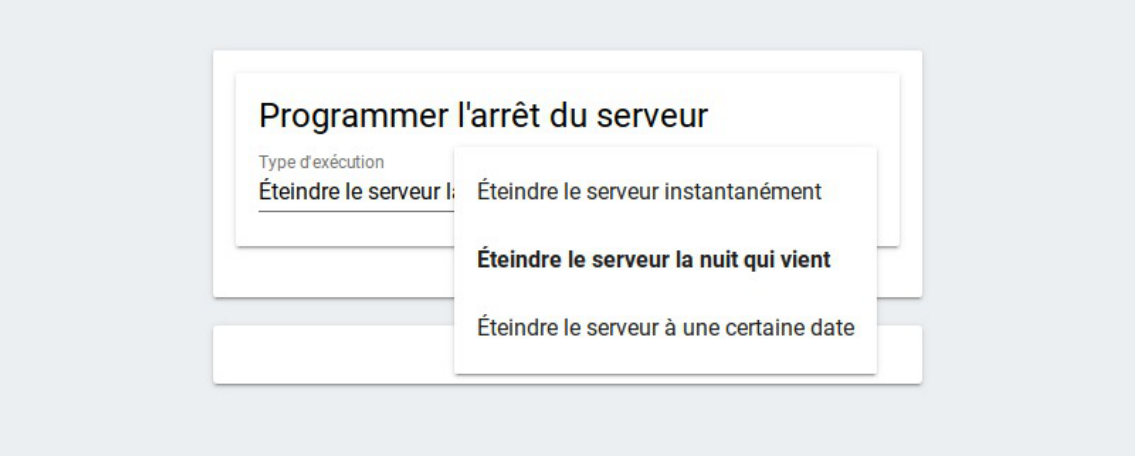
Éteindre

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



L'action Éteindre permet de programmer l'arrêt du serveur selon trois options de programmation :

- immédiatement ;
- la nuit suivante ;
- à une date et une heure données.



L'option permettant de préciser une date et un horaire d'arrêt nécessite de renseigner l'heure sous forme heure et minute et la date.

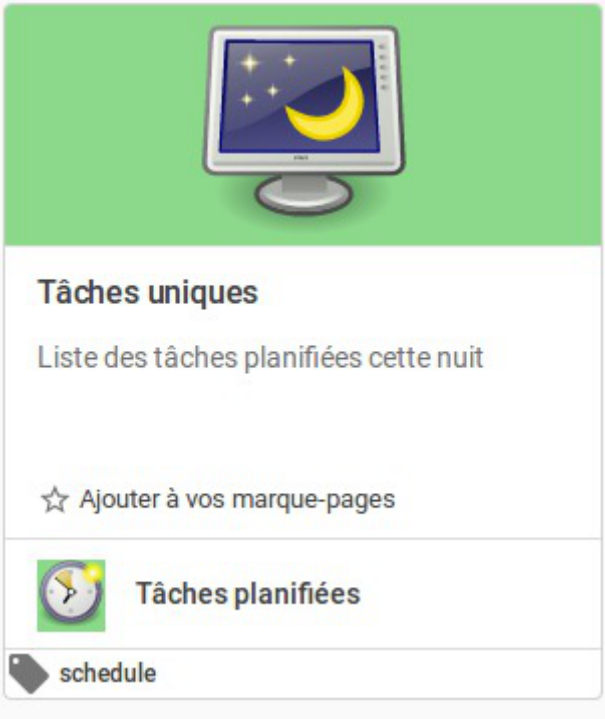
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



2.1.4. Action de tâches planifiées

Tâches planifiées cette nuit

L'action des tâches planifiées cette nuit permet de visualiser les tâches qui ont été planifiées "la nuit qui vient".



Il est possible de supprimer une action en cliquant sur la corbeille à droite de la ligne correspondante à la

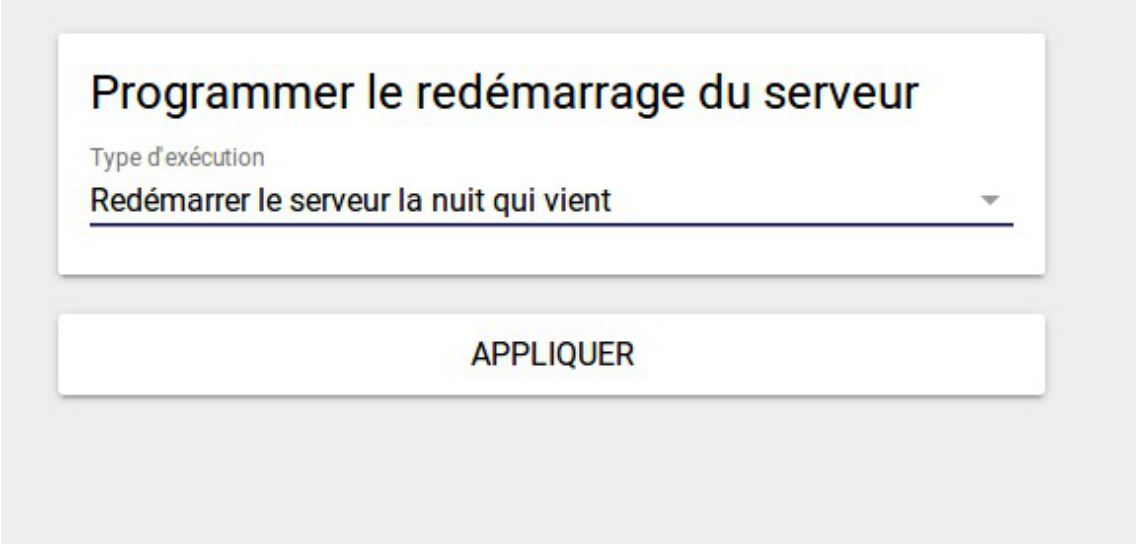
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

tâche.

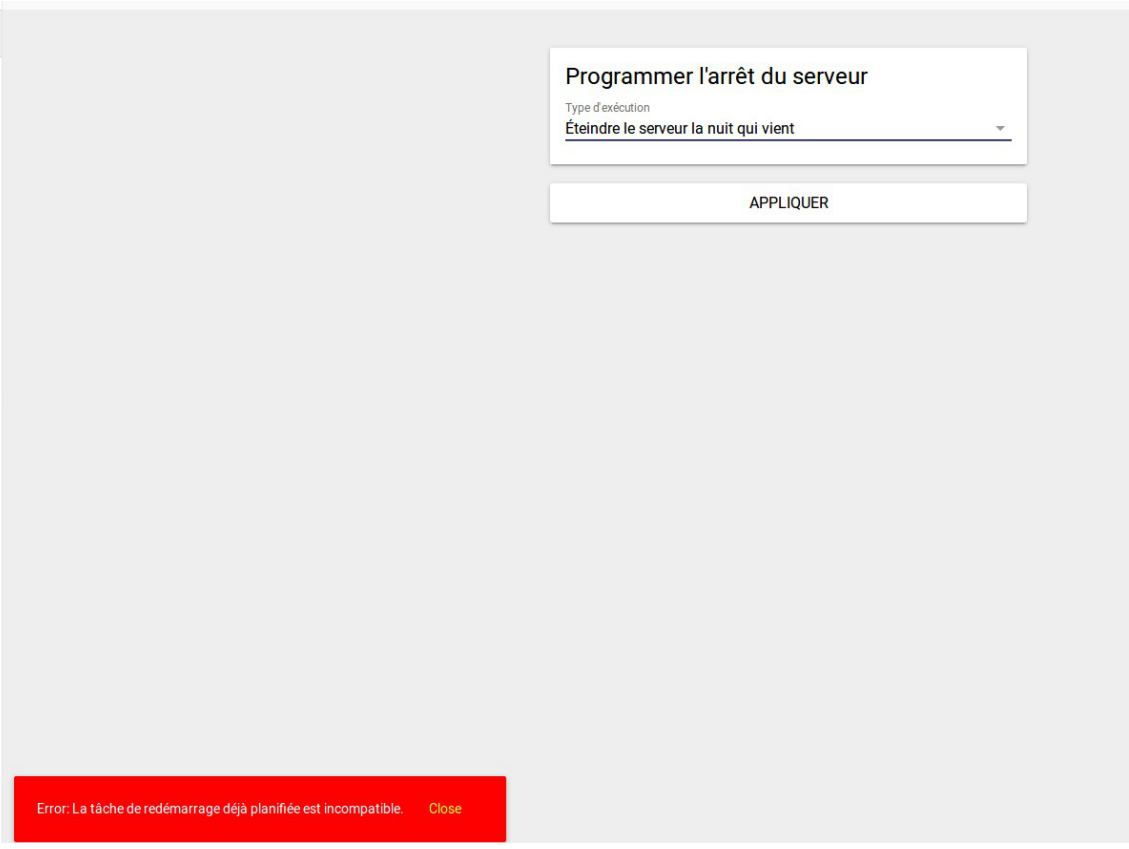


Exemple de tâches planifiées

Si un redémarrage du serveur a été programmé dans la nuit (`action système -> redémarrage du serveur`), l'action s'affiche dans la liste des tâches planifiées dans la nuit.



Si l'on souhaite programmer l'arrêt du serveur, l'EAD ne nous autorise pas à planifier cette action. En effet celle-ci est incompatible avec celle du redémarrage du serveur.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> Il faudrait supprimer l'action de redémarrage programmée dans la nuit, pour ensuite programmer à nouveau l'arrêt du serveur dans la nuit qui vient.
>
> L'action de redémarrage apparaît dans la liste des actions effectuées la nuit.



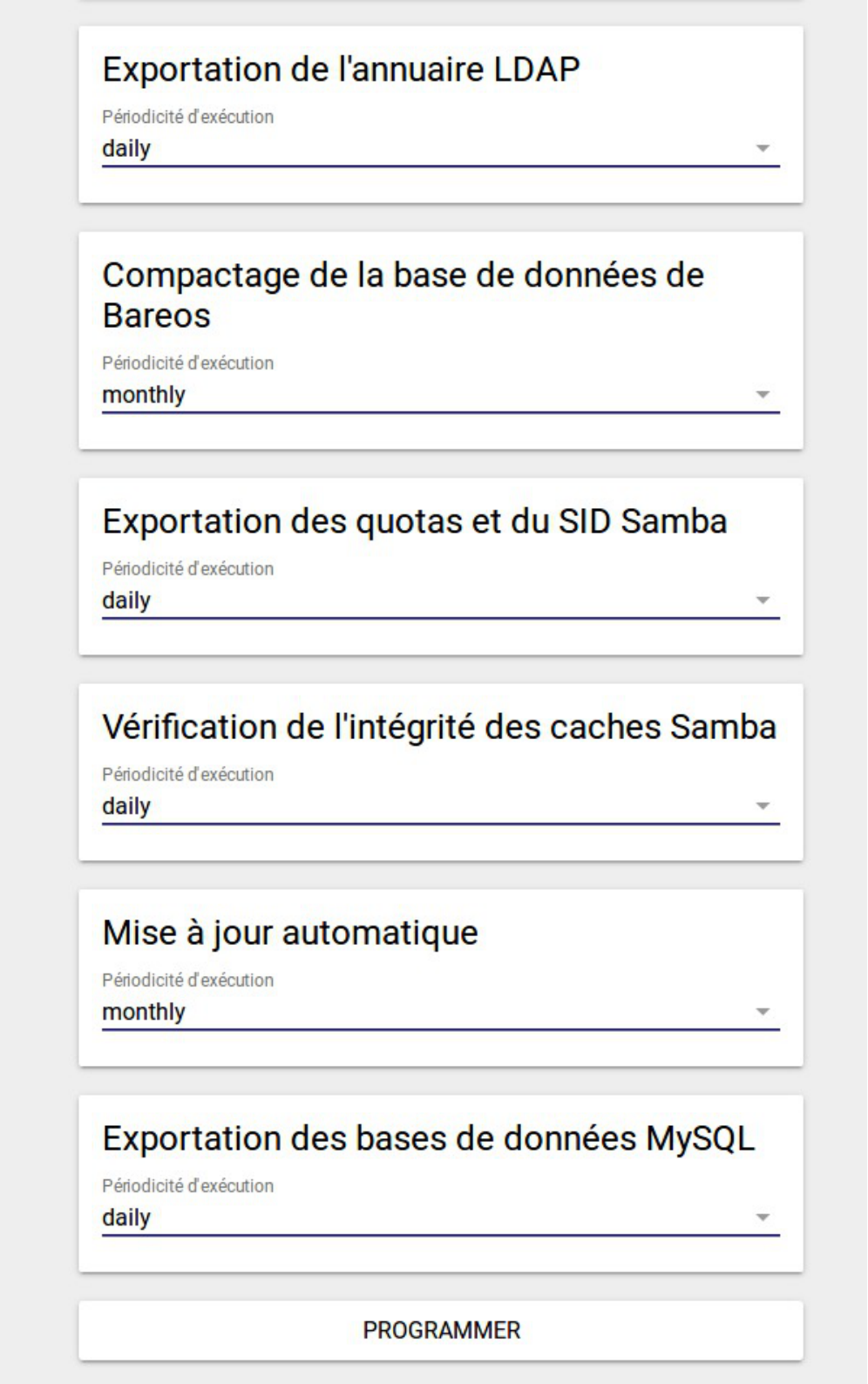
Liste des tâches planifiables

Il est possible de planifier :

- l'exportation de l'annuaire LDAP ;
- le compactage de la base de données de bareos ;
- l'exportation des quotas et du SID samba ;
- la vérification de l'intégrité des caches samba ;
- la mise à jour automatique ;
- l'exportation des bases de données MySQL.

Il est possible de planifier une ou plusieurs de ces tâches, elles sont prises en compte au moment du clic sur le bouton `PROGRAMMER` en bas de l'action :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



2.2. Fonctionnalités de l'EAD3 propres au module Amon

2.2.1. Actions liées au fonctionnement du pare-feu

Le paquet `era-actions`, pré-installé sur Amon et AmonEcole >= 2.8.1, apporte trois actions permettant d'activer/désactiver les règles optionnelles, de lister les règles de pare-feu activées et

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

d'ajouter/supprimer des règles volatiles.

2.2.1.a. Action gestion des règles de pare-feu optionnelles

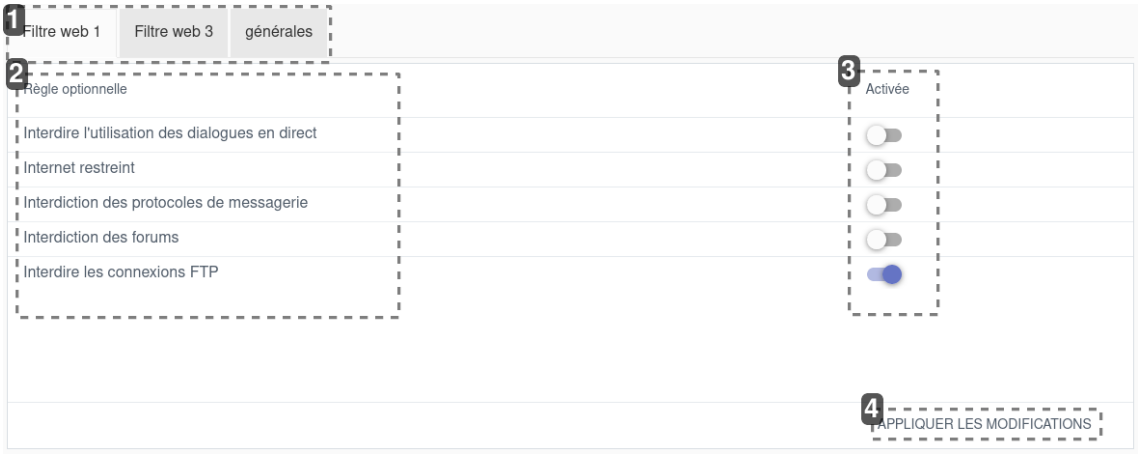
Les modèles de pare-feu ERA peuvent contenir des directives optionnelles EAD.

Une règle peut être :

- générale, si elle concerne uniquement l'interface externe ;
- spécifique à un filtrage, si elle concerne une interface interne de la zone, dans ce cas, elle apparaîtra dans le règles du filtre web auquel est rattaché l'interface source de la directive.

Pour modifier le statut d'une directive optionnelle :

1. activer ou désactiver une directive en cliquant sur le bouton correspondant de la seconde colonne,
2. valider les modifications en cliquant sur le bouton APPLIQUER LES MODIFICATIONS.



1



Onglets de zones

Les règles optionnelles sont attachées à une interface interne de la zone (onglets **Filtre web**) ou à l'interface externe (onglet **générales**).

La sélection s'effectue en cliquant sur l'onglet correspondant.

L'onglet **générales** est le seul à être obligatoirement présent. La présence des autres onglets dépend de la configuration des règles de filtrage du serveur.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2



Colonne des noms de règle

La première colonne du tableau affiche le nom de la règle.

3



Colonne du statut de la règle

La seconde colonne du tableau affiche et permet de changer le statut de la règle associée : désactivée (bouton blanc à gauche de la glissière) ou activée (bouton bleu à droite de la glissière).

4



Bouton de validation des changements

Les changements de statut effectués ne sont appliqués qu'après avoir cliqué sur le bouton `APPLIQUER LES MODIFICATIONS`.

Les directives optionnelles activées ou désactivées dans l'EAD sont enregistrées dans le fichier `/var/lib/eole/config/regles.csv` faisant le lien entre ERA et les directives optionnelles de l'EAD.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

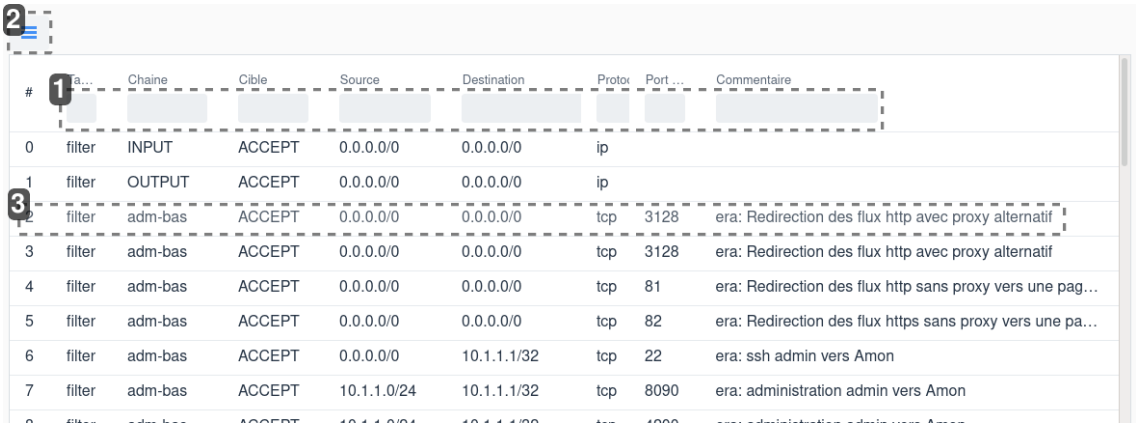
Pour les règles optionnelles, l'EAD prime sur ERA : elles sont pilotées par l'EAD. Une directive peut être marquée comment étant active par défaut dans ERA et ne pas être effectivement active car désactivée dans l'interface EAD.

2.2.1.b. Action liste des règles de pare-feu appliquées

Cette action permet de lister les règles iptables appliquées sur un serveur à un moment donné.

On retrouve les informations utiles suivantes :

- l'index ;
- le nom de la table (filter, NAT, …) ;
- la cible (ACCEPT, …) ;
- l'adresse source'
- l'adresse de destination ;
- le protocole (tcp, icmp, …) ;
- le port de destination ;
- le commentaire des directives ERA.



1

Champ de filtrage

Chaque colonne dispose d'un champ permettant de filtrer les entrées du tableau en fonction d'une chaîne de caractères.

2

Menu de sélection des colonnes affichées

Les colonnes peuvent être affichées ou masquées pour rendre l'affichage plus clair.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

3

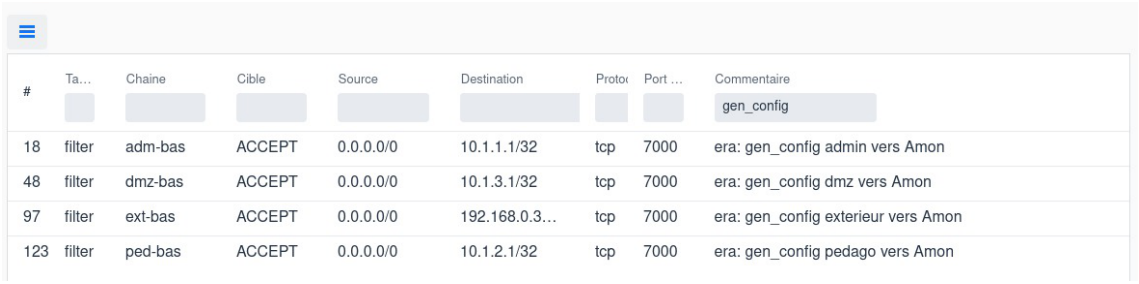
2 filter adm-bas ACCEPT 0.0.0.0/0 0.0.0.0/0 tcp 3128 era: Redirection des flux http avec proxy alternatif

Exemple d'une règle de pare-feu appliquée

Une règle avec toutes les informations disponibles fournit à l'administrateur :

- un numéro d'ordre d'application ;
- la table ;
- la chaîne ;
- la cible ;
- l'IP source ;
- l'IP de destination ;
- le protocole ;
- le port de destination ;
- le commentaire optionnel.

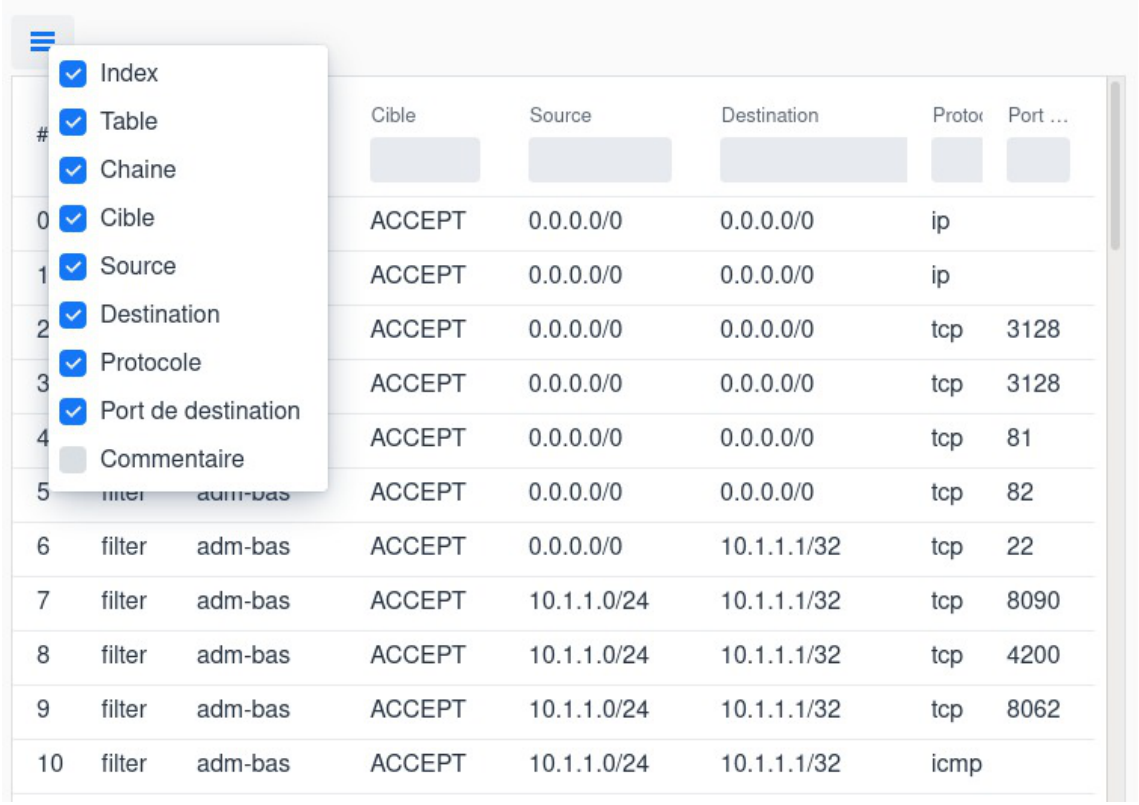
Pour chacune de ces informations, il est possible d'appliquer un filtre pour ne voir que les règles répondant à ce critère.



#	Ta…	Chaine	Cible	Source	Destination	Proto	Port …	Commentaire
								gen_config
18	filter	adm-bas	ACCEPT	0.0.0.0/0	10.1.1.1/32	tcp	7000	era: gen_config admin vers Amon
48	filter	dmz-bas	ACCEPT	0.0.0.0/0	10.1.3.1/32	tcp	7000	era: gen_config dmz vers Amon
97	filter	ext-bas	ACCEPT	0.0.0.0/0	192.168.0.3…	tcp	7000	era: gen_config exterieur vers Amon
123	filter	ped-bas	ACCEPT	0.0.0.0/0	10.1.2.1/32	tcp	7000	era: gen_config pedago vers Amon

Il est également possible de choisir quelles informations afficher pour adapter la quantité d'informations disponibles.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



#	Table	Chaine	Cible	Source	Destination	Proto	Port ...
0			ACCEPT	0.0.0.0/0	0.0.0.0/0	ip	
1			ACCEPT	0.0.0.0/0	0.0.0.0/0	ip	
2			ACCEPT	0.0.0.0/0	0.0.0.0/0	tcp	3128
3			ACCEPT	0.0.0.0/0	0.0.0.0/0	tcp	3128
4			ACCEPT	0.0.0.0/0	0.0.0.0/0	tcp	81
5	filter	adm-bas	ACCEPT	0.0.0.0/0	0.0.0.0/0	tcp	82
6	filter	adm-bas	ACCEPT	0.0.0.0/0	10.1.1.1/32	tcp	22
7	filter	adm-bas	ACCEPT	10.1.1.0/24	10.1.1.1/32	tcp	8090
8	filter	adm-bas	ACCEPT	10.1.1.0/24	10.1.1.1/32	tcp	4200
9	filter	adm-bas	ACCEPT	10.1.1.0/24	10.1.1.1/32	tcp	8062
10	filter	adm-bas	ACCEPT	10.1.1.0/24	10.1.1.1/32	icmp	

Enfin, chaque colonne est redimensionnable manuellement pour adapter sa largeur à la largeur de l'écran.



#	Table	Chaine	Cible	Source	Destination
0	filter	INPUT	ACCEPT	0.0.0.0/0	0.0.0.0/0
1	filter	FORWARD	ACCEPT	1.1.1.0/24	2.2.2.2/32
2	filter	FORWARD	ACCEPT	1.1.1.1/32	2.2.2.2/32
3	filter	OUTPUT	ACCEPT	0.0.0.0/0	0.0.0.0/0

2.2.1.c. Action gestion de règles de pare-feu volatiles

Cette action permet de gérer des règles de pare-feu volatiles.

Une règle volatile est une règle qui est ajoutée temporairement sur un serveur. Cette règle a vocation à être supprimée rapidement.

La règle est supprimée de deux manières :

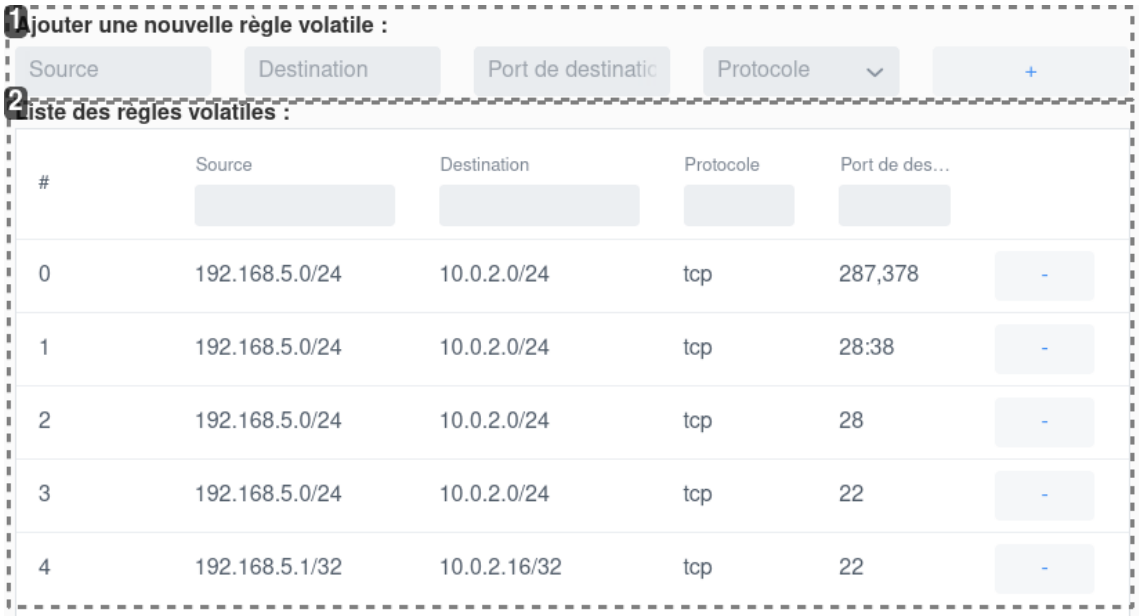
- au rechargement des règles de pare-feu (reconfigure, mise à jour, redémarrage du serveur, lors de la configuration de politique de filtrage du proxy, etc.) ;
- lorsque l'administrateur la supprime explicitement.

Une règle volatile est une règle qui comprend :

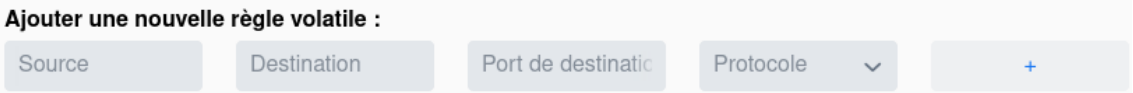
- une IP ou un réseau source ;
- une IP ou un réseau de destination ;
- un port de destination ;
- un protocole (TCP ou UDP).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

L'action est composée d'une zone prévue pour l'ajout de nouvelles règles et une zone de visualisation des règles déjà appliquées.



1

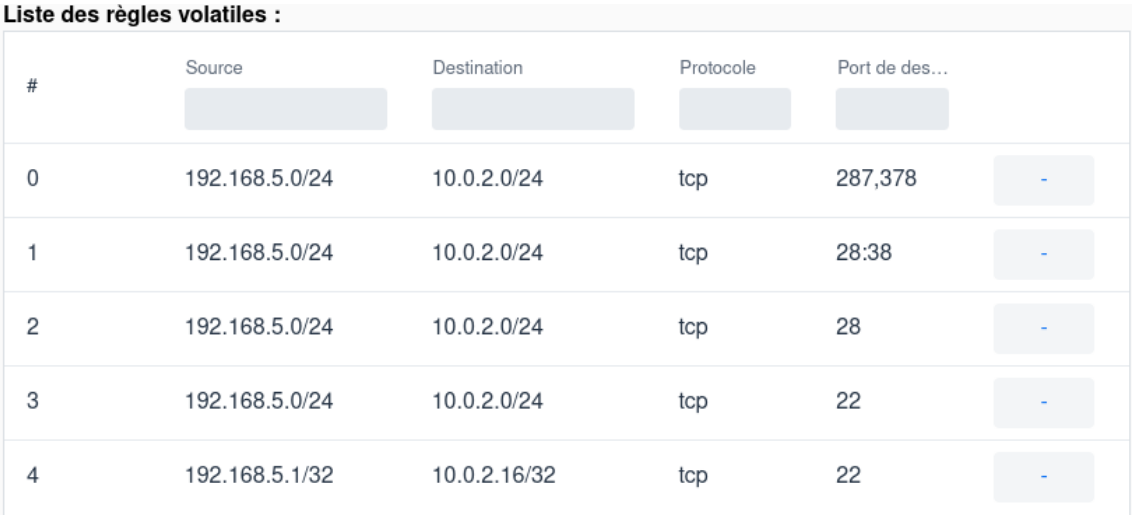


Formulaire d'ajout

Le formulaire d'ajout de règle volatile permet de renseigner :

- une IP source ;
- une IP de destination ;
- un port de destination ;
- le protocole.

2



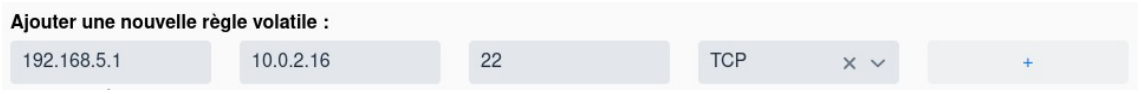
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Liste des règles actives

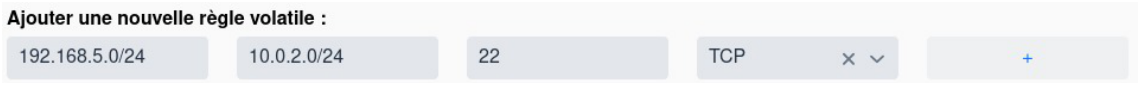
Chaque ligne du tableau affiche les informations pour une règle :

- l'IP source ;
- l'IP de destination ;
- le protocole ;
- les ports de destination ;
- le bouton permettant de supprimer cette règle.

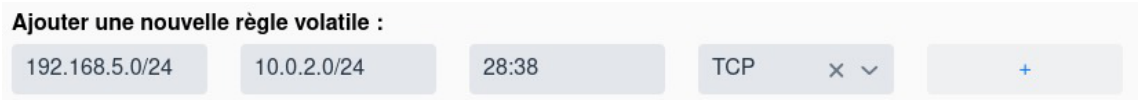
Il est possible de faire des règles avec des IP :



Plus largement, il est possible de définir des réseaux (au format CIDR) :



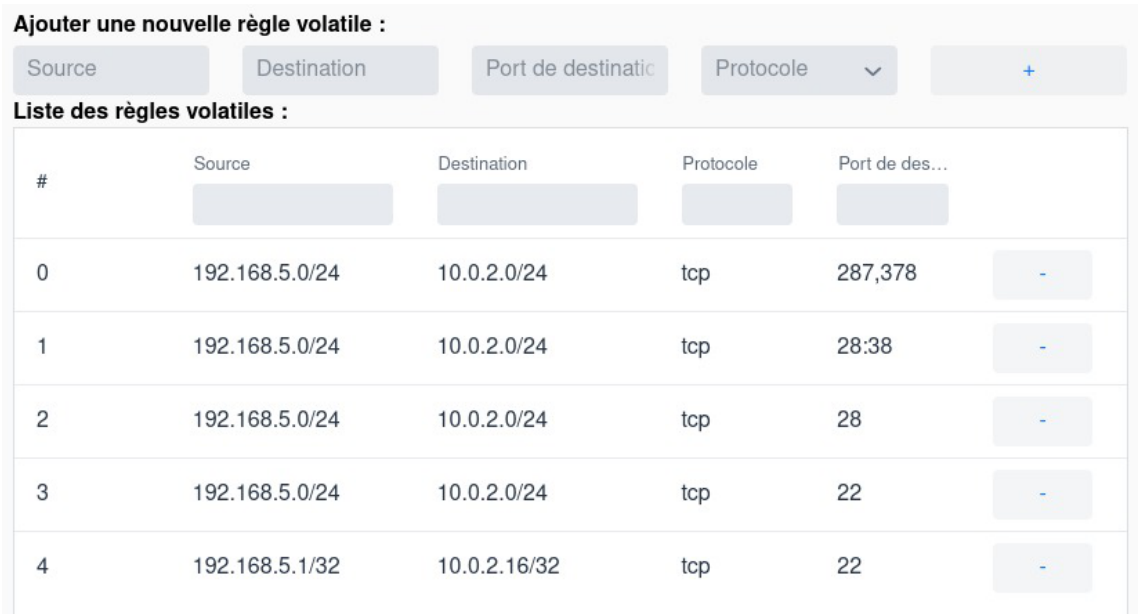
Le port peut également être une plage de ports (ici, tous les ports entre 28 et 38) :



Les ports multiples sont également pris en charge :



Lorsque la règle est appliquée, elle apparaît dans la liste des règles volatiles :



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Il est possible de filtrer les règles ou de redimensionner les colonnes comme pour l'action **règles de pare-feu appliquées**.

Pour supprimer la règle, il suffit de cliquer sur le bouton à la droite de la règle dans le tableau.

3. Fonctionnalités de l'EAD propres au module Amon

3.1. 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).

3.1.1. 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.715] 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`) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `/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

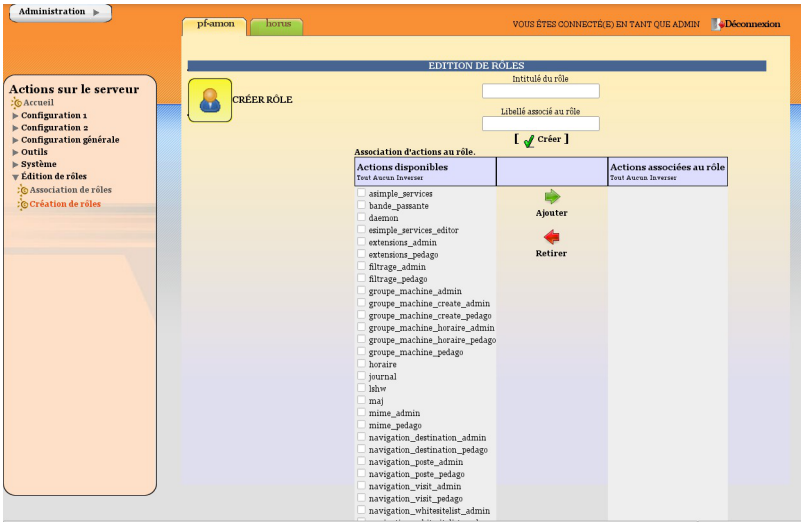
Pour créer un nouveau rôle cliquer sur :

- `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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.

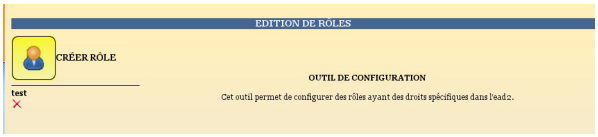
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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_admi**n (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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Modification/suppression d'un rôle

3.1.2. 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.715] 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

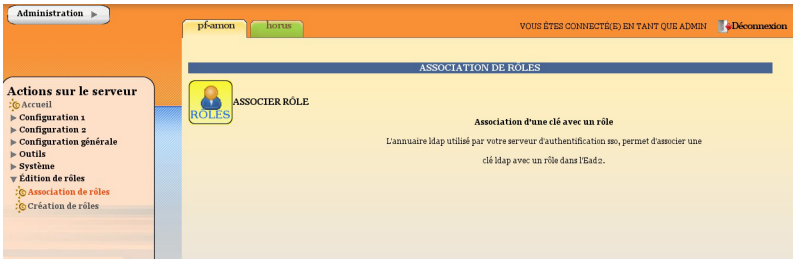
Quand un utilisateur se connecte sur l'EAD, en local ou en SSO, le système d'authentification renvoie des informations le concernant.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 :

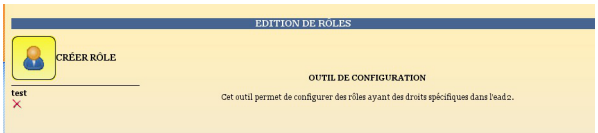
- l'élève fait partie de la classe ;
- la valeur de la clé LDAP typeadmin :
  - 0 → enseignant
  - 1 → administrateur
  - 2 → enseignant responsable de classe
  - 3 → personnel administratif
- le login de l'utilisateur ;
- le ou les groupes de l'utilisateur.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Modification/suppression d'un rôle

3.1.3. 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 :

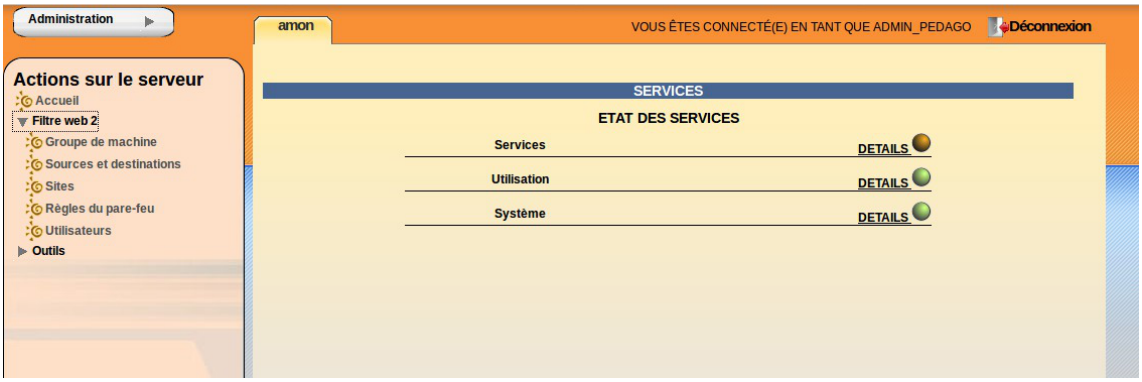
- activation/désactivation de règles de pare-feu (directives optionnelles) ;
- gestion d'exceptions de cache et d'authentification proxy ;
- gestion des options du filtrages web pour les différentes instances, politiques et groupes ;
- test de la bande passante du serveur ;
- consultation des statistiques 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

déléguer la gestion des options de filtrage pour le filtre n°2, traditionnellement associé à la zone pédagogique.



3.2. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles[p.709].

Une règle peut être :

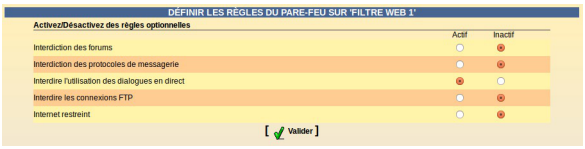
- générale, si elle concerne uniquement l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone, dans ce cas, elle apparaîtra dans les règles du filtre web auquel est rattaché l'interface source de la directive.

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

Les directives optionnelles activées/désactivées dans l'EAD sont enregistrées dans le fichier : `/var/lib/eole/config/regles.csv`

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.538]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

3.3. 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 :

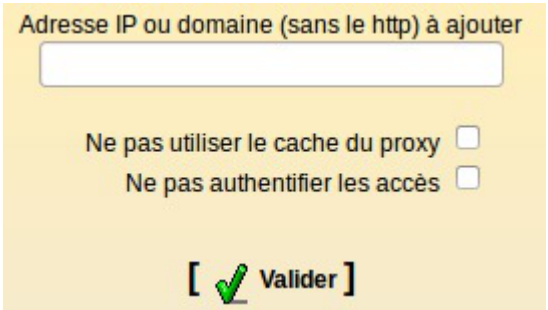
- ne pas utiliser de cache ou d'authentification pour certains sites (destination) ;
- ne pas utiliser de cache ou d'authentification pour certaines machines locales (source).

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les exceptions "destinations" sont écrites dans :

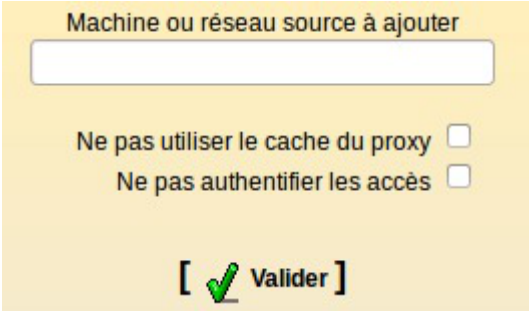
- /etc/squid/domaines_nocache_user
- /var/lib/eole/domaines_noauth_user : référence pour la génération des fichiers :
  - /etc/squid/domaines_noauth_user
  - /etc/guardian/common/domaines_noauth_user

Sur le module *AmonEcole*, ces fichiers sont dans le conteneur *reseau*.

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.



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

Les exceptions "sources" sont écrites dans :

- /etc/squid/src_nocache_user
- /etc/squid/src_noauth_user

Sur le module *AmonEcole*, ces fichiers sont dans le conteneur *reseau*.

Personnalisations académiques

À partir d'EOLE 2.8, les exceptions d'authentification pour les destinations doivent être déclarées à la fois dans Squid[p.731] et dans e2guardian[p.710].

Le format des adresses à fournir à e2guardian est différent de celui utilisé pour Squid (pas de "." devant un nom de domaine "global", interdiction de déclarer un sous-domaine d'un

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> domaine déjà présent).

Des listes de sites et d'adresses académiques peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

- `/etc/squid/domaines_nocache_acad` : liste de destinations pour lesquelles ne pas utiliser le cache ;
- `/etc/squid/src_noauth_acad` : liste de sources à ne pas authentifier ;
- `/etc/squid/src_nocache_acad` : liste de sources pour lesquelles ne pas utiliser le cache ;
- `/etc/squid/domaines_nopeerproxy` : liste de destinations pour lesquelles on n'utilise pas le proxy père ;

Listes pour e2guardian :

- `/etc/guardian/common/domaines_noauth` ; Le fichier domaines_noauth contient les exceptions provenant de GenConfig et d'un template Creole ; Dans gen_config => Exceptions proxy => Liste des domaines de destination à ne pas authentifier (variables Creole :proxy_noauth)
- `/etc/guardian/common/domaines_noauth_acad` ; Le fichier domaines_noauth_acad est par convention modifié/envoyé par Zéphir.



> L'utilisation des fichiers `/etc/squid/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.348]

3.4. 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 : `Filtre web 1` et `Filtre web 2` ;
- de manière plus fine, par politique de filtrage ;
- de façon prioritaire sur les utilisateur puis sur les machines si l'authentification est désactivée sinon de façon prioritaires sur les machines puis sur les utilisateurs.

En fonction de la configuration du filtrage effectuée dans l'interface de configuration du module deux sections nommée filtre web peuvent être disponibles dans l'EAD : Filtre web 1 et Filtre web 2.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



La section Filtre web 3 est visible si une deuxième instance de Squid a été activée dans l'interface de configuration du module.

Certaines fonctionnalités n'ont pas d'intérêt dans le cadre du `Filtre web 3` puisqu'elles sont est déjà couvertes par les 2 autres filtres qui se partagent la gestion de toutes les interfaces.

3.4.1. Groupe de machine : 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 :

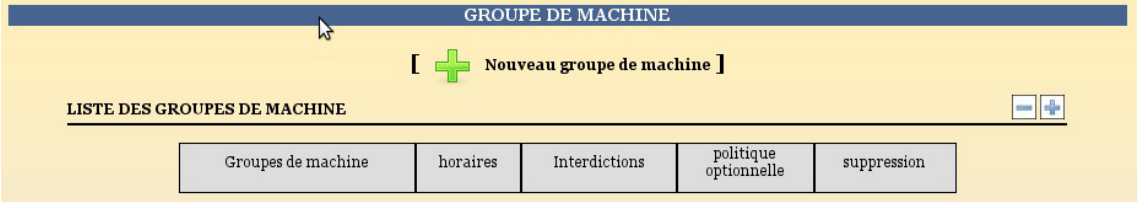
- de lui interdire l'accès au réseau ;
- de lui interdire la navigation web seulement ;
- de lui autoriser la navigation web selon des horaires ;
- de lui associer une politique de filtrage web spécifique

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

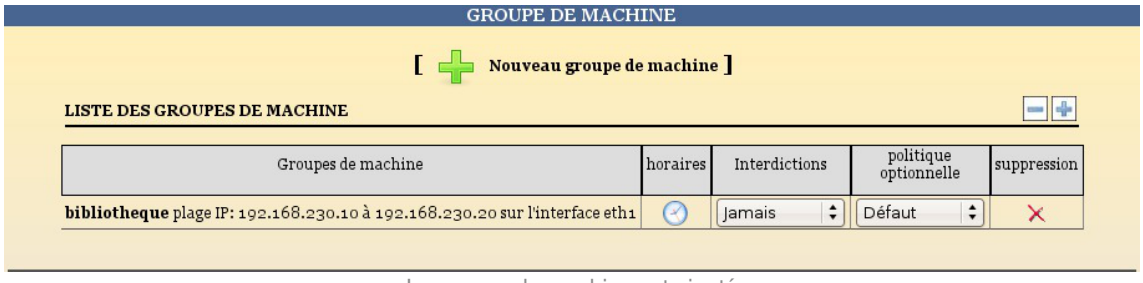


Formulaire de création

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.



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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` : permet de ne jamais interdire l'accès au web ;
- `Le web tout le temps` : permet d'interdire la navigation web tout le temps.

  L'accès au proxy, sur le port 3128 et selon la configuration, sur les ports du second proxy (3129 par défaut) est bloqué pour les plages d'IP stockées dans des ipset.

  À partir de la version 2.6.1 d'EOLE, la navigation sans proxy ne subit pas de restrictions particulières, elle s'effectue donc avec les règles déjà en place sur le module (par défaut : affichage d'une page d'erreur indiquant que le proxy n'est pas configuré).
- `Le web selon des horaires` : permet d'interdire la navigation web selon des horaires sont à définir au préalable (utilise les mêmes règles que `Le web tout le temps` mais avec des plages horaires) ;
- `Toute activité réseau` : permet d'interdire toute activité réseau (toutes les requêtes issues des plages d'adresse IP stockées dans des ipset sont rejetées par des règles iptables).

Le filtrage et les restrictions basées sur des plages horaires sont appliquées par l'utilisation du module *time* du logiciel iptables.

iptables interprète les dates en UTC[p.734], il y a donc un décalage normal entre ce qui est saisi dans l'interface et les informations renvoyées par la commande `iptables-save`.

Interdire le groupe de navigation web

Dans la colonne `Interdictions`, choisir `Le web tout le temps`.

Si vous désirez faire une interdiction de navigation selon des horaires, il faut :

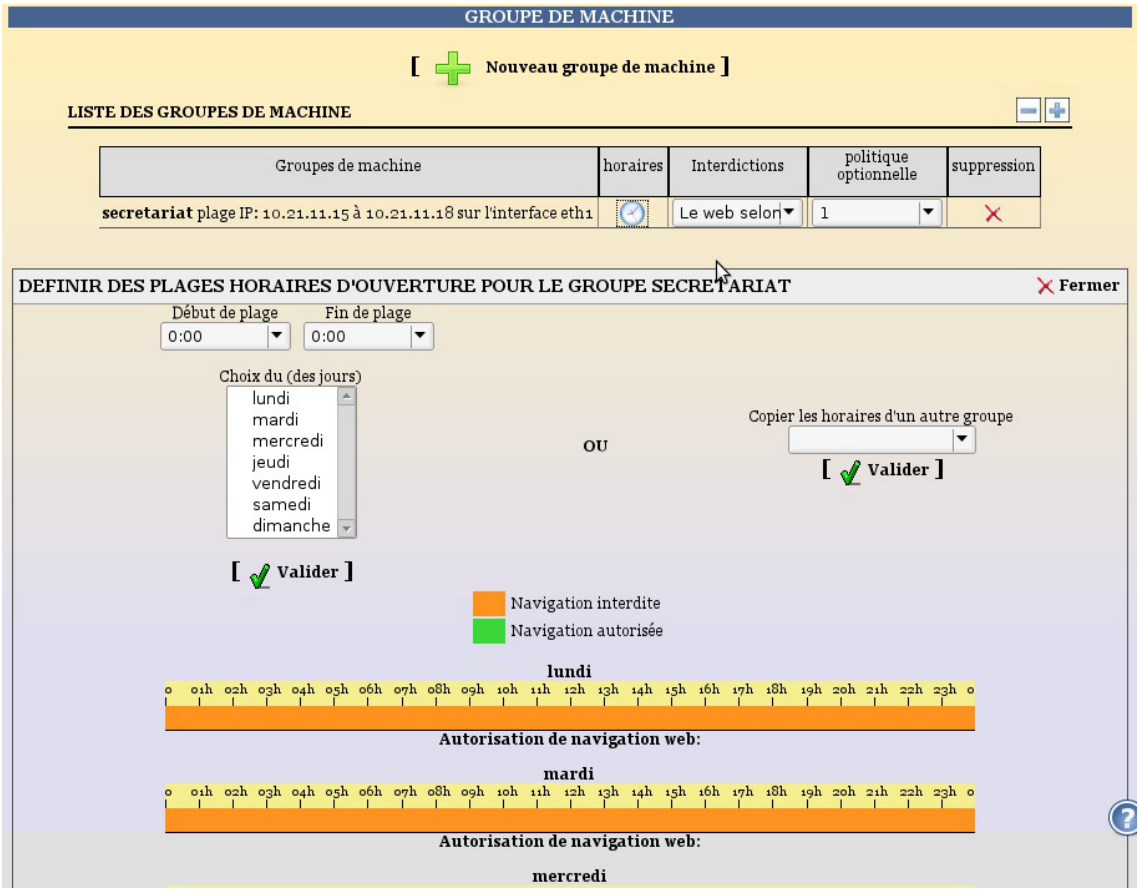
- configurer des horaires ;
- appliquer l'interdiction.

Configuration des horaires

Dans la colonne `Interdictions`, choisir `Le web selon horaires`.

Cliquer sur l'horloge, la gestion des horaires apparaît.

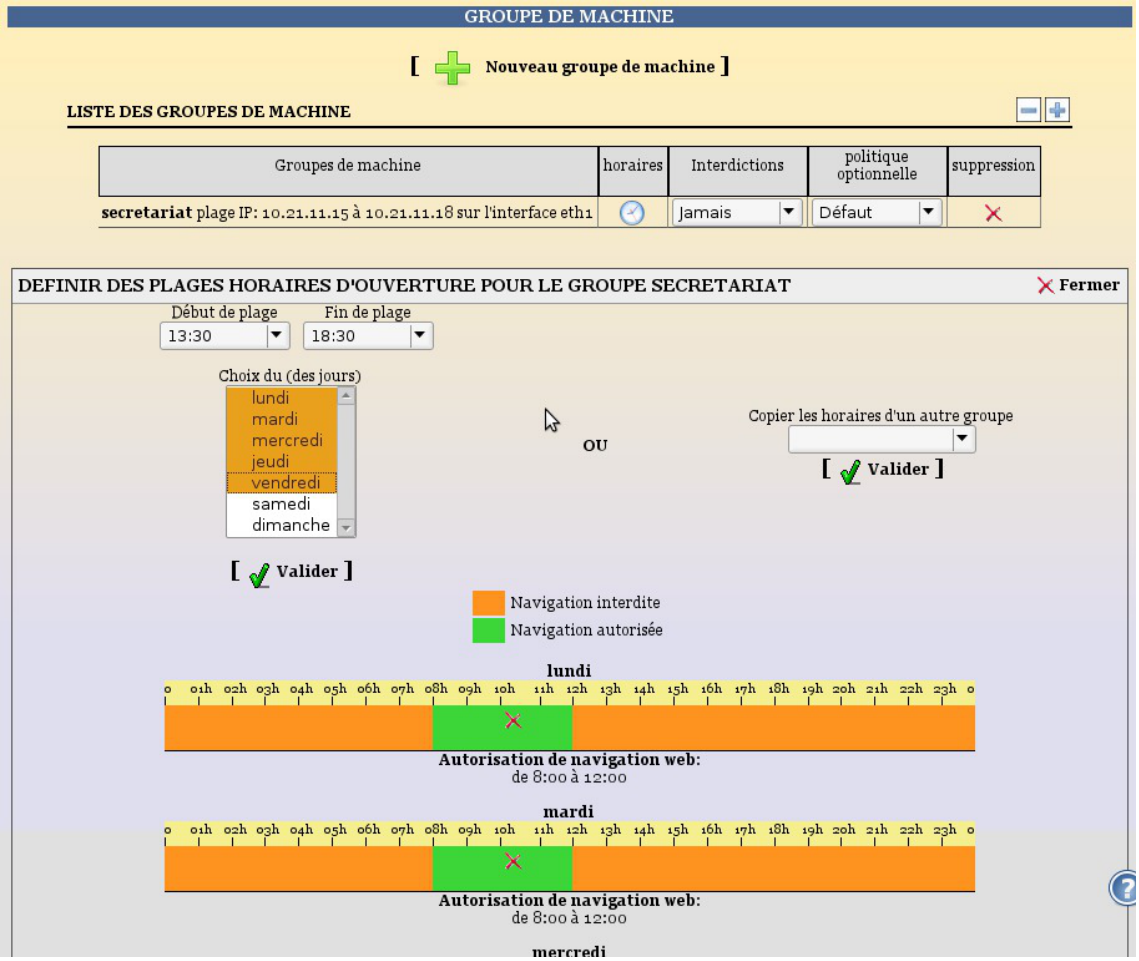
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Gestionnaire d'horaires pour les groupes de machine

- choisir la plage horaire d'autorisation ;
- choisir les jours d'applications ;
- valider.

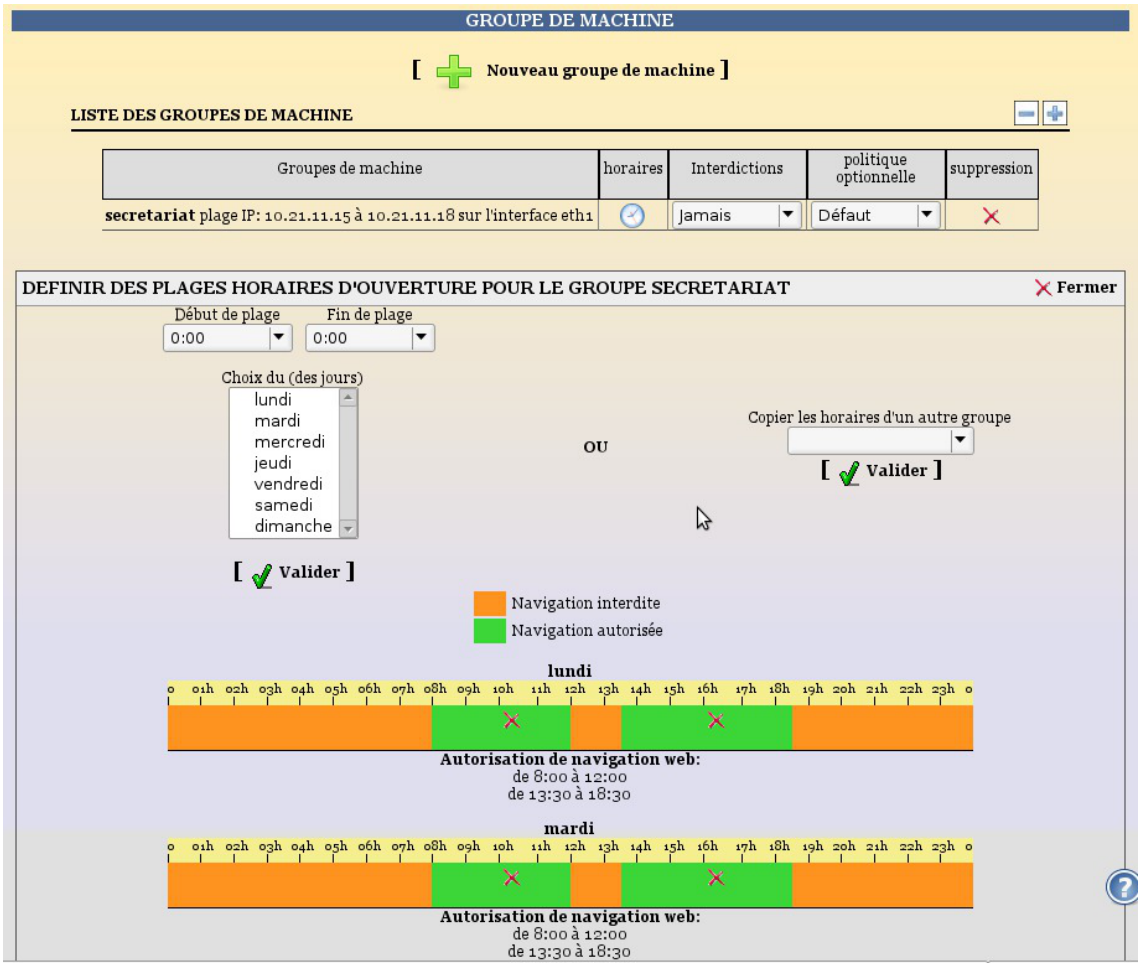
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Remplir le formulaire

Les plages horaires définies s'affichent (la croix permet de supprimer la plage).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 ou plusieurs politiques de filtrage à un groupe de machine. Elles proviennent du logiciel de filtrage e2guardian et sont associées aux plages d'adresses IP grâce à la fonctionnalité *ipgroups* du plugin d'authentification *ip* intégré à ce logiciel.

Pour associer une politique de filtrage, choisir la politique dans la colonne `politique optionnelle`.

Certaines politiques de filtrage sont fixes :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- modérateur ;
- interdits ;
- mode liste blanche.

D'autres sont configurables :

- Défaut ;
- 1 ;
- 2 ;
- 3 ;
- 4.

Le mode modérateur n'est pas compatible avec l'authentification NTLM : #19351 [https://dev-eole.ac-dijon.fr/issues/19351] .

Correspondance entre numéro de politique et mode de fonctionnement

Pour chaque instance de e2guardian, 8 politiques sont pré-définies par les fichiers `guardianfX.conf` :

- politique n°1 : politique par défaut (`politiquedefaut`) ;
- politique n°2 : utilisateur modérateur (`groupmoderateurs`) ;
- politique n°3 : utilisateur interdit (`groupinterdits`) ;
- politique n°4 : utilisateur en mode liste blanche (`grouplisteblanche`) ;
- politique n°5 : politique de filtrage personnalisée n°1 (`politique1`) ;
- politique n°6 : politique de filtrage personnalisée n°2 (`politique2`) ;
- politique n°7 : politique de filtrage personnalisée n°3 (`politique3`) ;
- politique n°8 : politique de filtrage personnalisée n°4 (`politique4`).

Supprimer un groupe de machine

Pour supprimer un groupe de machine, cliquez sur la croix en face de votre groupe de machine.

Ajouter des ipset personnalisés

À partir d'EOLE 2.7.0, la création d'un groupe de machine ou la génération des règles du bastion[p.704] supprime uniquement les ipset gérés par le module (ie : ceux qui sont préfixés par les mots clés : `groupe-` et `bastion-`).

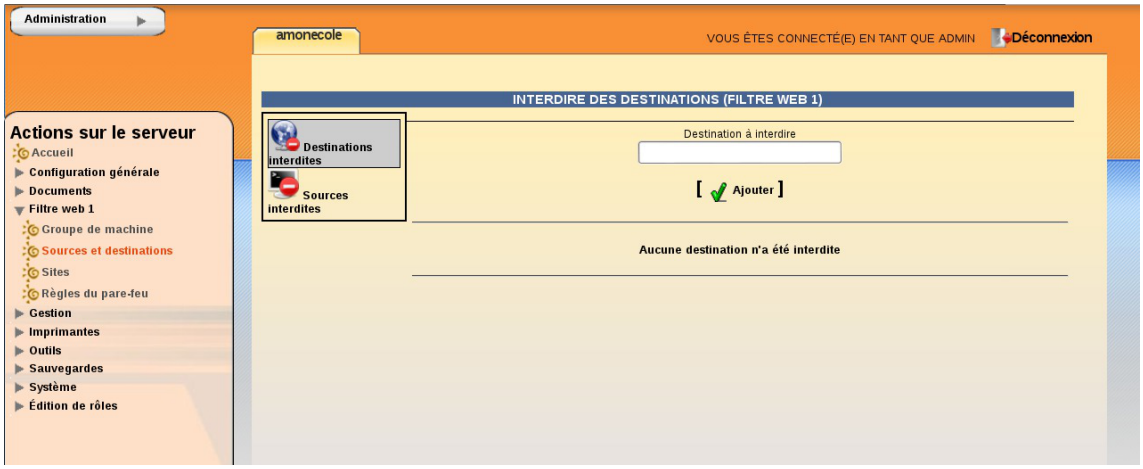
3.4.2. Sources et destinations : Interdire l'accès à un sous-réseau depuis une interface

Dans l'EAD il est possible d'interdire l'accès à un sous-réseau depuis une interface.

Cette fonctionnalité se base sur des règles iptables standard et sur l'utilisation du module *time* d'iptables

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

dans le cas des destinations interdites par plage horaire.



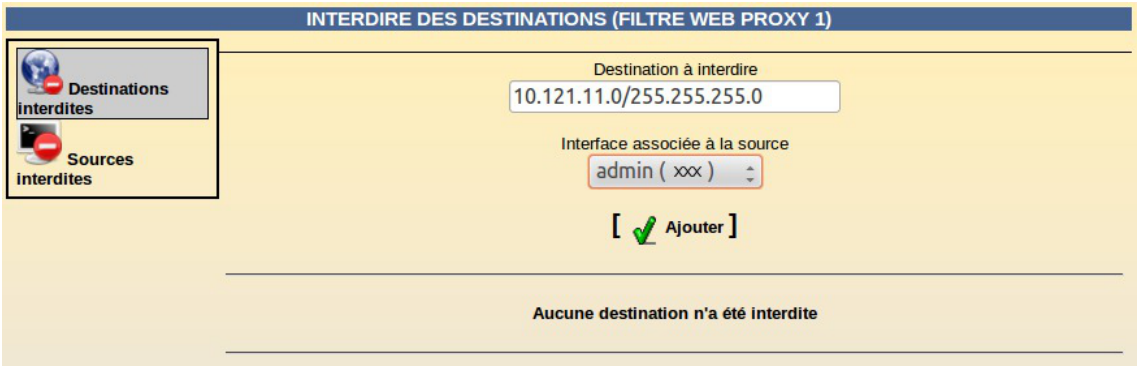
Vue d'ensemble pour l'ajout d'une destination à interdire

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).

Interdire l'accès au sous-réseau 10.121.11.0/255.255.255.0 depuis l'interface admin (xxx)



Ajout d'une destination à interdire

Soit l'interface X sur la zone de filtre web X.

- Saisir `10.121.11.0/255.255.255.0` dans `Destinations à interdire` ;
- Choisir `admin (xxx)` 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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

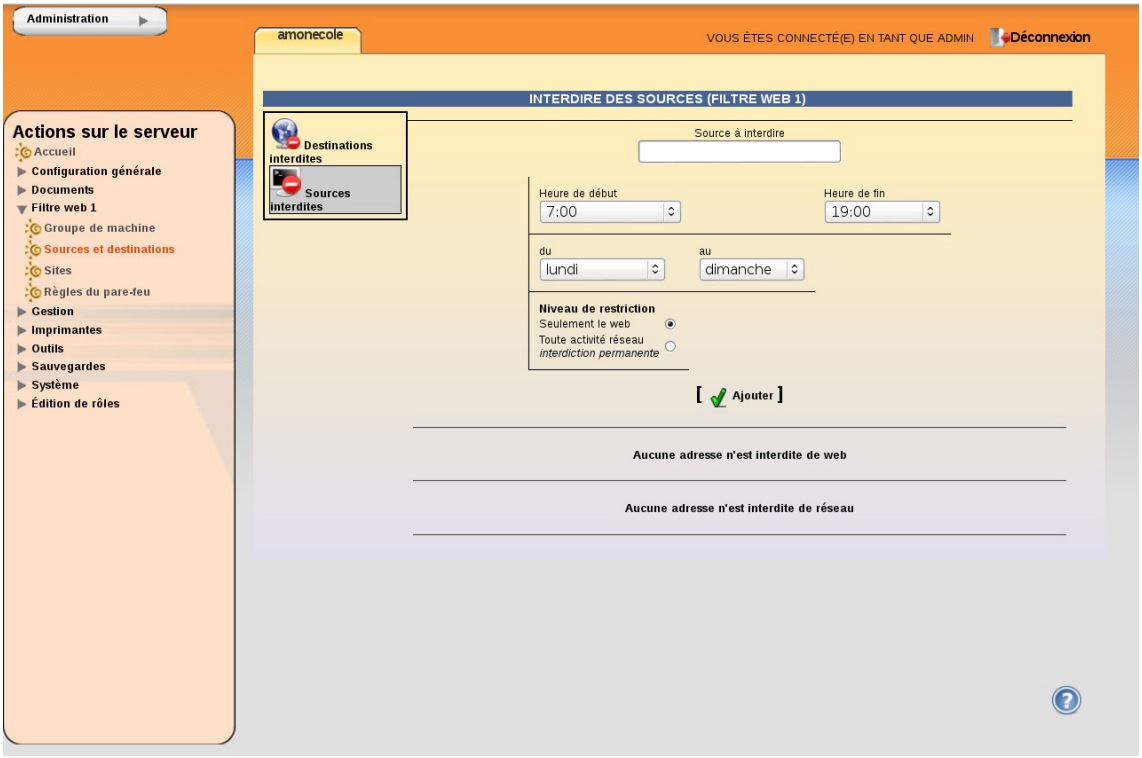
Nommage des filtres dans la configuration du filtrage web

Onglet Filtrage web : Configuration du filtrage web [p.285]

3.4.3. Sources et destinations : 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 .

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

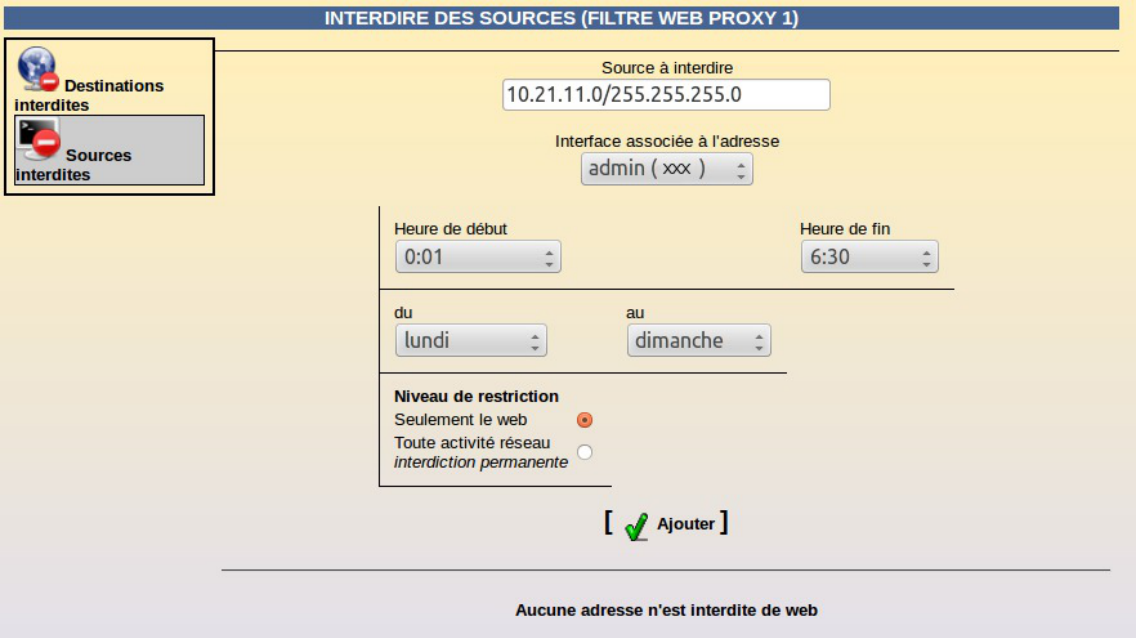
Les paramètres à saisir sont :

- 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.

> Avec le niveau de restriction ◉ Seulement le web, l'accès au proxy, sur le port 3128 et selon la configuration, sur les ports du second proxy (3129 par défaut).
>
> À partir de la version 2.6.1 d'EOLE, la navigation sans proxy ne subit pas de restrictions particulières, elle s'effectue donc avec les règles déjà en place sur le module (par défaut : affichage d'une page d'erreur indiquant que le proxy n'est pas configuré).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Interdire l'accès web depuis le sous-réseau 10.21.11.0/255.255.255.0 provenant de l'interface 1 tous les jours entre minuit et 6 heures du matin



Ajout d'une source à interdire

Soit l'interface 1 sur la zone de filtre web 1 :

- Saisir `10.121.11.0/255.255.255.0` dans `Source à interdire` ;
- Choisir `admin (xxx)` 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.

Le filtrage et les restrictions basées sur des plages horaires sont appliquées par l'utilisation du module *time* du logiciel iptables.

iptables interprète les dates en UTC[p.734], il y a donc un décalage normal entre ce qui est saisi dans l'interface et les informations renvoyées par la commande `iptables-save`.

Annuler une interdiction

Dans le menu de l'EAD, choisir l'entrée portant le nom du filtre choisi dans l'interface de configuration du module, par défaut `Filtre web 1`. Puis sélectionner `Sources et destinations` et enfin `Sources interdites`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

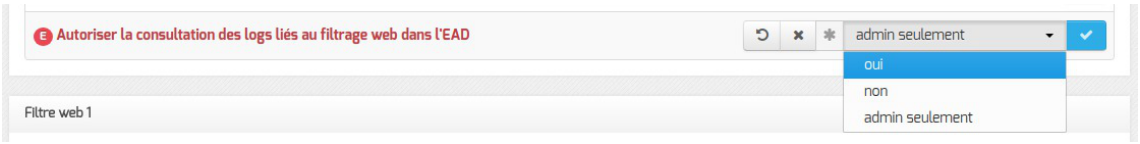
Onglet Filtrage web : Configuration du filtrage web [p.285]

3.4.4. Visites des sites : Observatoire des navigations

L'observatoire des navigations est un outil de consultation des logs de l'outil de filtrage e2guardian[p.710].

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 :

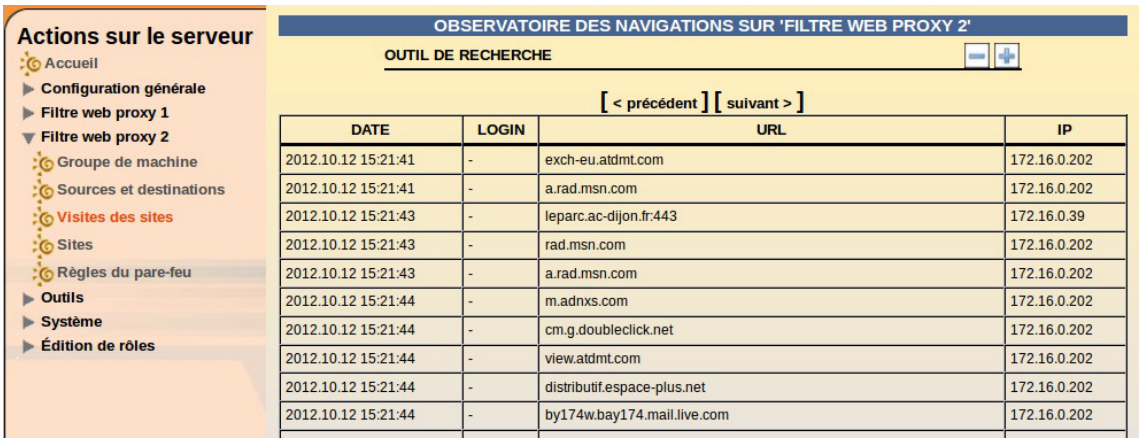
- `oui` : accès autorisé pour les utilisateurs EAD possédant les actions `navigation_visit_admin` et/ou `navigation_visit_pedago` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `non` : accès interdit pour tout le monde, personne ne voit le lien `Visites des sites` (configuration par défaut) ;
- `admin seulement` : accès autorisé uniquement pour le rôle `admin`.

Consultation

La consultation des visites de sites se fait au travers de l'EAD, menu : `Filtre web X/visites des sites`.



> Les noms des menus (ici : `Filtre web proxy 2`) sont modifiables dans l'interface de configuration du module (variables `dansguardian_ead_filtre1` et `dansguardian_ead_filtre2`).

3.4.5. Sites : Bases de filtres optionnels

Les bases de filtres proposées sur le module Amon sont des copies de celles gérées par l'université de Toulouse 1 Capitole : http://cri.univ-tlse1.fr/blacklists [http://cri.univ-tlse1.fr/blacklists/].



L'université de Toulouse 1 Capitole diffuse depuis de nombreuses années une liste noire d'URLs, gérée par Fabrice Prigent afin de permettre un meilleur contrôle de l'utilisation d'Internet.

Les bases, publiées sous licence d'utilisation Creative Commons by-sa 4.0 [http://creativecommons.org/licenses/by-sa/4.0/deed.fr], sont largement utilisées par les écoles et sont également intégrées dans un grand nombre d'outils libres ou commerciaux, en complément d'autres listes.

Les bases sont mises à jour 2 à 3 fois par semaine en fonction des disponibilités du mainteneur, elles peuvent être enrichies grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Ces bases de filtres proposent des catégories avec des listes de domaines et d'URL triés par catégories.

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- par filtre web ;
- par politique de filtrage.

La mise à jour des bases de filtres est lancée automatiquement toutes les nuits

Un rapport de mise à jour est disponible sur la page d'accueil de l'EAD.

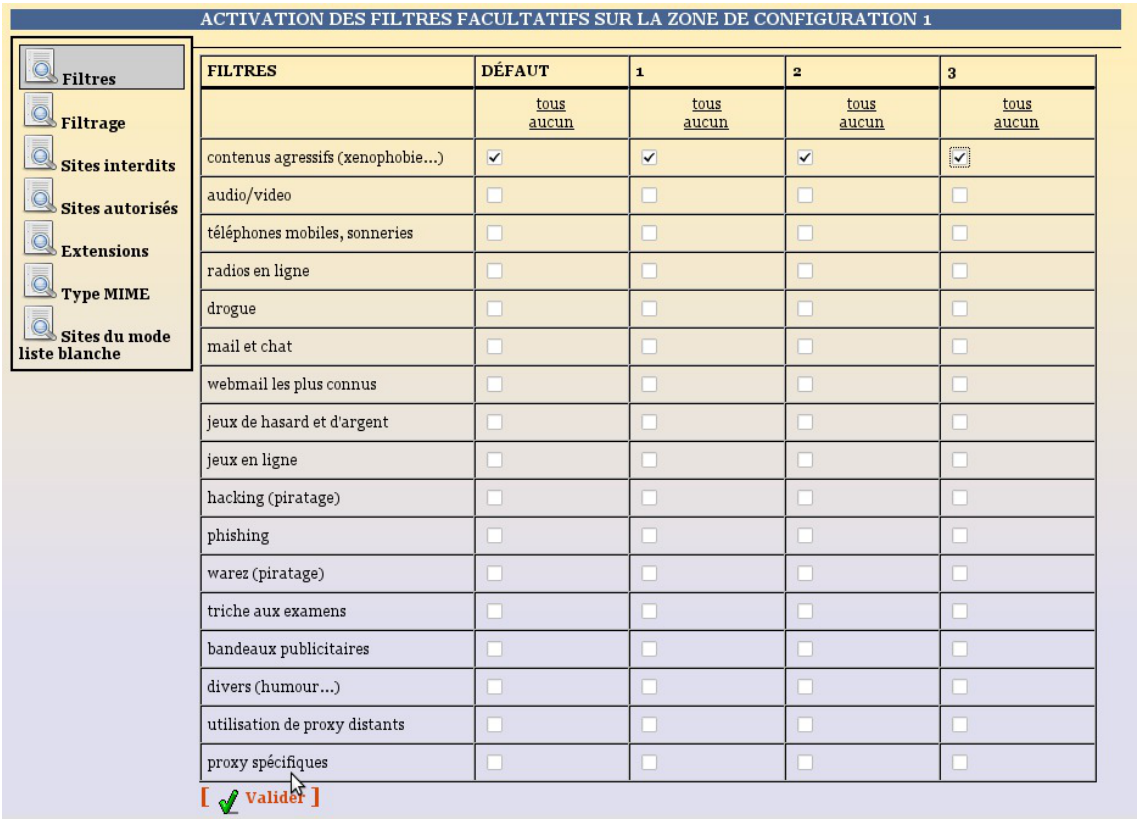


Rapport de mise à jour des bases de filtres

Pour activer la catégorie "agressif" sur toute la zone de configuration 1

Dans Filtre 1 / Sites / Filtres :

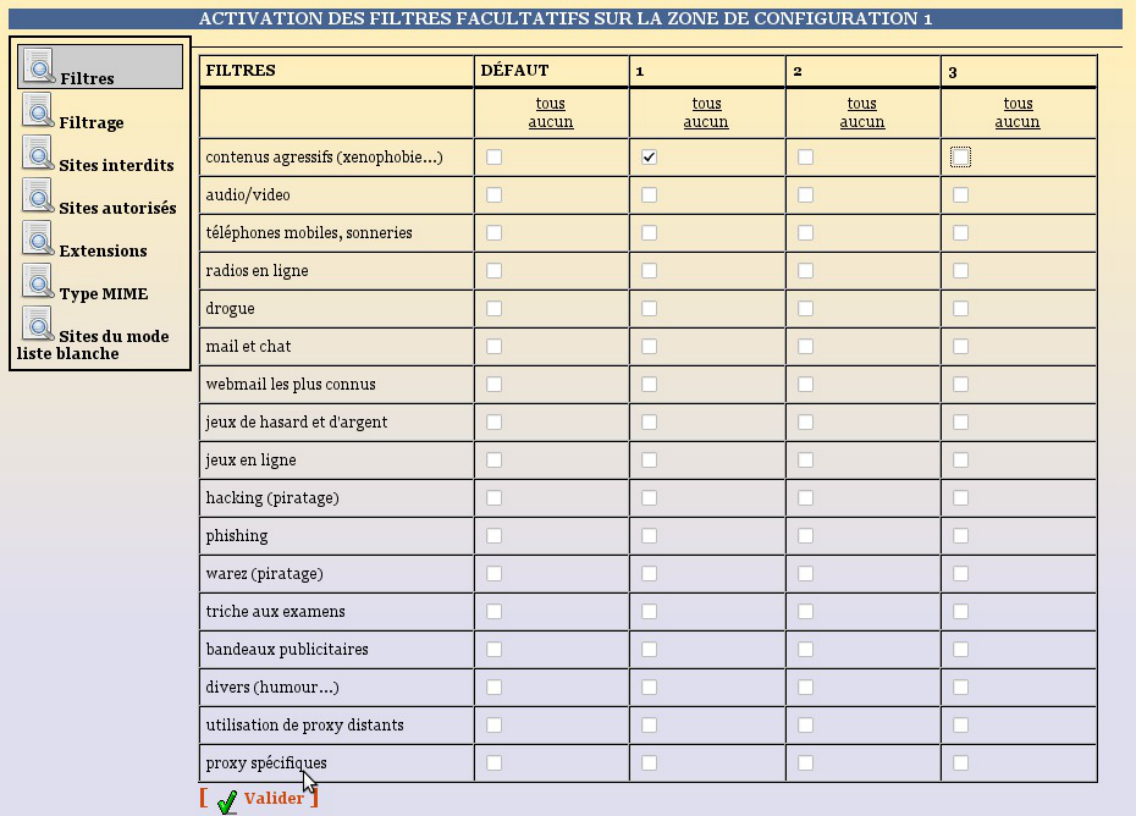
- cocher les quatre cases (pour les quatre politiques de filtrage de la zone 1) ;
- valider.



Activation de filtres optionnels

Pour activer une catégorie seulement pour une politique de filtrage[p.727], seule la case correspondant à la politique doit être cochée.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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/sbin/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*** .

3.4.6. Sites : Filtrage syntaxique

Configuration du filtrage syntaxique

Le module Amon filtre dynamiquement les pages web grâce au filtrage syntaxique[p.712].

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 :

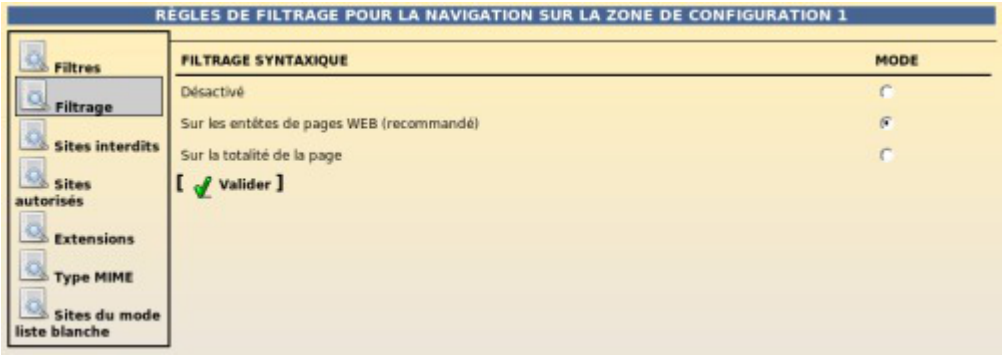
- sur les balises méta[p.704] (par défaut) ;
- sur la page entière ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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>`

Limite de pondération

Le réglage par défaut de la limite de pondération peut être modifié dans l'interface de configuration du module dans l'onglet `Filtrage web`.

Mode safe search dans les moteurs de recherche

En complément, des redirections DNS sont mises en place afin que le mode *safe search*[p.729] des principaux moteurs de recherche et sites d'hébergement de vidéos soit activé automatiquement (Qwant, Youtube, Bing, Google…).

Des variables de configuration, disponibles dans l'onglet `Mode restreint`, permettent d'activer ou non le mode restreint pour certaines applications.

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`.

3.4.7. Sites : Interdire et autoriser des domaines

Interdire des domaines et des URL

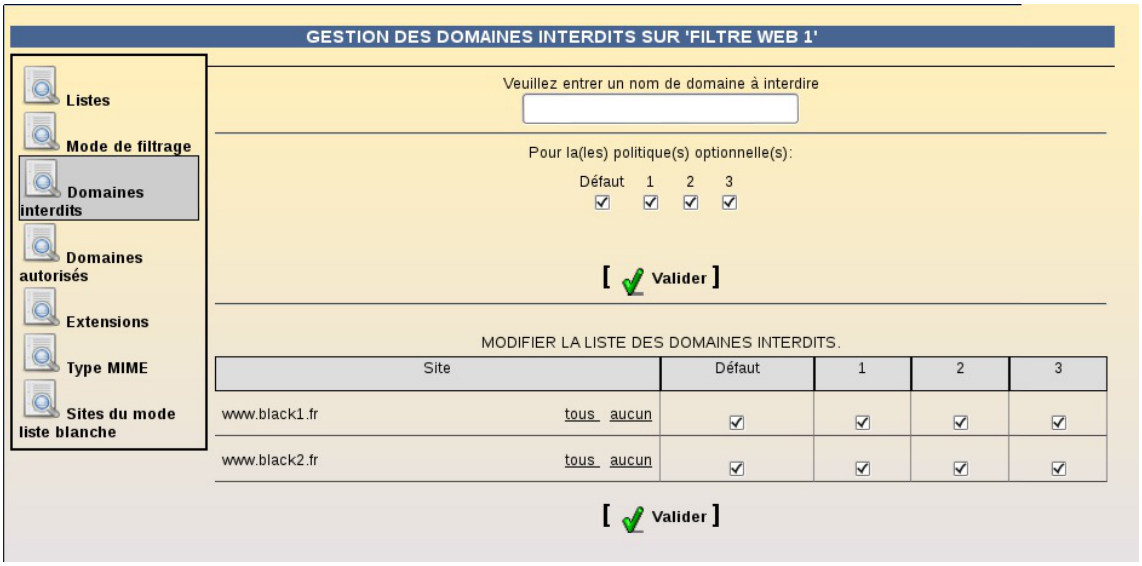
Il est possible de compléter la liste de sites interdits (liste noire[p.718]) en ajoutant des domaines ou des URL sur la liste personnalisée de domaines interdits.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

Ajout de sites interdits personnalisés par les académies ou les collectivités

Des listes de domaines et d'URL peuvent être gérées indépendamment de l'EAD par l'intermédiaire des fichiers suivants :

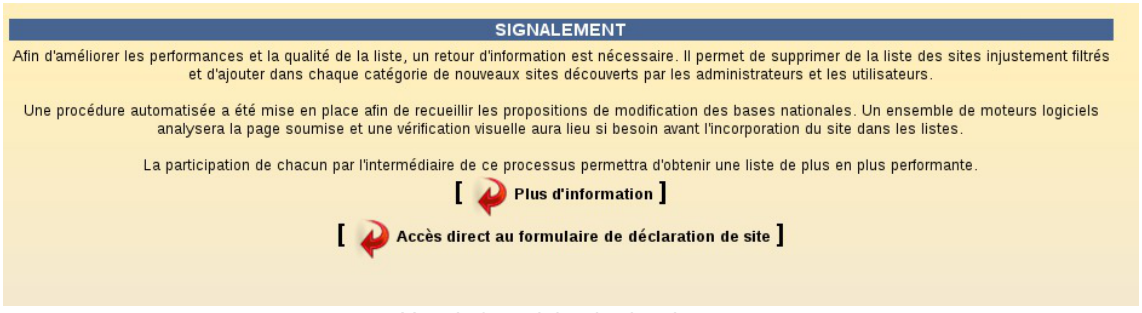
- `/var/lib/blacklists/dansguardian<num_instance>/common/domains_acad`
- `/var/lib/blacklists/dansguardian<num_instance>/common/urls_acad`

Sur un module AmonEcole, ces fichiers sont dans le conteneur `internet`.

Signaler de sites

Il est possible de signaler des domaines à interdire qui amélioreront les performances et la qualité des bases nationales de domaines interdits.

Pour cela, aller dans `Outils` / `Signalements`.



Vue du formulaire de signalement

Une procédure automatisée a été mise en place afin de recueillir les propositions de domaine à interdire dans les bases nationales.

Un ensemble de moteurs logiciels analysera l'URL soumise et une vérification visuelle aura lieu si besoin avant l'incorporation du domaine dans les listes de domaines interdits.

La participation de chacun à ce processus permet d'améliorer les bases nationales et leur performance et ce afin que chacun puisse en bénéficier.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Il est également possible de faire une signalement directement auprès de l'université de Toulouse 1 Capitole grâce à une formulaire en anglais : http://dsi.ut-capitole.fr/cgi-bin/squidguard_modify.cgi.

Autoriser des domaines et des URL

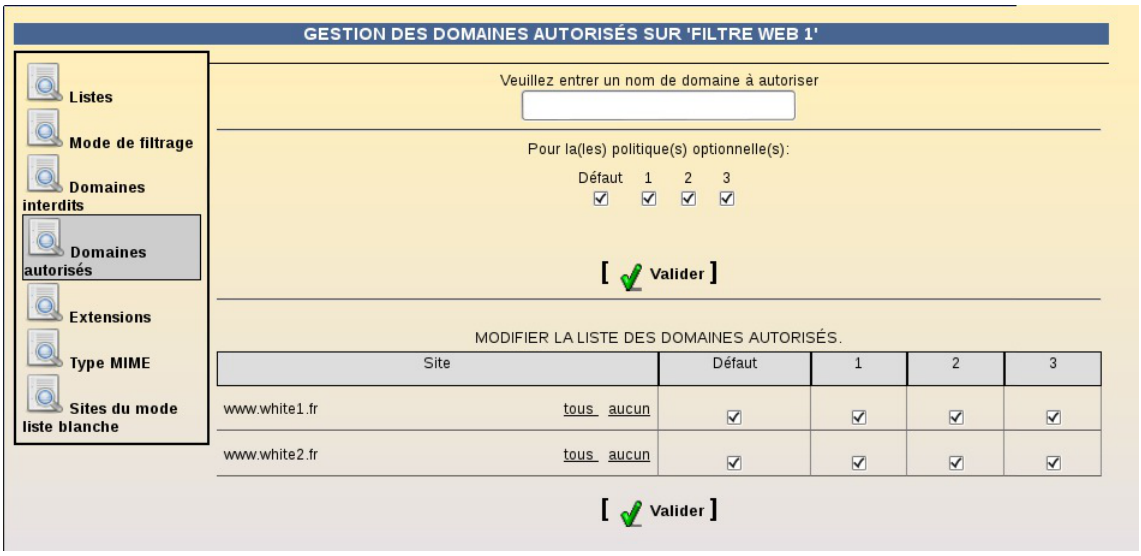
Il est possible de forcer l'autorisation de domaines ou d'URL (liste blanche[p.718]) en les ajoutant à la liste des domaines autorisés.

Cette liste de domaines s'applique :

- sur une zone de filtre web portant le nom du filtre choisi dans l'interface de configuration du module ;
- de manière plus fine par politique de configuration (si des utilisateurs ou des groupes de machine ont été associés à des politiques optionnelles).

Le formulaire se trouve dans `Filtre web 1` / `Sites` / `Sites autorisés`

Le formulaire qui permet d'autoriser des domaines est atteignable par le menu portant le nom du filtre choisi dans l'interface de configuration du module, `Filtre web 1` par défaut puis `Sites` / `Domaines autorisés`.



Autorisation de sites pour les quatre politiques de la zone de configuration sur le filtre nommé par défaut "Filtre web 1"

Les domaines autorisés sont écrits dans :

`/var/lib/blacklists/dansguardian<num_instance>/f<num_politique>/whites`

Sur le module AmonEcole, ces fichiers sont dans le conteneur `internet`.

Ajout de sites autorisés personnalisés par les académies ou les collectivités

Il est possible d'ajouter manuellement des domaines dans la liste blanche afin d'autoriser l'accès à ces domaines dans tous les cas. Pour ce faire, il suffit d'éditer le fichier `/var/lib/blacklists/white/freelist` et d'y ajouter un domaine par ligne (exemple : `departement41.fr`).

Sur le module AmonEcole, ces fichiers sont dans le conteneur `internet`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

3.4.8. Sites : Interdire des extensions et des types MIME

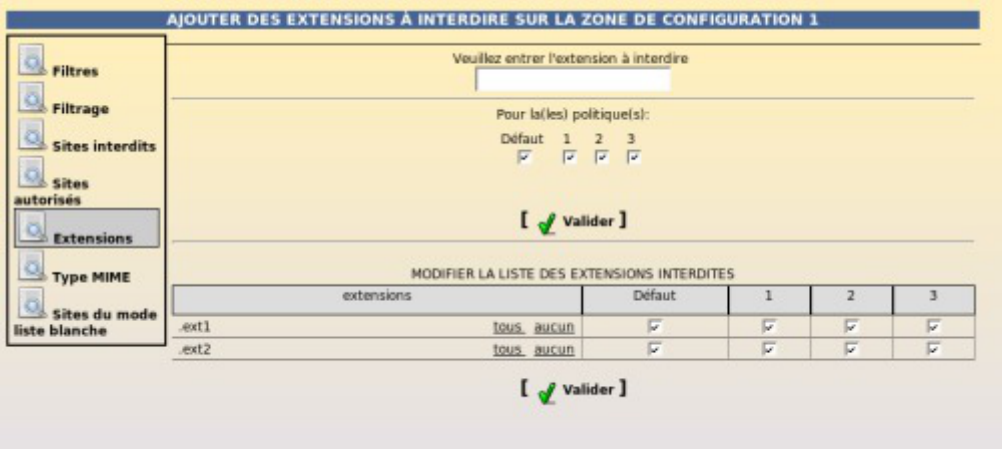
Interdire des extensions

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`.



Interdiction d'extensions pour les quatre politiques de la zone de configuration 1

Cette fonctionnalité n'est pas compatible avec le protocole HTTPS.

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

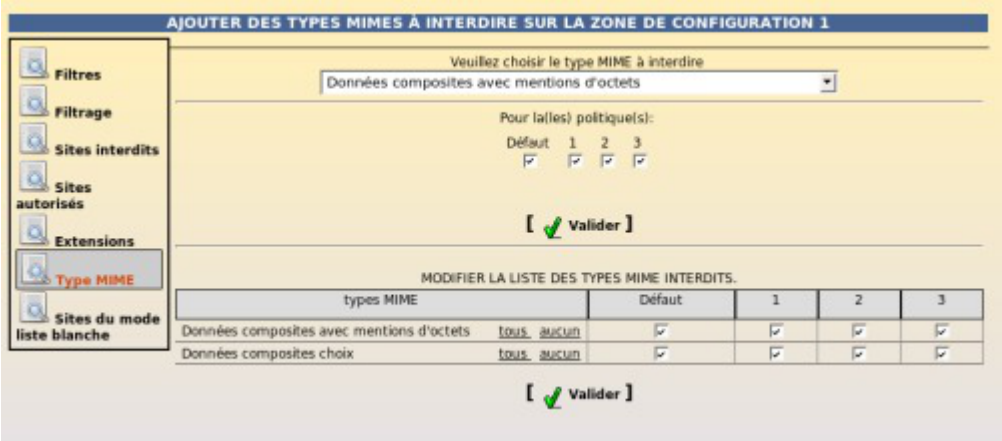
Il est possible d'interdire des types MIME[p.733]. Cette interdiction fonctionne comme celle des extensions.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Interdiction de types MIME pour les quatre politiques de la zone de configuration 1

Cette fonctionnalité n'est pas compatible avec le protocole HTTPS.

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*** .

3.4.9. Sites : Politique liste blanche

Le politique liste blanche[p.718] permet de restreindre la navigation web à une liste de sites autorisés.
Le principe est "tout est interdit sauf".

Le mode liste blanche n'est compatible que lorsque `déchiffrement HTTPS` est activé sur Squid (dans `gen_config` (cf. Onglets Squid et Squid2 : activation du déchiffrement HTTPS) [p.154]).

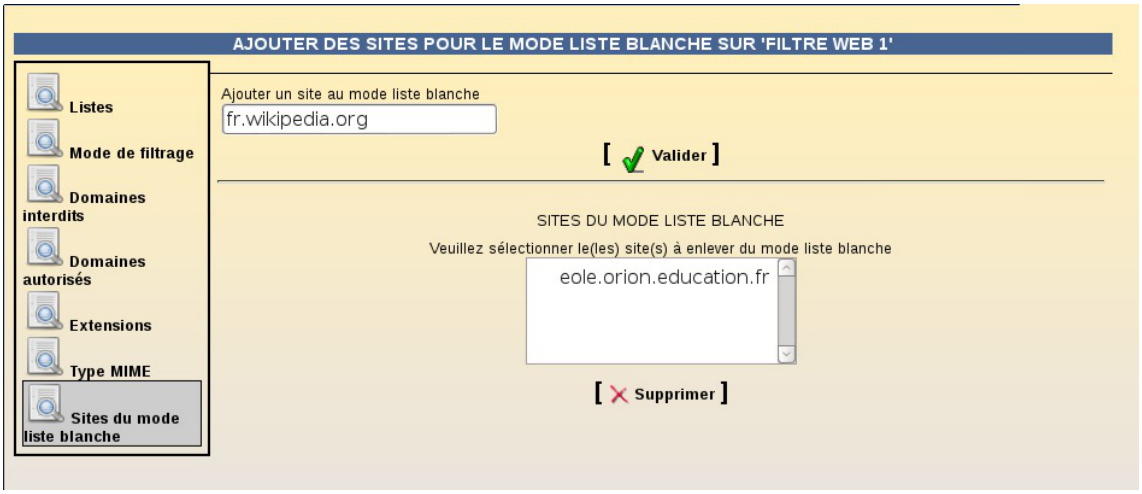
Restreindre la navigation au site Wikipédia pour les utilisateurs en mode liste blanche de la zone nommée par défaut "Filtre web 2"

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).

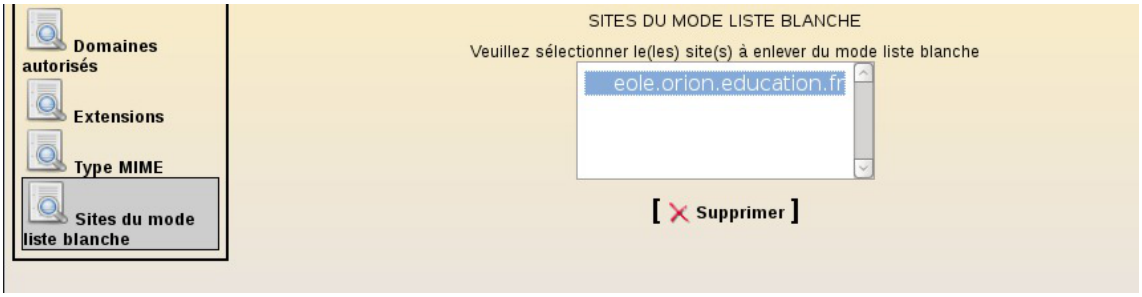
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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`.

3.4.10. Utilisateurs : 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.

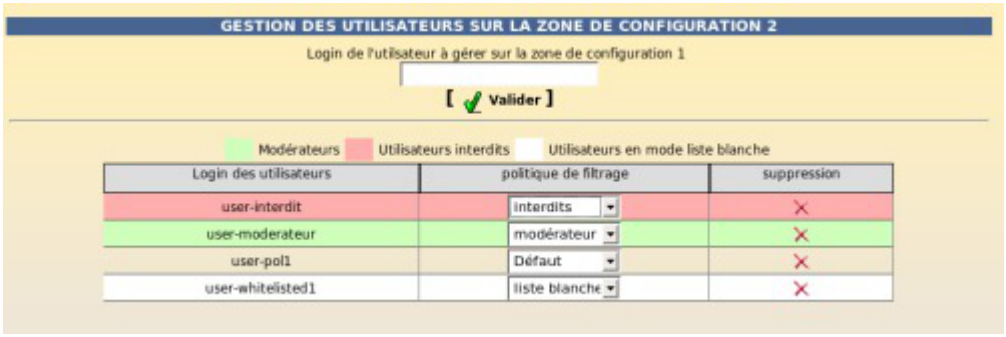
Placer un professeur sur la liste des modérateurs pour la zone de filtre web 1

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` :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- entrer le nom de l'utilisateur ;
- valider ;
- choisir `Modérateur` dans la liste.



Configurer des politiques de filtrage pour un utilisateur sur la zone de filtre web 2

Ces informations sont stockées dans :

`/var/lib/blacklists/dansguardian<num_instance>/common/filtergroupslist`

Sur AmonEcole, ces fichiers sont dans le conteneur ***`reseau`*** *.*

Si le menu `Utilisateurs` n'apparaît pas, c'est que la zone n'est pas authentifiée.

Le mode modérateur n'est pas compatible avec l'authentification NTLM : #19351 [https://dev-eole.ac-dijon.fr/issues/19351] .

Correspondance entre numéro de politique et mode de fonctionnement

Pour chaque instance de e2guardian, 8 politiques sont pré-définies par les fichiers `guardianfX.conf` :

- politique n°1 : politique par défaut (`politiquedefaut`) ;
- politique n°2 : utilisateur modérateur (`groupmoderateurs`) ;
- politique n°3 : utilisateur interdit (`groupinterdits`) ;
- politique n°4 : utilisateur en mode liste blanche (`grouplisteblanche`) ;
- politique n°5 : politique de filtrage personnalisée n°1 (`politique1`) ;
- politique n°6 : politique de filtrage personnalisée n°2 (`politique2`) ;
- politique n°7 : politique de filtrage personnalisée n°3 (`politique3`) ;
- politique n°8 : politique de filtrage personnalisée n°4 (`politique4`).

3.5. Outil d'analyse de logs LightSquid

LightSquid est un analyseur de logs pour le proxy/cache Squid[p.731].

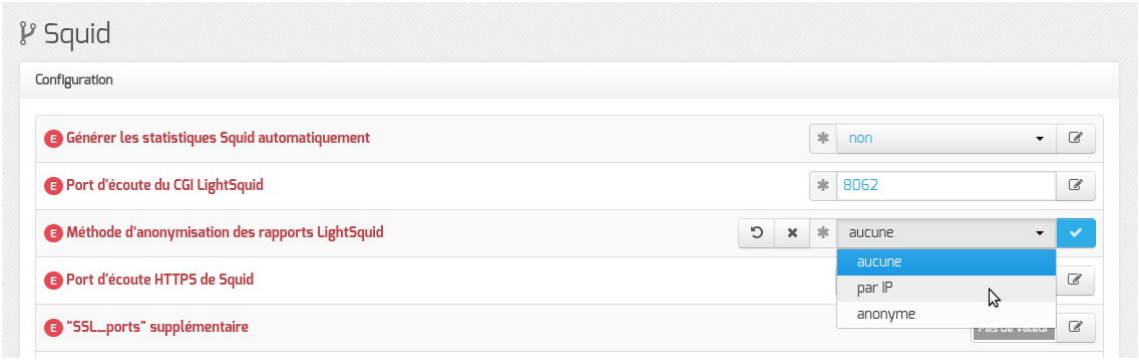
Les statistiques générées manuellement ou automatiquement par cet outil sont consultables dans l'interface EAD.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

http://lightsquid.sourceforge.net/

Configuration

LightSquid se paramètre dans l'interface de configuration du module, dans l'onglet expert `Squid`. Pour activer la génération automatique des statistiques (toutes les nuits) il faut passer la variable `Générer les statistiques Squid automatiquement` à `oui`. Le port par défaut est 8062.



Paramétrage de Lightsquid

La génération des statistiques proxy peut se faire manuellement, en exécutant la commande `squid_parselogs.sh`.

La méthode d'anonymisation des statistiques générées est également paramétrable :

- `aucune` : aucune anonymisation ;
- `par IP` : n'affiche que les adresses IP ;
- `anonyme` : entièrement anonyme (remplace par un tiret).



Suite à un incident, les statistiques sont celles de la veille, il faut penser à forcer la génération manuellement.

Techniquement, LightSquid fonctionne en mode *cgi* sur un port local (8062 par défaut).

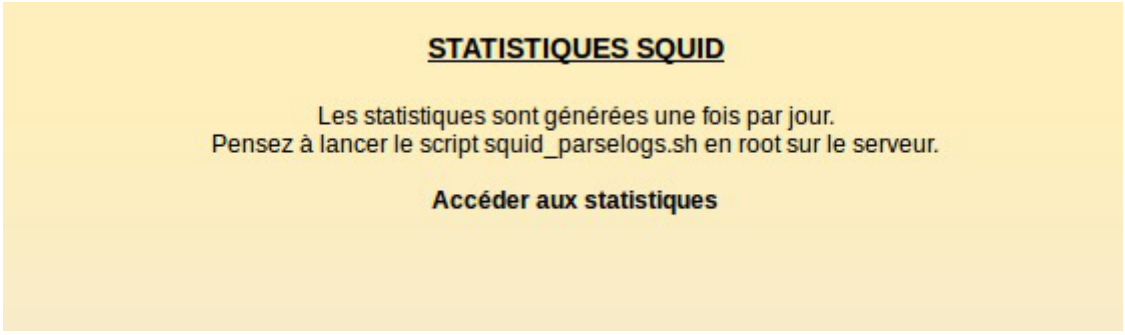
Cela entraîne certaines limitations :

- la ré-authentification nécessaire en mode "pam" ;
- l'accès aux statistiques est impossible depuis un frontend EAD distant.

Consultation

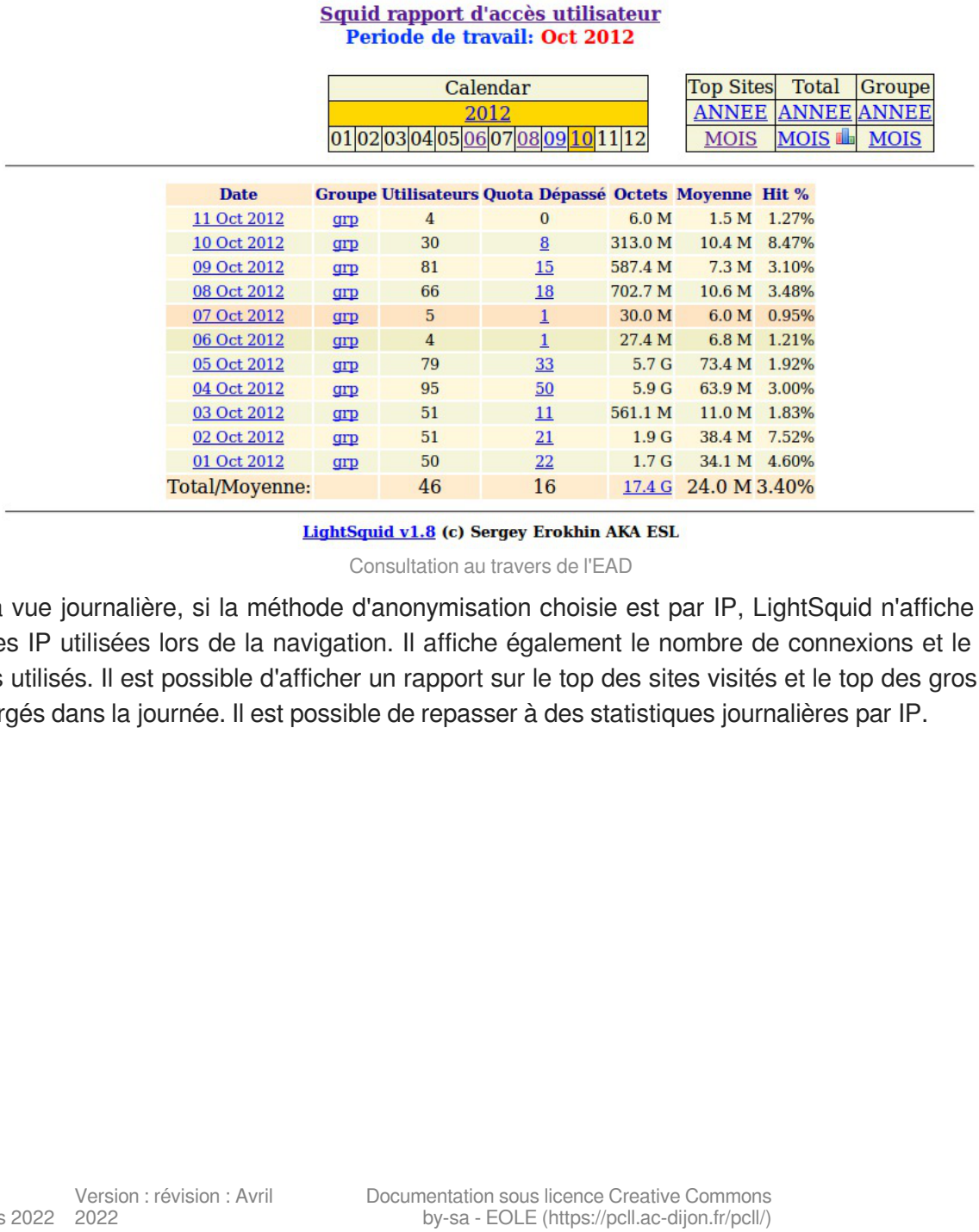
La consultation des statistiques LightSquid se fait au travers de l'EAD, dans le menu `Outils` / `Statistiques proxy`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Pour afficher les statistiques il faut cliquer sur le lien `Accéder aux statistiques`. La navigation se fait dans une nouvelle fenêtre qui demande une authentification. Par défaut, ces statistiques ne sont accessibles que pour le rôle `admin`, un clic sur le bouton `Connexion` sans mot de passe permet de passer à la demande d'authentification pour le compte `root`.

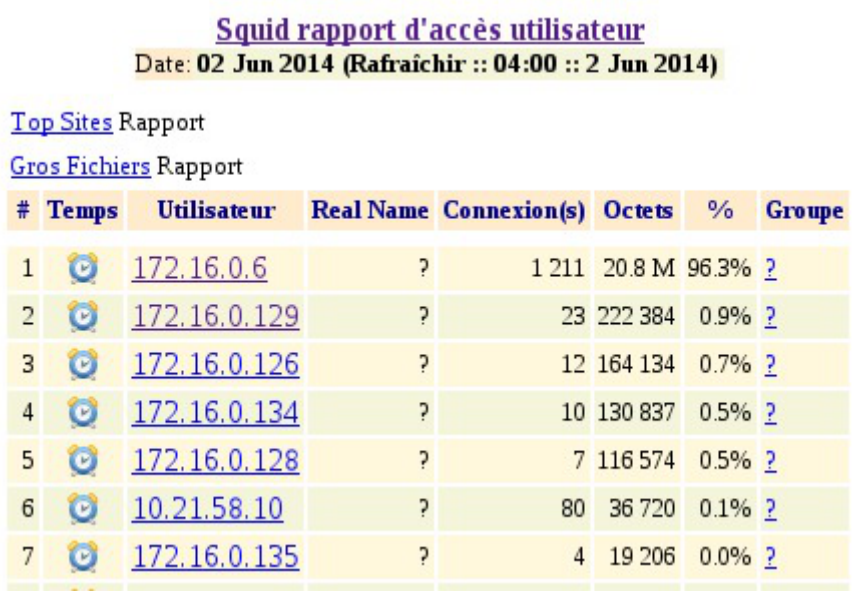
Une fois connecté la vue initiale propose de naviguer dans les statistiques par date (année, jour, mois), par groupe, par quota dépassé.



Consultation au travers de l'EAD

Dans la vue journalière, si la méthode d'anonymisation choisie est par IP, LightSquid n'affiche que les adresses IP utilisées lors de la navigation. Il affiche également le nombre de connexions et le nombre d'octets utilisés. Il est possible d'afficher un rapport sur le top des sites visités et le top des gros fichiers téléchargés dans la journée. Il est possible de repasser à des statistiques journalières par IP.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Squid rapport d'accès utilisateur

Date: 02 Jun 2014 (Rafraîchir :: 04:00 :: 2 Jun 2014)

Top Sites Rapport

Gros Fichiers Rapport

#	Temps	Utilisateur	Real Name	Connexion(s)	Octets	%	Groupe
1		172.16.0.6	?	1 211	20.8 M	96.3%	?
2		172.16.0.129	?	23	222 384	0.9%	?
3		172.16.0.126	?	12	164 134	0.7%	?
4		172.16.0.134	?	10	130 837	0.5%	?
5		172.16.0.128	?	7	116 574	0.5%	?
6		10.21.58.10	?	80	36 720	0.1%	?
7		172.16.0.135	?	4	19 206	0.0%	?

Vue journalière des statistiques

Dans la vue des statistiques journalières par IP, toutes les adresses visitées par l'utilisateur s'affichent avec le nombre de connexions et les octets consommés.



Squid rapport d'accès utilisateur

Utilisateur: 172.16.0.6 (?)

Groupe: ?

Date: 02 Jun 2014

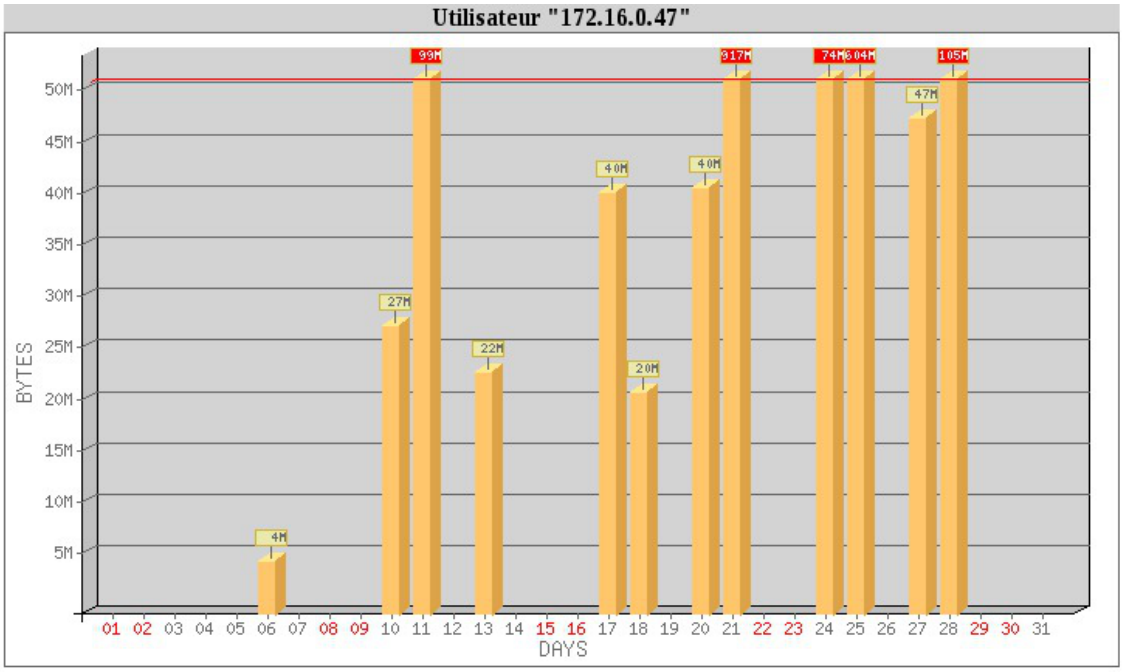
User download "Big Files"

Total					
			20.8 M		
#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	osce106-ilspn25-p.activeupdate.trendmicro.com	28	19.6 M	19.6 M	94.3%
2	osce106-ilspn25wr-p.activeupdate.trendmicro.com	16	869 227	20.5 M	3.9%
3	92.51.156.70	1 152	340 194	20.8 M	1.5%
4	cyberlib.crdp-poitiers.org:443	14	25 142	20.8 M	0.1%
5	ctldl.windowsupdate.com	1	337	20.8 M	0.0%
Total			20.8 M		

Vue journalière par IP des statistiques

Dans la vue par mois, un clic sur la consommation total des Octets donne un classement de la consommation d'octets par adresse IP. Dans le tableau affiché, un graphe mensuel de la consommation d'octets par adresse IP est disponible.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Graphe mensuel de la consommation d'octets pour une adresse IP

4. ERA, éditeur de règles pour le module Amon

4.1. Introduction

4.1.1. Présentation

Présentation et fonctionnalités

L'outil EOLE de génération de règles de pare-feu[p.725] pour les modules Amon et AmonEcole se nomme ERA[p.711].

Il permet de gérer la description de la politique de sécurité d'un pare-feu[p.725]. 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.716], de manière à instancier ces règles sur un pare-feu[p.725] cible.

ERA et sa documentation sont sous licence libre.

Interface ERA

À partir d'EOLE 2.9, l'interface ERA s'exécute dans un conteneur[p.707] logiciel Podman[p.726].

L'image `era` est téléchargée depuis le site hub.eole.education [http://hub.eole.education] .

Le serveur doit donc pouvoir accéder à ce domaine au même titre qu'aux serveurs de mise à jour des modules.

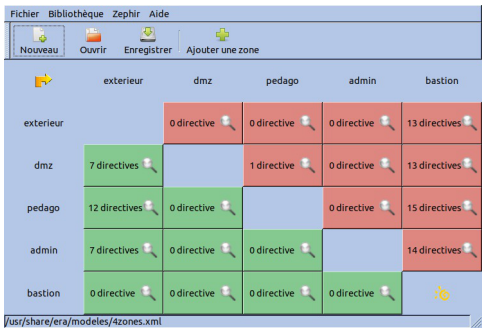
Un logiciel en deux parties

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.716] 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 :



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.

4.1.2. Les fichiers XML de modèles

Un modèle[p.721] est un fichier de description du pare-feu. Le format d'enregistrement est un format XML[p.735].

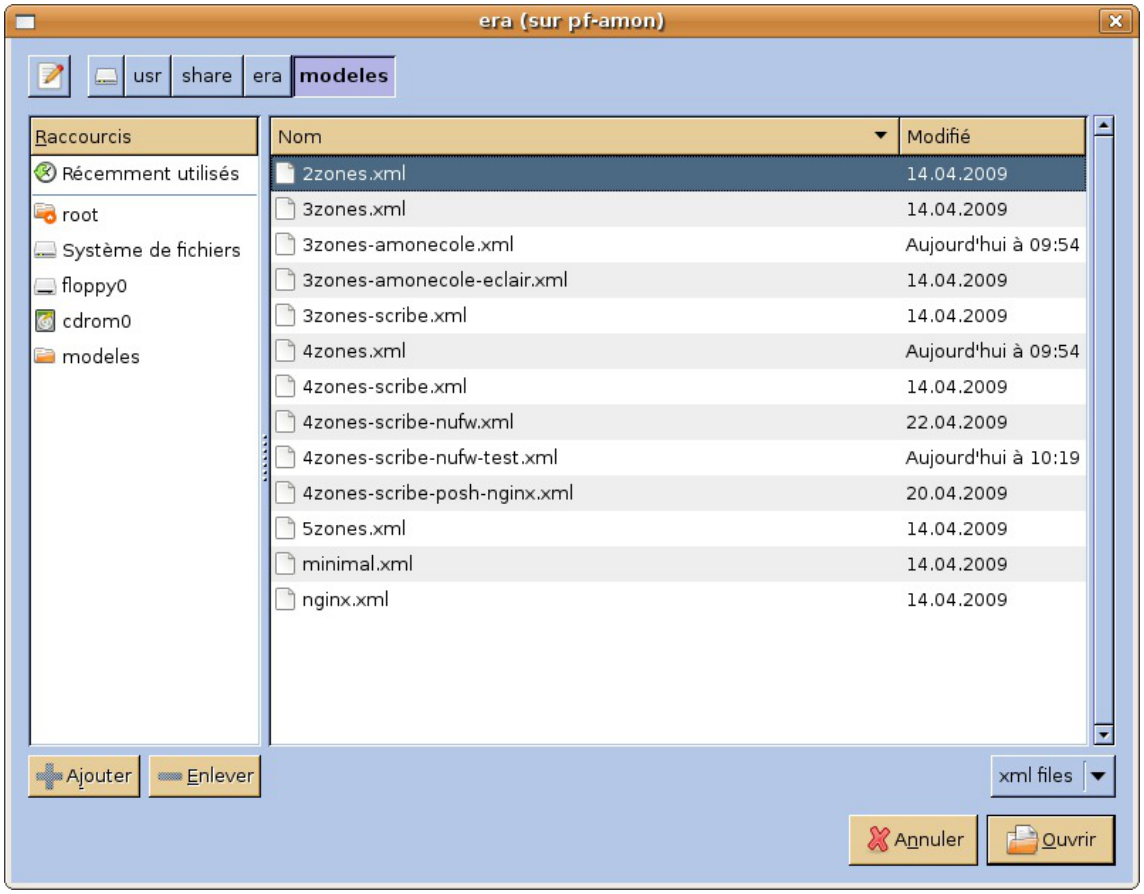
Divers modèles caractéristiques de description de pare-feu sont disponibles dans le répertoire `/usr/share/era/modeles` et sont des exemples de types de pare-feu (deux, trois, quatre ou cinq cartes réseau).

Création d'un modèle personnalisé

En général il est préférable, pour commencer un pare-feu, de partir d'un des modèles exemples, et d'y ajouter des directives (ou bien d'en enlever).

Partez de préférence d'un modèle qui correspond au nombre de cartes réseau dont vous disposez sur le serveur.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Boite de dialogue d'ouverture d'un modèle

Lorsque vous modifiez un modèle exemple, il faut impérativement l'enregistrer sous un autre nom, sinon les modifications seront perdues à la prochaine mise à jour du paquet `era`.

Le nouveau fichier XML doit être enregistré dans le répertoire `/usr/share/era/modeles/`.

Enfin, pour que le serveur utilise ce modèle, il faut modifier la variable *`type_amon`* (`Modèle de filtrage` dans l'onglet `Firewall` de l'interface de configuration du module).

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>`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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.709].

Les numéros de version sont généralement corrélés avec les versions des modules EOLE : 2.0, 2.3, 2.4, 2.42.

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.

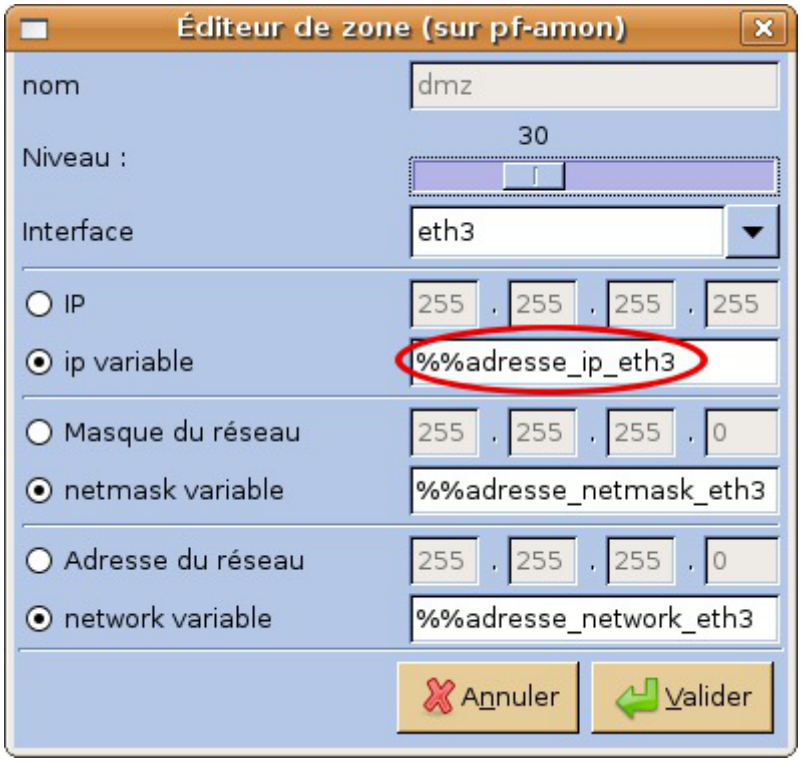
4.1.3. Utilisation de variables Creole

ERA[p.711] 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.708] (elles commencent par `%%`) plutôt que des valeurs fixes.

Le fichier XML de description de pare-feu devient alors un template[p.733] Creole.

Dans la fenêtre d'édition d'une zone, entrer une valeur du type `%%ip_variable` plutôt qu'une valeur IP fixe.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> Une adresse IP de zone peut être templatisée (IP en variable Creole)

Variables multi-valuées

Creole propose un concept de variables multi-valuées qui peuvent également être utilisées dans ERA.

Si une variable `%%variable` est multi-valuée (au sens de Creole, c'est-à-dire que la variable contient une liste de valeurs), et que cette variable est présente dans une règle iptables, alors la règle sera répétée autant de fois que de valeurs dans `%%variable` puisque cette fonctionnalité génère du code avec une boucle for :

```
%for %%v in %%variable /sbin/iptable bla bla %%v bla bla %end for
```

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.

4.2. Utilisation

4.2.1. Les zones de sécurité

Présentation

L'éditeur ERA est un outil de conception par zones[p.735]. Une zone[p.735] 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`.

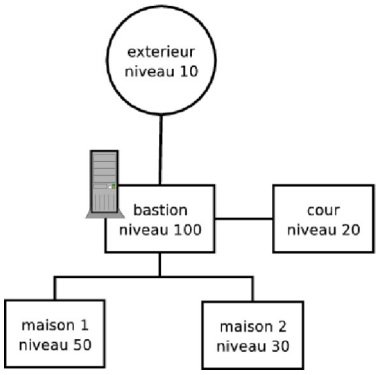
Les zones sont ensuite ordonnées par niveau de sécurité[p.723] sous forme d'entiers de 0 à 100.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.712] 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.712] qui y sont associées.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 l'interface 1

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`

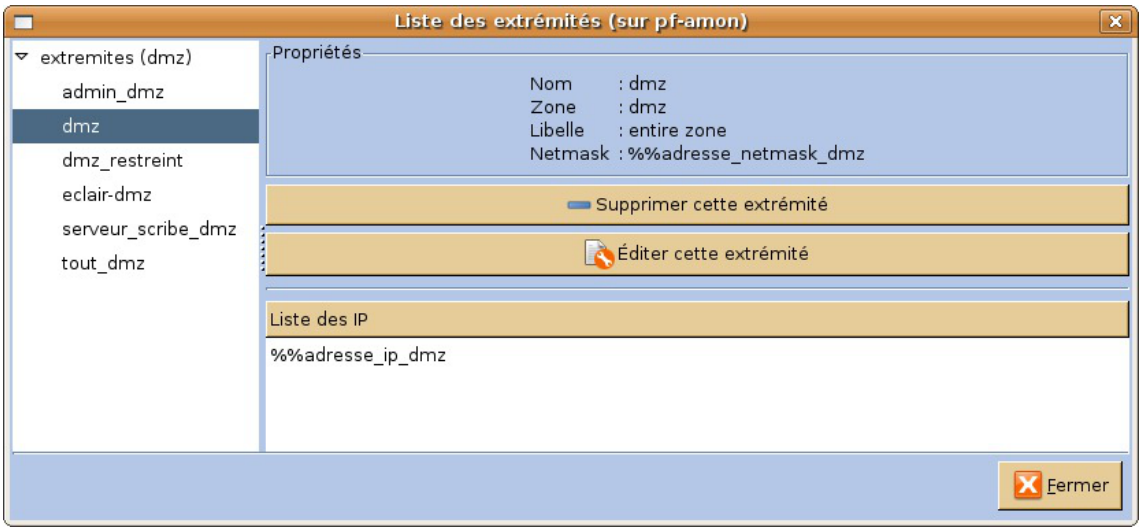
`netmask variable :` `%%id vlan_eth1[0].adresse_netmask_vlan_eth1`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Ajouter une extrémité

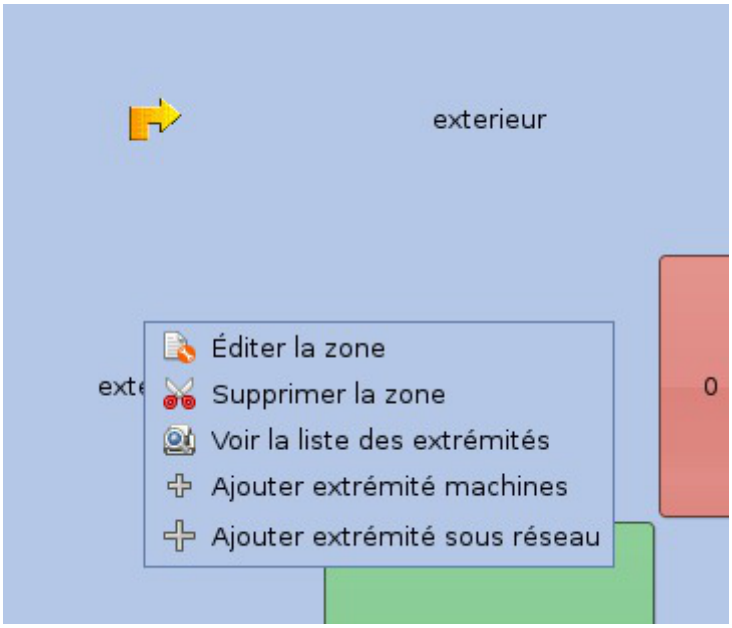
La liste des extrémités est disponible dans le menu bibliothèque / extrémités.

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.



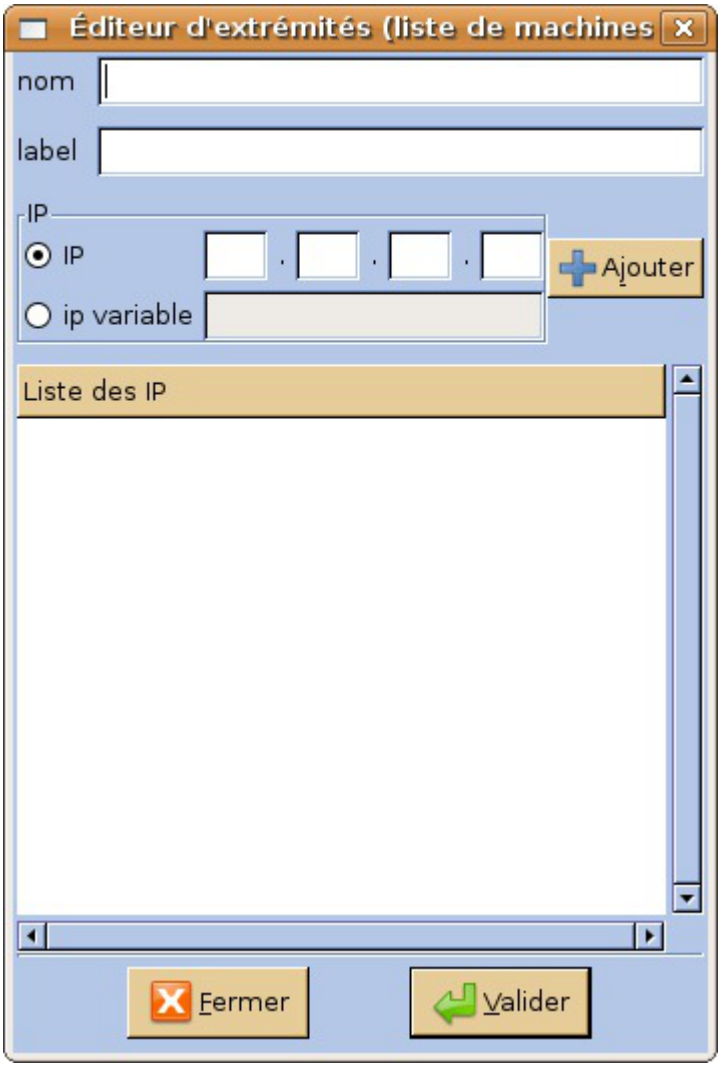
Liste des extrémités

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.

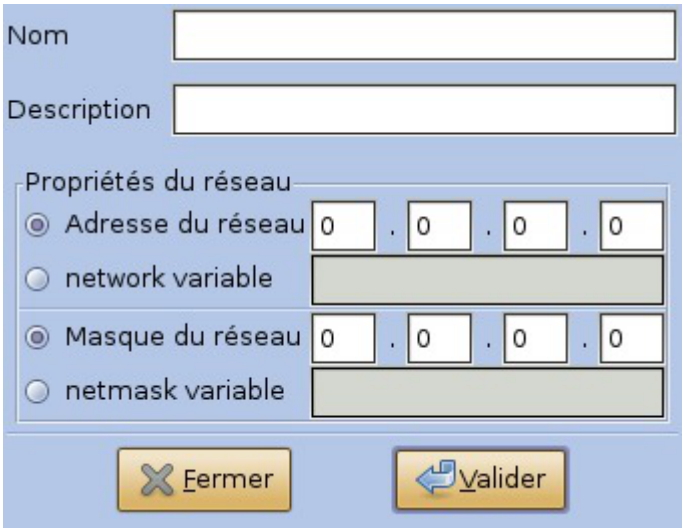


Un clic droit sur le nom d'une zone affiche le menu contextuel relatif à cette zone

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Ajout d'une extrémité dans le cas d'une liste de machines

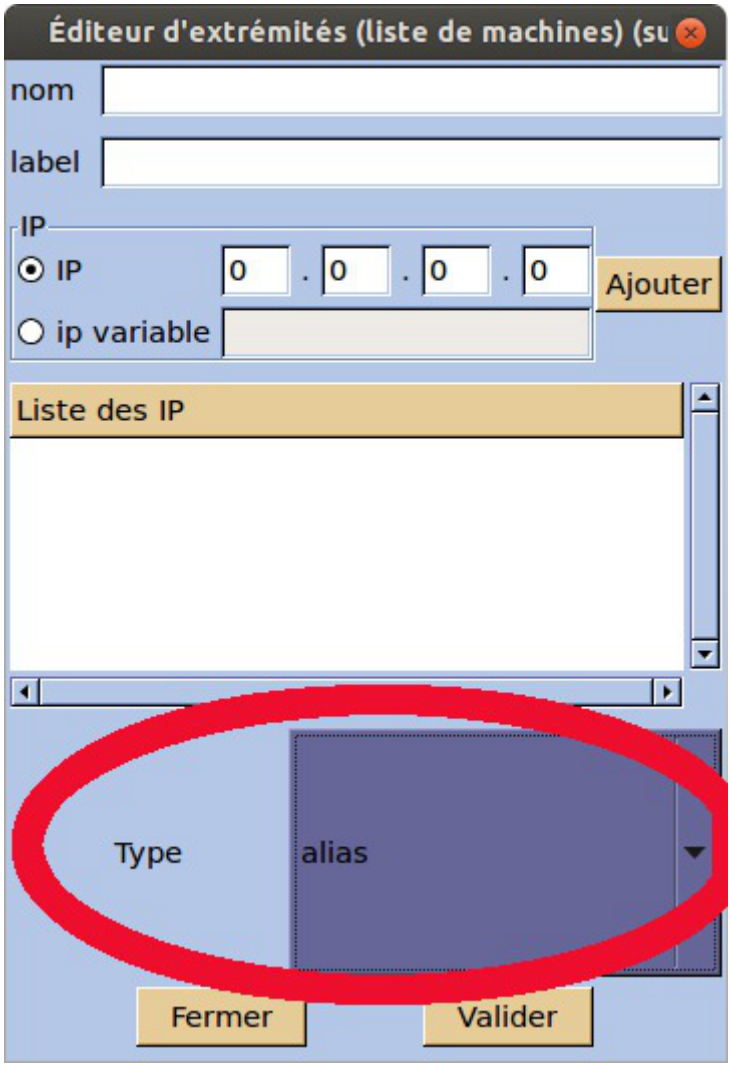


Ajout d'une extrémité de type sous réseau

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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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 l'interface 2 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.

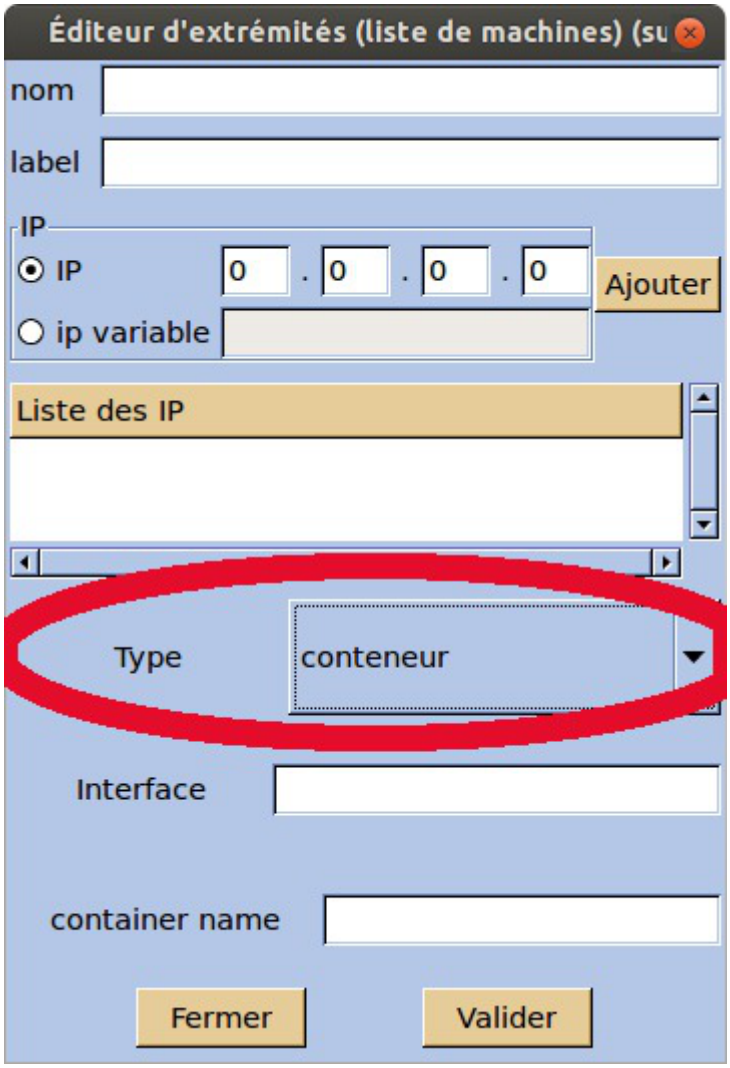
Les mauvaises fausses bonnes idées pour créer un alias

- 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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"...)

4.2.2. 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.712] 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.712]" et le "flux descendant[p.712]".

Les "flux montants[p.712]" concernent les zones[p.735] d'un niveau de sécurité plus faible vers un niveau de sécurité plus élevé, et réciproquement pour les "flux descendants[p.712]".

Pour pouvoir ordonner les flux en vue d'une cohérence globale, il convient ensuite de modéliser le "

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

tableau des flux[p.732]".

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).

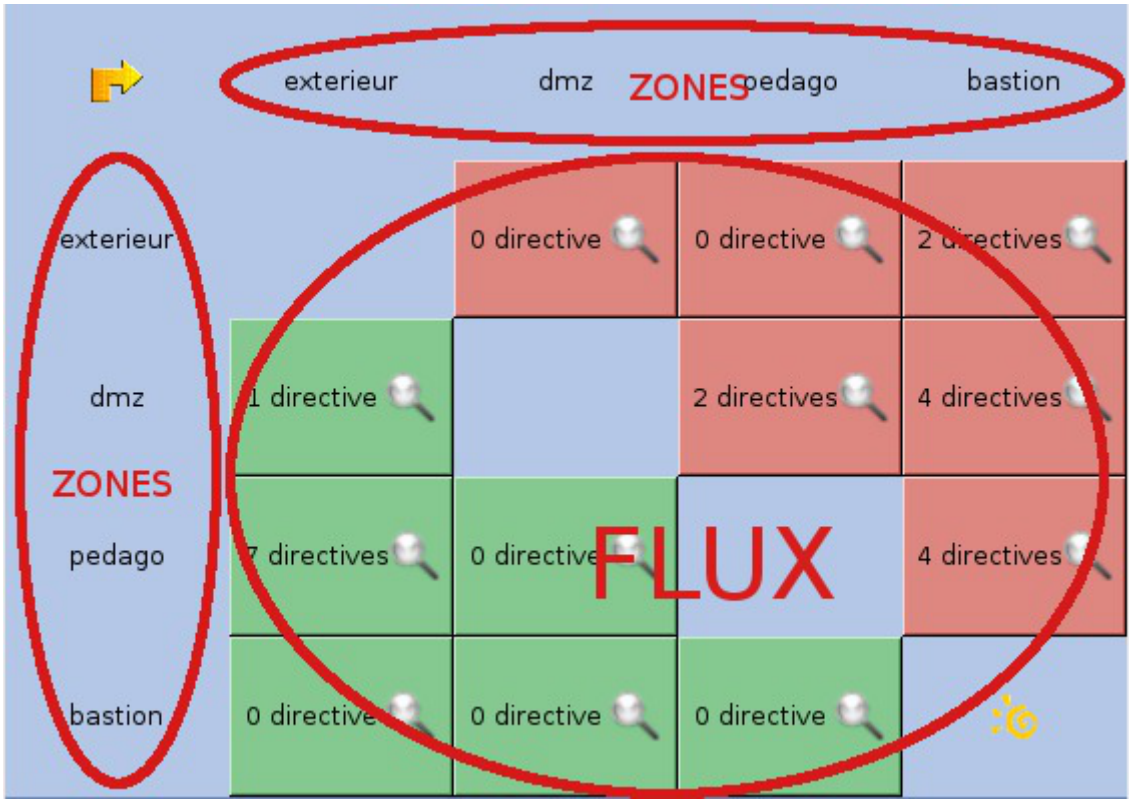
Changement de la politique par défaut

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Interface d'ERA avec un modèle chargé

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.

4.2.3. Les directives

4.2.3.a. Présentation

Une directive[p.721] 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".

4.2.3.b. Les services et les groupes de services

Avant de pouvoir créer une directive, il faut d'abord créer un service[p.730].

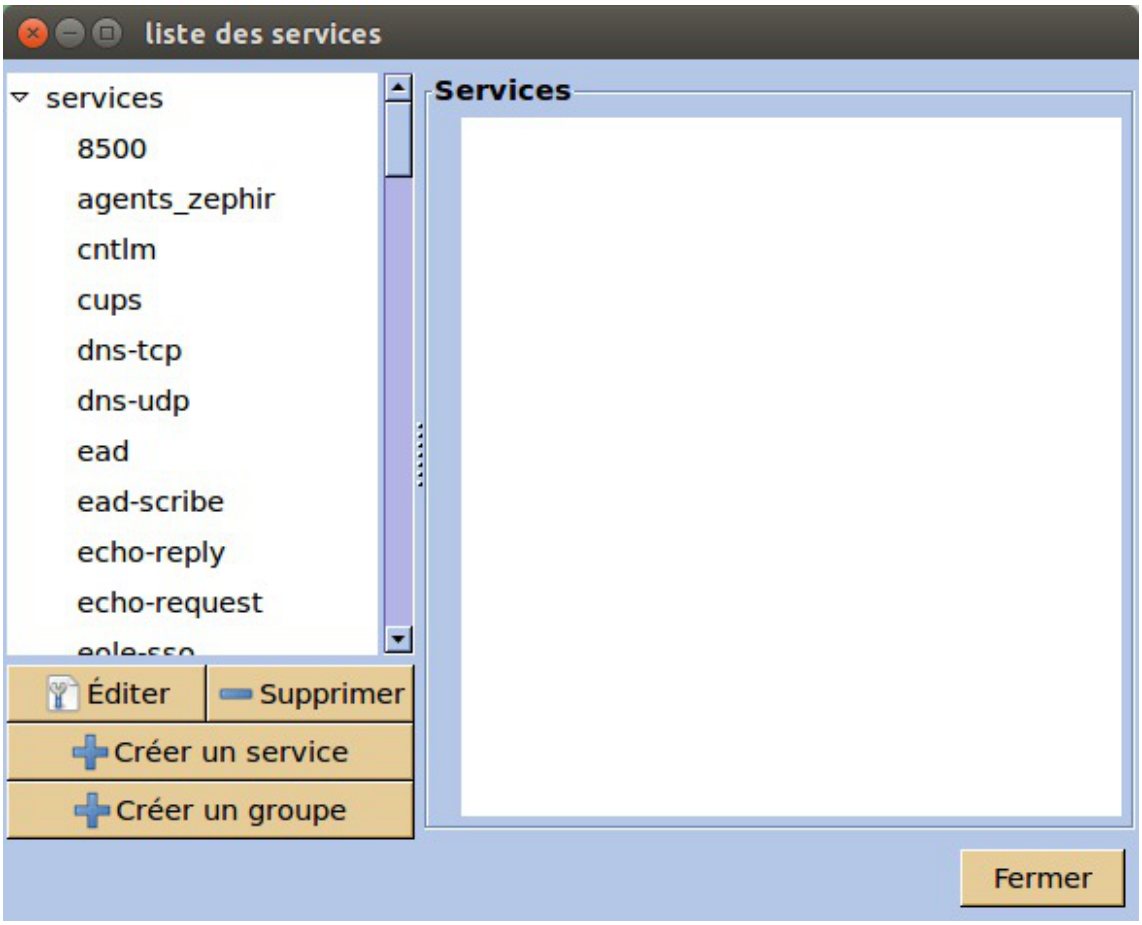
Par exemple, le service "serveur web" est défini par le protocole HTTP sur le port 80.

Il y a déjà une bibliothèque de services prédéfinis dans ERA.

Pour lister ces services, aller dans le menu : `Bibliothèque > services`.

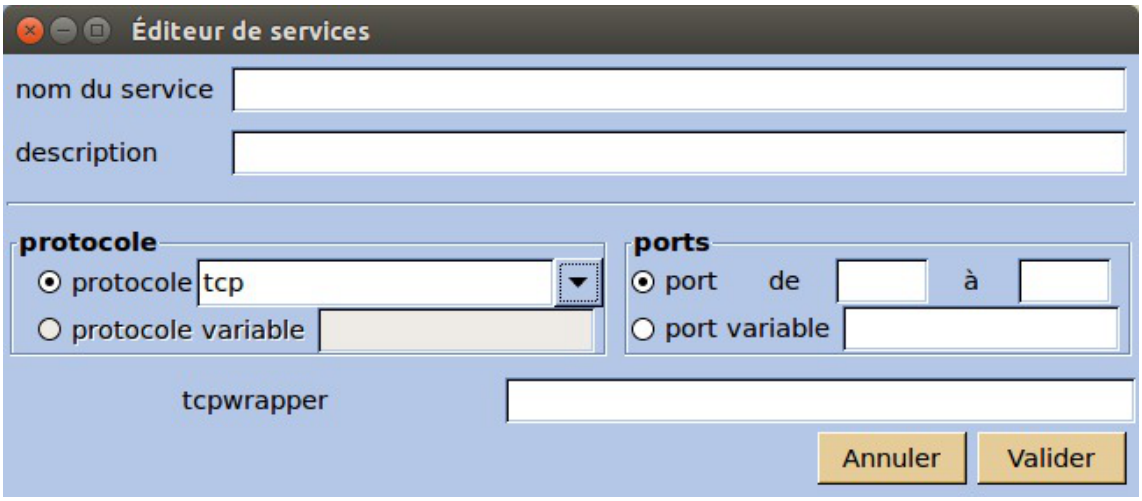
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

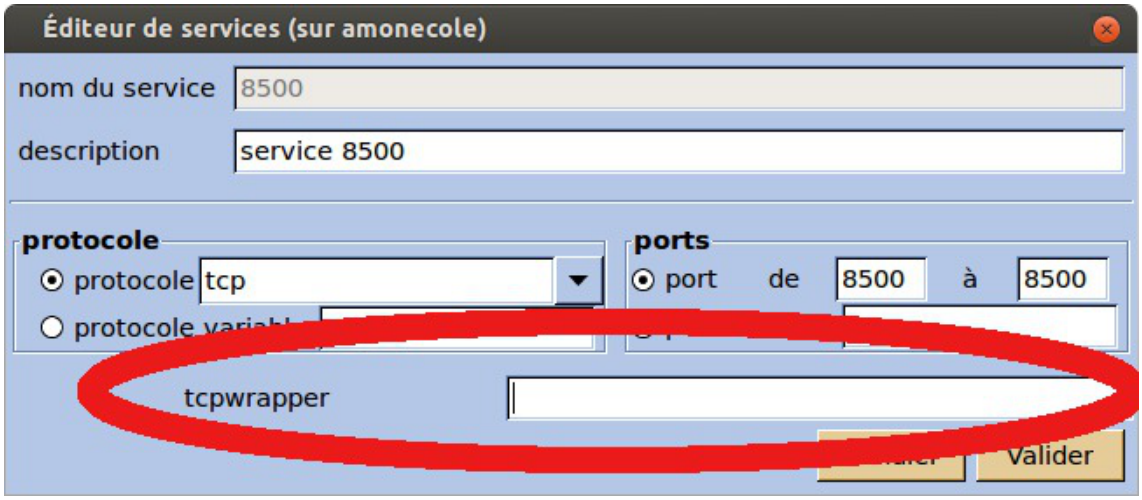
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.



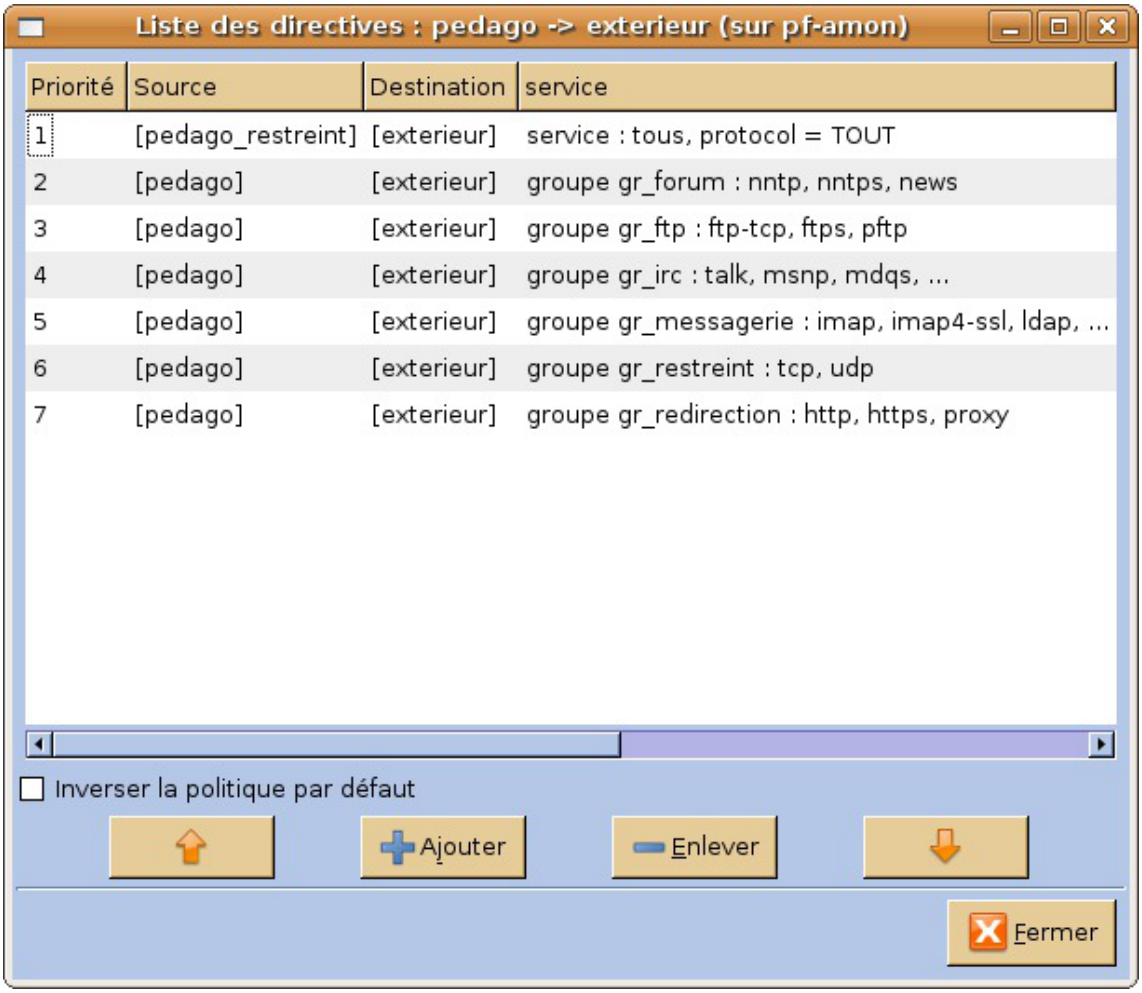
le tcpwrapper en mode conteneur

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.

4.2.3.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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Fenêtre de liste des directives dans un flux donné

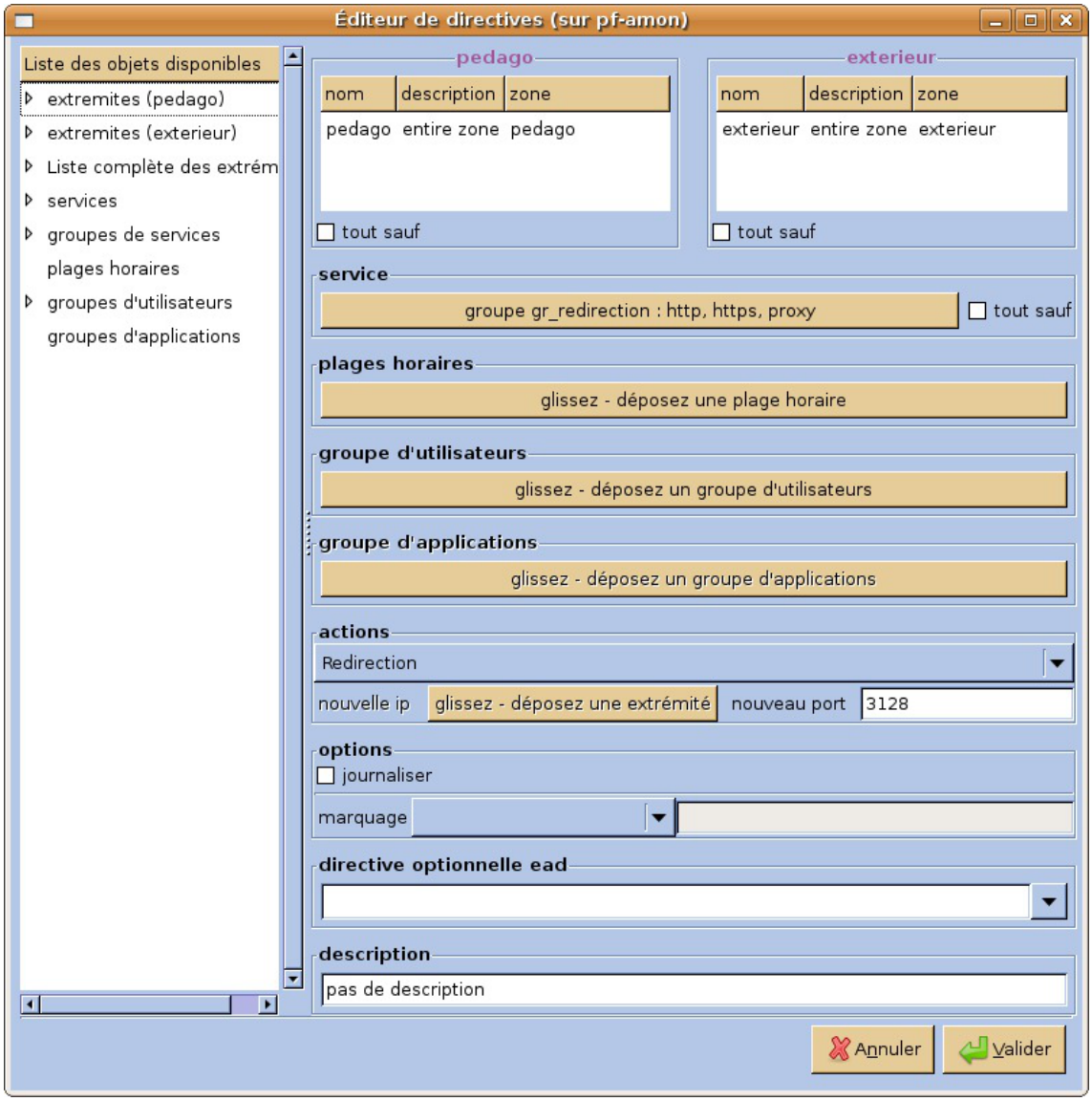
Les directives sont triées par ordre croissant. C'est l'ordre dans lequel seront appliquées les règles sur le pare-feu cible.



Les directives de `nat` et `redirection` sont appliquées forcément avant les autres. Ceci est le comportement de Netfilter[p.722].

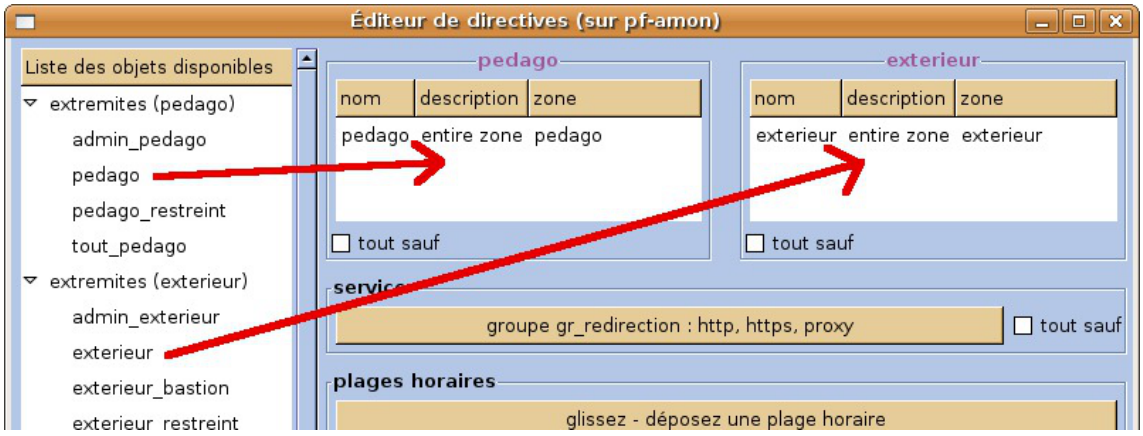
Depuis cette fenêtre, il est possible d'éditer une nouvelle directive (en double-cliquant dessus) ou d'en ajouter une si nécessaire.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Fenêtre d'édition des directives

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.



Glisser-déposer d'une extrémité pour la source et la destination d'une directive

Lors de la création de la directive, il est possible de mettre une liste d'extrémité de n'importe quel type (machine, sous-réseau...) comme source ou comme destination. Dans ce cas, la fonctionnalité "tout sauf" d'inversion des extrémités est désactivée.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

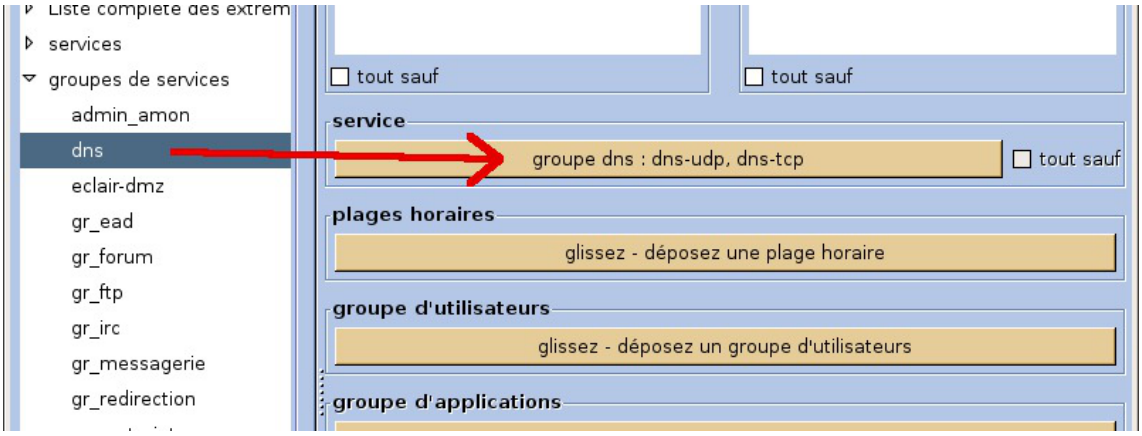
Si vous ne renseignez pas les extrémités, c'est la zone entière qui est prise (plus précisément l'extrémité désignant la zone entière).

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.



Sélection d'un service depuis l'éditeur de directive

> 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

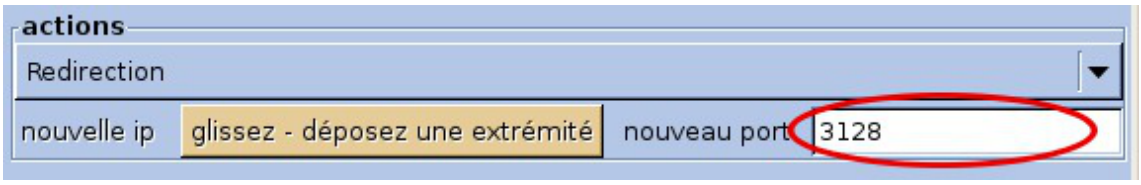


Type standard de directive (autorisation/interdiction)

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).



Directive de redirection

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.



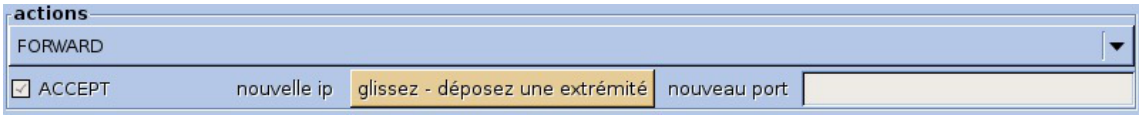
Glisser-déposer de l'extrémité de redirection

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

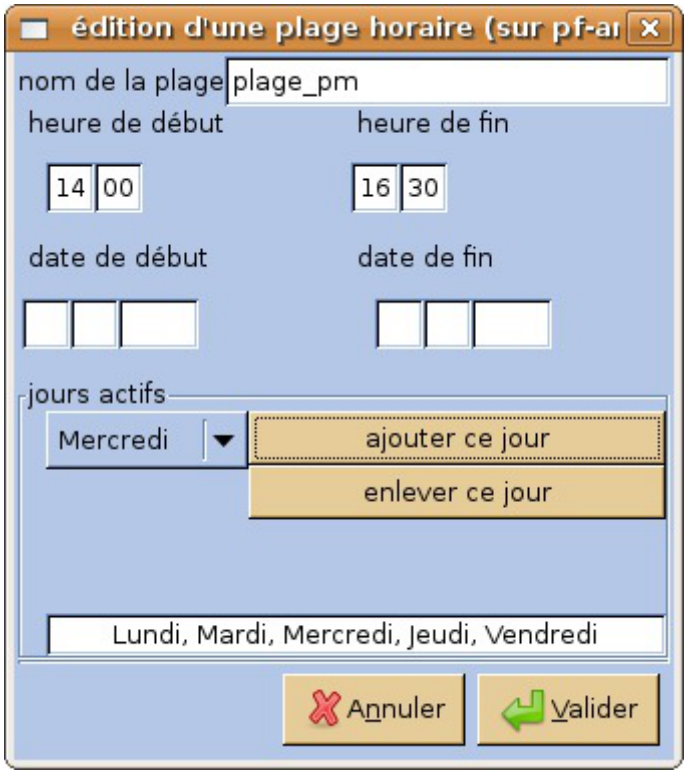
Création d'une plage horaire

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.



Ajouter des plages horaires

Le filtrage et les restrictions basées sur des plages horaires sont appliquées par l'utilisation du module *time* du logiciel iptables.

iptables interprète les dates en UTC[p.734], il y a donc un décalage normal entre ce qui est saisi dans l'interface et les informations renvoyées par la commande `iptables-save`.

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 plage horaire d'une directive

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> La journalisation

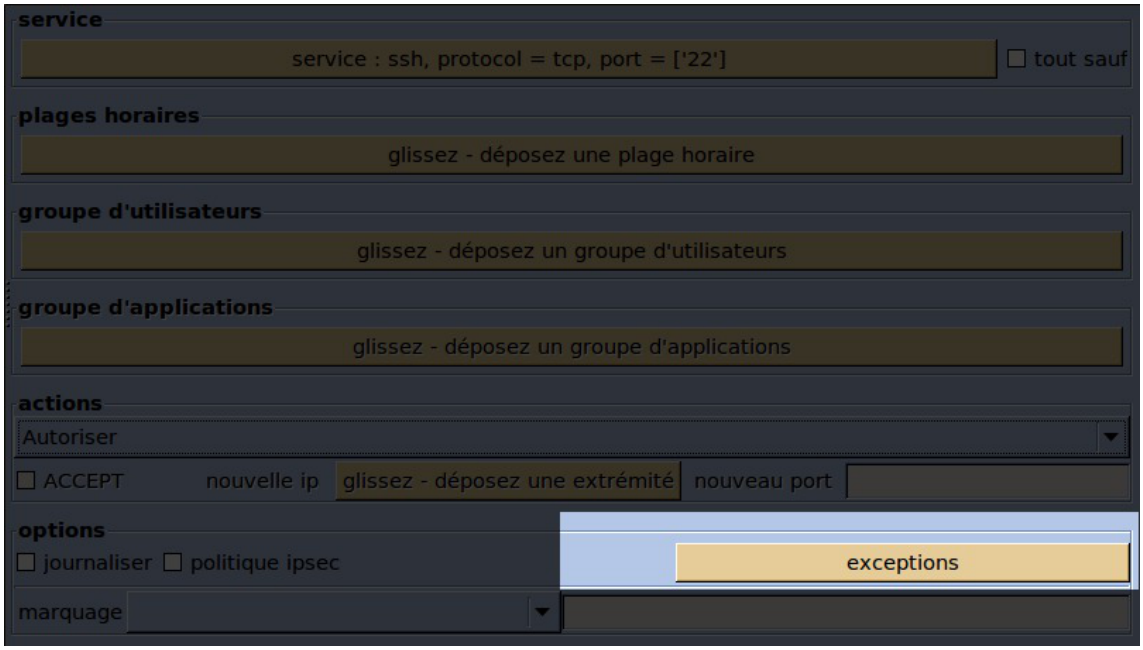
La case "journaliser" permet de tenir un journal des événements (logs) de la directive (grâce à ULOG).



Journaliser la directive

> Gérer des exceptions

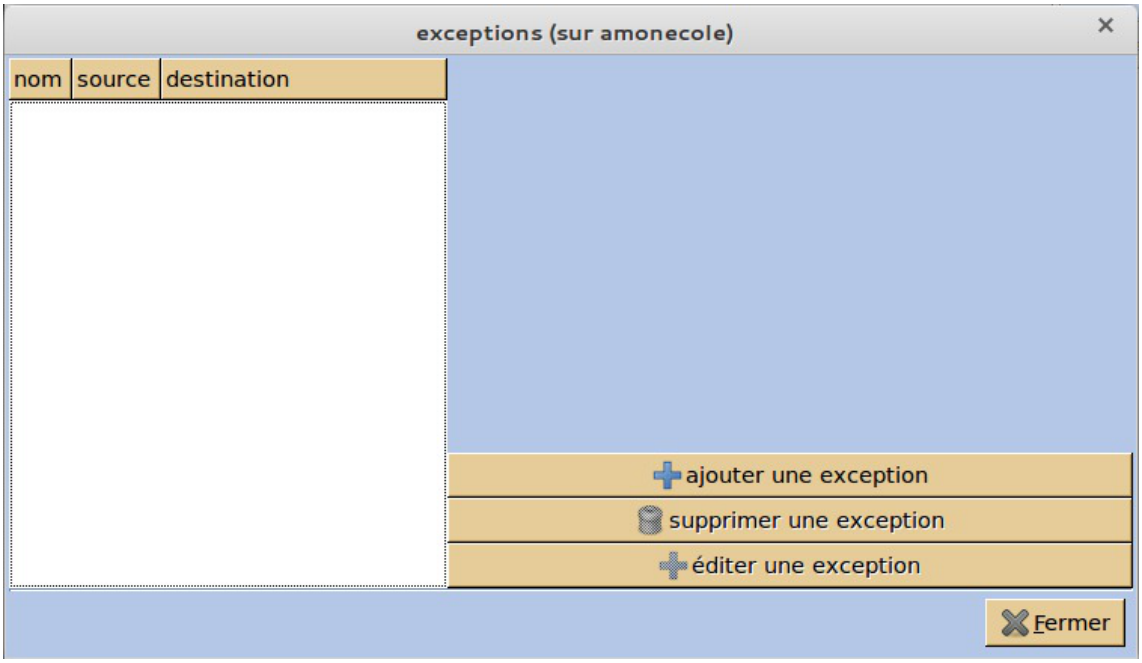
Dans l'éditeur de directives il est possible d'ajouter des exceptions.



L'éditeur d'exceptions permet :

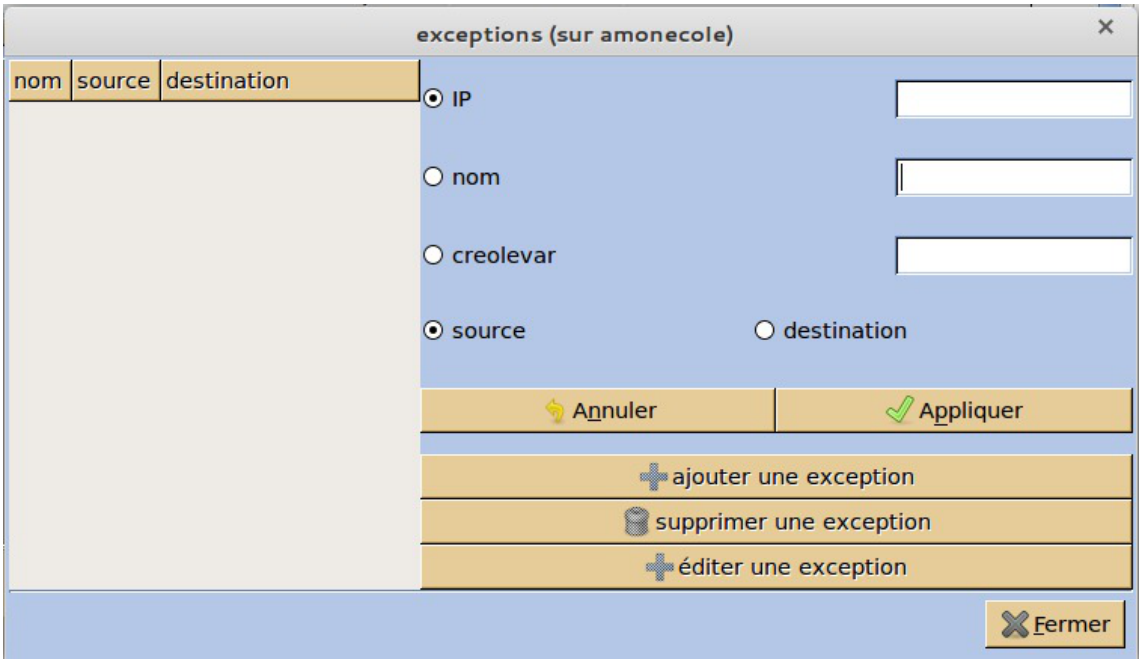
- d'ajouter une exception ;
- d'éditer une exception ;
- de supprimer une exception.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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.716] permettant d'identifier un paquet grâce à une marque spécifiée dans l'interface.

> Les directives optionnelles

Présentation

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Une directive optionnelle[p.709] est une directive qui va être activable ou désactivable depuis l'interface EAD[p.710].

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

Les directives optionnelles activées/désactivées dans l'EAD sont enregistrées dans le fichier : `/var/lib/eole/config/regles.csv`

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 utiliser d'autres caractères accentués.

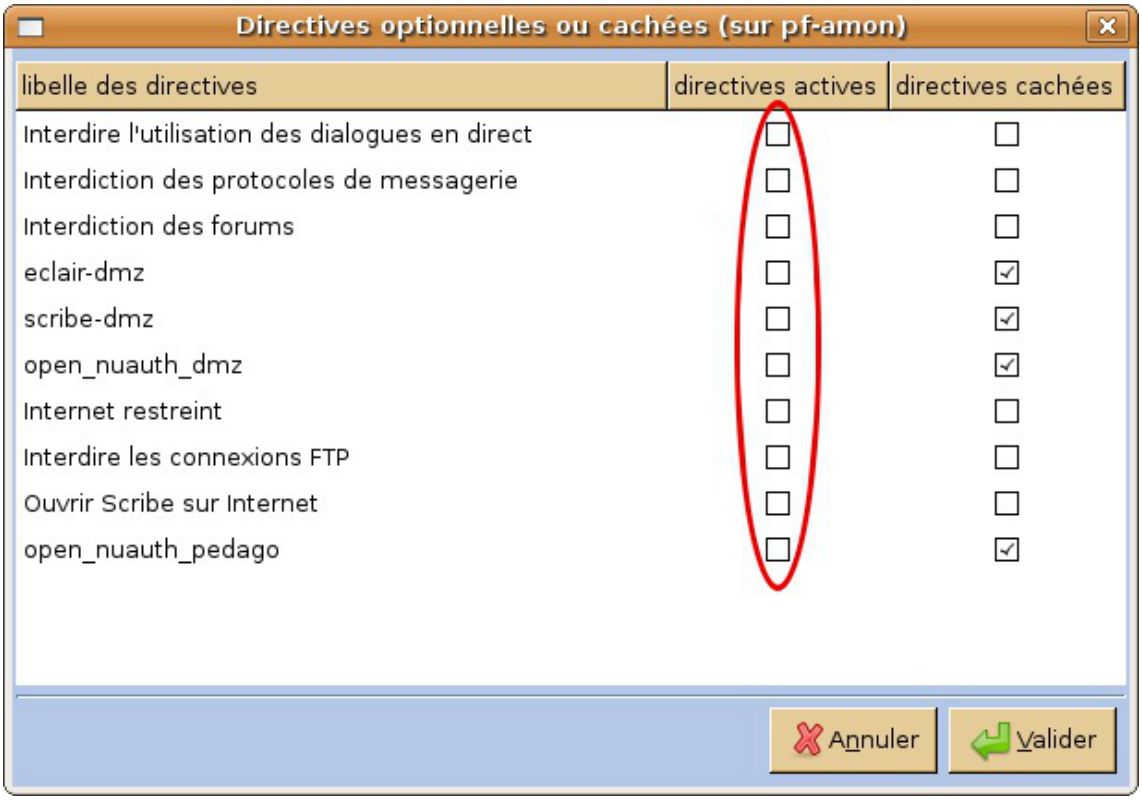
Directive optionnelle active

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Fenêtre de la bibliothèque permettant d'étiqueter une directive comme optionnelle

Directive optionnelle active et inactive

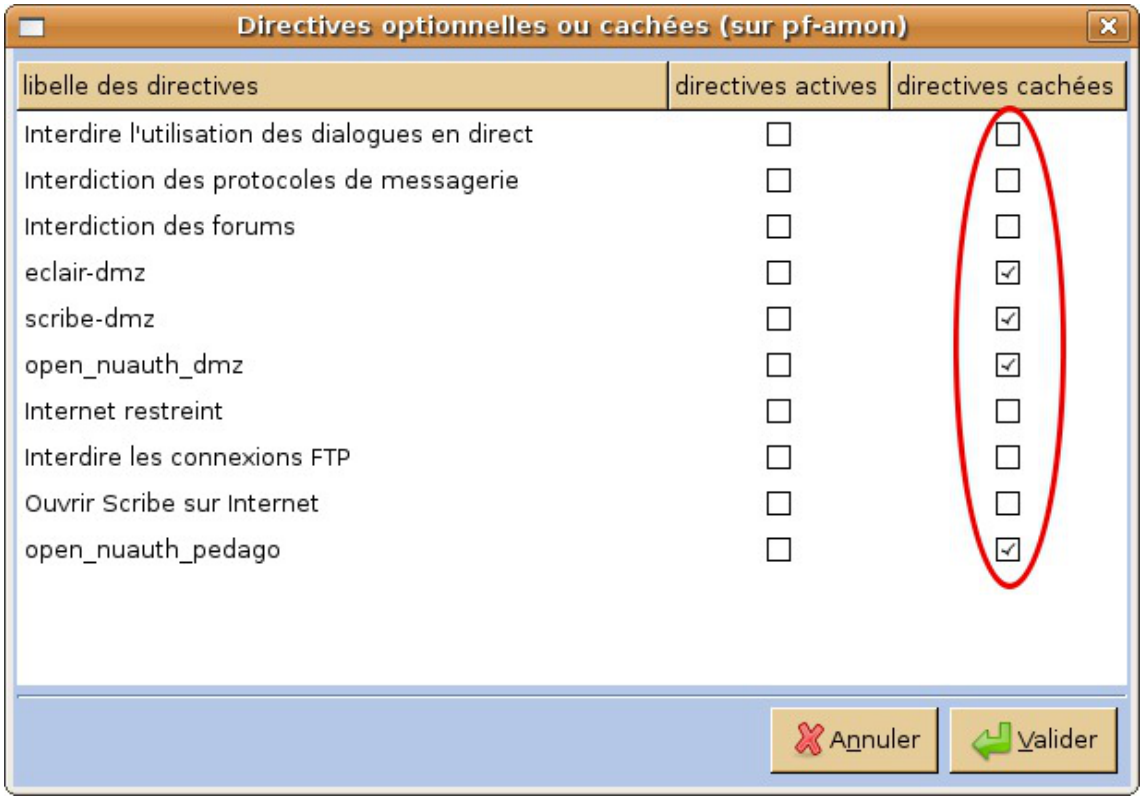
Dans le cas de l'activation/désactivation d'une directive optionnelle, il faut bien comprendre que c'est l'EAD qui prime par rapport à ERA. À la première instanciation du serveur, ERA détermine si la directive optionnelle est active ou inactive, mais une fois le serveur est instancié c'est depuis l'interface 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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Les 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.488]

Le format XML interne [p.546]

4.2.4. La qualité de service

La qualité de service ne concerne que les flux des zones internes vers l'extérieur. C'est une QOS[p.728] *externe*.

Le qualité de service est un système de **minimum garanti**.

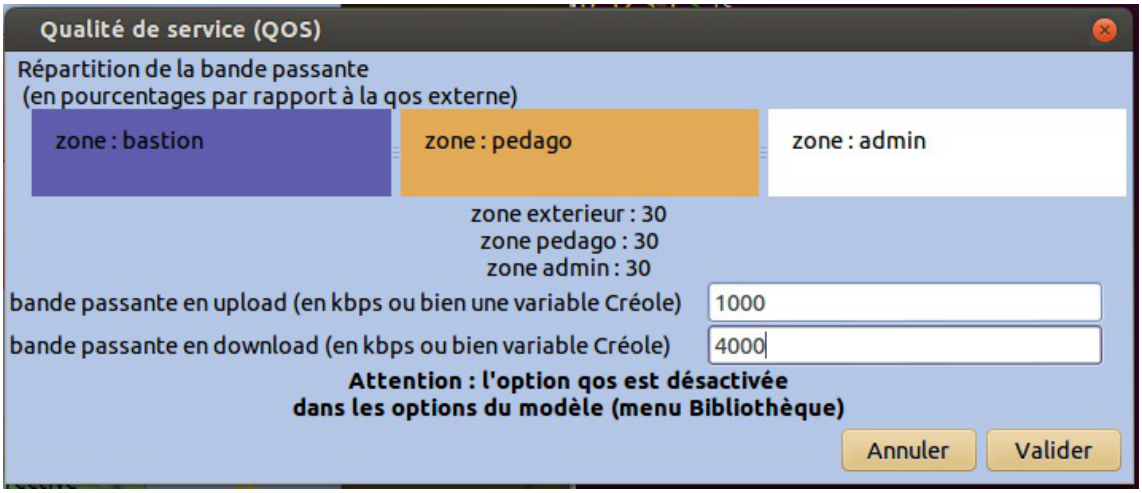
Elle n'entraîne pas de sous-utilisation de la bande passante, car si une zone n'atteint pas son minimum d'utilisation, ce qui reste est réparti dynamiquement entre les autres zones.

Il est possible d'accéder à la fenêtre de gestion de la QOS[p.728] de deux manières :

- depuis le menu `Bibliothèque` / `Qualité de service (QOS)` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- en cliquant sur la zone *Extérieur* depuis le tableau des flux.



Gestion de la Qualité de Service

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

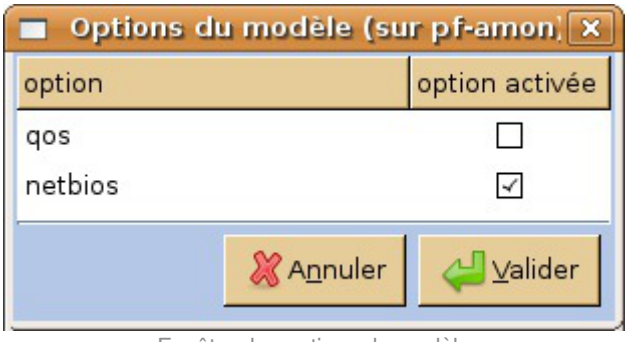
La QOS peut être définie dans un modèle sans être activée !

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.

4.2.5. 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Activer netbios permet d'ajouter des règles permettant de bloquer les requêtes du réseau Microsoft vers l'extérieur. Cette règle est activée par défaut.

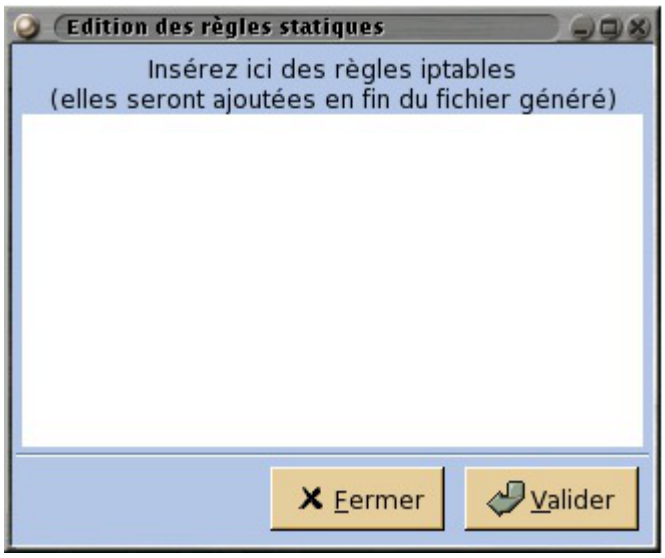
Si vous voulez utiliser les règles de Qualité de Service (QOS), il est indispensable de l'activer dans cette fenêtre. Par défaut, les règles de QOS ne sont pas actives.

4.2.6. L'inclusion statique

Il est possible d'ajouter des règles iptables personnalisées. Ces règles peuvent utiliser des variables Creole[p.708].

On accède à la fenêtre des inclusions statiques par le menu `Bibliothèque` / `Inclusion Statique`.

Il s'agit d'une zone de saisie de texte. Ces règles seront exécutées en dernier.



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.

Les règles statiques obtenues après traitement sont consultables dans le script dédié : `/etc/eole/inclusion_statique`.

4.2.7. 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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

4.2.8. Communication avec Zéphir

La connexion au Zéphir est possible depuis le menu `Zephir`.



Connexion à Zéphir

Sur les versions récentes d'EOLE, du fait des vérifications ajoutées au niveau des certificats, il n'est plus possible d'utiliser directement l'adresse IP du serveur Zéphir.

Importer un modèle

ERA intègre la possibilité d'échanger des modèles avec un serveur Zéphir.

Lors du 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

4.3. Directives optionnelles ERA depuis l'EAD

Les modèles de pare-feu ERA peuvent contenir des directives optionnelles[p.709].

Une règle peut être :

- générale, si elle concerne uniquement l'interface externe ;
- spécifique à une zone de configuration, si elle concerne une interface interne de la zone, dans ce cas, elle apparaîtra dans les règles du filtre web auquel est rattaché l'interface source de la directive.

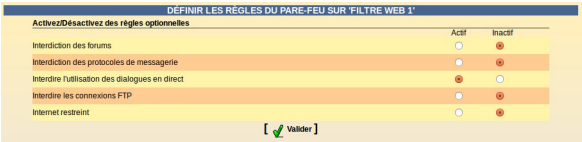
La configuration générale est accessible par le menu EAD : `Configuration générale` / `Règles du pare-feu`.

La configuration spécifique est accessible par le menu EAD : `Filtre web X` / `Règles du pare-feu` :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Pour valider une directive optionnelle :

- choisir Actif ;
- valider.



Activation des directives optionnelles dans l'EAD

Les directives optionnelles activées/désactivées dans l'EAD sont enregistrées dans le fichier : /var/lib/eole/config/regles.csv

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.538]

4.4. Compléments techniques

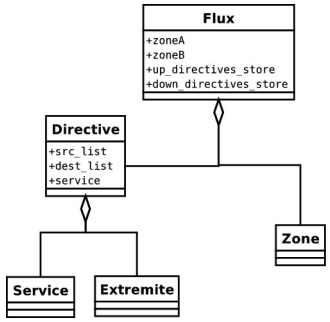
4.4.1. Le format XML interne

Les composantes 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 :



La représentation interne (objets)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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"
```

4.4.2. Comportement du Backend

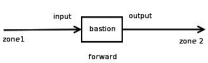
Règles implicites : le REDIRECT

Un redirect doit inclure aussi une chaine input chaine xxx-bas. A une règle de forward vient donc se greffer une règle de type input.



règles implicites : le redirect

Il y a une règle de forward (une redirection) :



La règle de forward

la chaine input qui vient se greffer sur le redirect (sur le forward) est implicite.un forward z1->z2 doublé

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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).

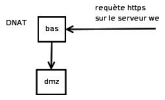
Règles implicites : Le DNAT et le SNAT

Lors d'un DNAT, une règle de type input est doublée d'un forward (elle s'ajoute à un FORWARD).

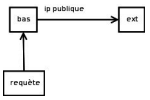
Même chose pour le masque de SNAT.

Exemple : un serveur de la DMZ répond à une requête sur le port 80 du bastion.

Un INPUT est transformé en FORWARD.



requête de DNAT



Une règle de type SNAT

Un poste de travail peut surfer sur le web avec l'IP publique du bastion. Cela permet de surfer masqué.

4.4.3. 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 au 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.

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 du compilateur en ligne de commande

Aller dans le répertoire `/usr/share` et exécuter le compilateur avec un fichier de modèle de pare-feu adapté :

```
root@amon:/usr/share# ./era/backend/compiler --help
Usage:
Script de generation de regles iptables a partir d'un modele ERA.

```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
5 compiler [options] era_model_file.xml
```

Par exemple :

```
root@amon:/usr/share# ./era/backend/compiler era/modeles/3zones.xml
```

Différentes options sont possibles, taper `--help` pour les détails ou consulter le fichier `/usr/share/era/bastion.sh` qui correspond à ce qui est exécuté par le service **bastion**.

4.5. Quelques références

- Site officiel EOLE (présentation, téléchargement) : https://pcll.ac-dijon.fr/eole/
- Code source du logiciel (versions, branches, tags) : https://dev-eole.ac-dijon.fr/projects/era/repository
- Conteneurisation : https://gitlab.mim-libre.fr/EOLE/eole-2/era/
- Images de conteneur : https://hub.eole.education/harbor/projects/7/repositories/era

5. Gestion des tunnels : RVP

Pré-requis

Le réseau virtuel privé (RVP)[p.728] 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.

ARV[p.704] 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.



On ne peut pas utiliser le logiciel ARV d'un Sphynx 2.6 ou inférieur pour générer des configurations IPSec d'Amon 2.7/2.8.

Il faut obligatoirement générer les configurations IPSec d'un Amon 2.8 à partir du logiciel ARV d'un Sphynx 2.7 ou 2.8.

Toutefois, si vous utilisez les fonctionnalités de Zéphir, il faudra un serveur Sphynx 2.8 pour importer/générer/diffuser les configurations serveurs et VPN.

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` ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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...

Commandes

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`.

Gestion du service

Les opérations du service *rvp* ont été intégrées dans le service *strongswan*, il faut donc l'utiliser en remplacement :

```
root@amon:~# service strongswan start
```

et

```
root@amon:~# service strongswan stop
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

6. Résoudre des dysfonctionnements liés au MTU

Le PMTUd (Path MTU[p.721] discovery), activé par défaut sur les modules EOLE, est une technique permettant de déterminer, dans un réseau informatique, la taille du MTU[p.721] 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.715] de type 3 (Destination Unreachable) / code 4 (Fragmentation Needed and Don't Fragment was Set) sont bloqués quelque part sur le réseau.

Un des phénomènes permettant de diagnostiquer un problème lié au PMTUd est l'accès à certains sites (ou certaines pages d'un site) n'aboutissant pas (la page reste blanche) ou les courriels n'arrivant pas dans le client de messagerie.

Il est possible de forcer la valeur du MTU pour une interface donnée dans l'onglet `Réseau avancé` de l'interface de configuration du module en mode expert.



Les commandes `ping`, `ip route` et `tracepath` sont utilisées pour ajuster les valeurs.

Utilisation de la commande `ping`

La commande `ping` permet de réaliser des tests en forçant la taille des paquets :

- ping OK avec une taille forcée à la valeur 1400 :

```
root@amon:~#  ping -M do -s 1400 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1400(1428) bytes of data.
1408 bytes from platon.ac-dijon.fr (194.167.18.17): icmp_seq=1 ttl=62 time=1.38 ms

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.380/1.380/1.380/0.000 ms
```

- ping KO avec une taille forcée à la valeur 1500 :

```
root@amon:~#  ping -M do -s 1500 pcll.ac-dijon.fr -c1
PING listeseole.ac-dijon.fr (194.167.18.17) 1500(1528) bytes of data.
ping: local error: Message too long, mtu=1500

--- listeseole.ac-dijon.fr ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Utilisation de la commande `ip route`

La commande `ip route get to` permet de visualiser les problèmes de MTU.

```
# ip route get to 172.X.Y.Z
172.X.Y.Z dev eth0 src 10.67.V.W
cache expires 508sec mtu 1400
```

La commande `ip route flush cache` permet quant à elle de vider le cache.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Utilisation de la commande `tracepath`

La commande `tracepath` permet d'identifier où se trouvent les limitations du MTU.

```
# tracepath 172.X.Y.Z
1?: [LOCALHOST] pmtu 1500
1?: [LOCALHOST] pmtu 1438
1: 192.168.A.B 1.353ms
1: 192.168.C.D 1.972ms
2: 192.168.E.F 2.014ms
3: 192.168.G.H 1.657ms
4: 192.168.I.J 3.026ms
5: 192.168.K.L 2.543ms pmtu 1400
5: 172.M.N.O 9.930ms
6: no reply
...
```

Voir aussi...

Onglet Réseau avancé [p.228]

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 9

Paramétrage des postes client

1. Authentification NTLM/SMB hors domaine

À partir d'EOLE 2.8.1, lorsque l'authentification est configurée en mode `NTLM/KERBEROS`, les postes hors domaine peuvent utiliser directement le proxy authentifié.

La mise en œuvre du proxy NTLM n'est donc plus utile dans cette version.

Voir aussi...

Configurer la découverte automatique du proxy avec WPAD [p.348]

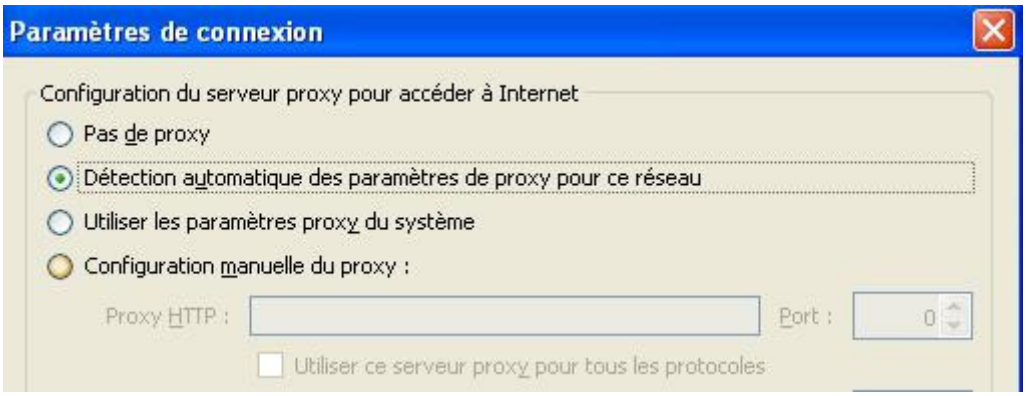
Onglet Proxy authentifié : 4 méthodes d'authentification [p.300]

2. Configurer la découverte automatique du proxy avec WPAD

WPAD[p.734] est un protocole qui permet la découverte automatique du proxy par les navigateurs.

Le principe est simple, si le navigateur est configuré pour détecter automatiquement la configuration du proxy, il essayera de télécharger le fichier : `wpad.<domaine local>/wpad.dat` ou le fichier `proxy.pac`.

Configuration côté client



Détection automatique du proxy dans Firefox

Par défaut, les adresses pour lesquelles le proxy ne sera pas utilisé sont : 127.0.0.1 et le réseau local.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La détection automatique du proxy par les navigateurs peut notamment être imposée par GPO[p.713].

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.722] 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.

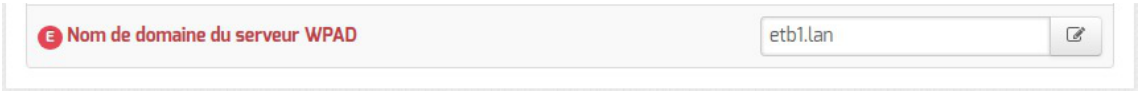
Configuration sur le module Scribe

Le serveur DHCP doit être activé et correctement configuré sur le module Scribe (ou AmonEcole).

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 utilisée pour accéder au fichier WPAD tandis que pour des postes de travail GNU/Linux c'est le nom de domaine local qui sera utilisé pour accéder au fichier WPAD.



Dans l'interface de configuration du module, en mode expert, il faut saisir dans le `Nom de domaine du serveur WPAD` de l'onglet `Dhcp` la même valeur que celle du champ `Nom de domaine privé du réseau local` de l'onglet `Général`.

Pour être pris en compte, les changements doivent être enregistrés et suivis de la commande `reconfigure` sur le module.

Configuration sur le module Amon

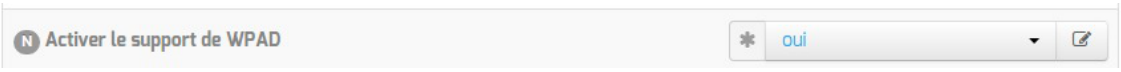
WPAD est mis à disposition sur les modules Amon et AmonEcole au travers du paquet `eole-wpad`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Sur un module personnalisé, il n'est fonctionnel que si le paquet `eole-proxy` est installé.

Pour fonctionner correctement, il faut que l'URL `wpad.<nom domaine local>` correspondre à l'adresse IP du serveur web.

Le support de WPAD doit être activé et correctement configuré sur le module Amon.



Activation de WPAD dans l'onglet Services

Dans l'onglet `Services` de l'interface de configuration du module `Activer le support de WPAD` doit être placé à `oui`.



Vue de l'onglet Wpad dans l'interface de configuration du module

Cela rend disponible l'onglet `Wpad` au sein duquel le `Nom de domaine du service WPAD` doit être rempli avec la même valeur que le `Nom de domaine privé du réseau local` présent dans l'onglet `Général`.

Si vous souhaitez utiliser un autre nom de domaine qui ne correspondrait pas au `Nom de domaine privé du réseau local` de l'onglet `Général`, il faut le déclarer dans le champ `Nom domaine local supplémentaire ou rien` de l'onglet `Zones-dns`.

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

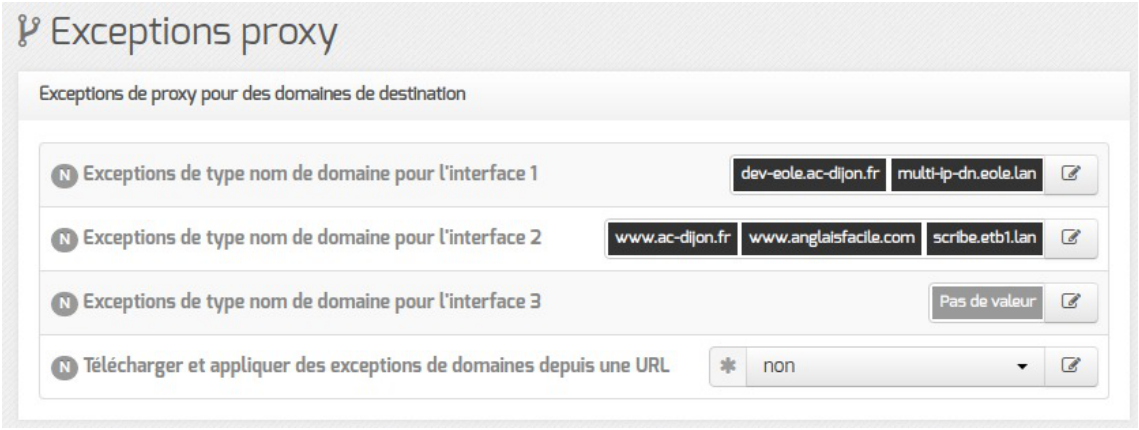
Dans l'onglet `Exceptions proxy` de l'interface de configuration du module il est possible d'ajouter des exclusions dans la configuration automatique du proxy.

Il est possible de déclarer différents types d'exceptions.

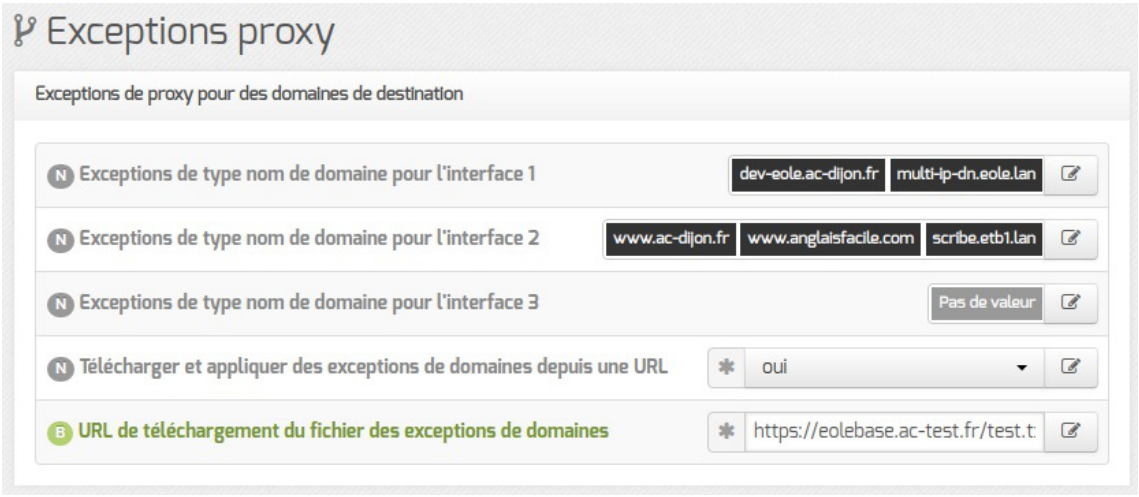
Exception de proxy pour des domaines de destination

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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



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



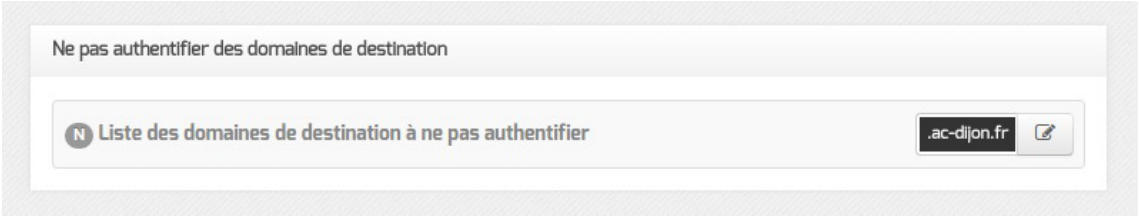
Il est également possible de fournir une liste de noms de domaine ou d'IP à inclure dans les exceptions au proxy depuis une URL, en activant la variable `Télécharger et appliquer des exceptions de domaine depuis une URL`.



Si vous utilisez une copie des modèles ERA fournis, il faudra l'adapter pour obtenir les règles supplémentaires

Exception au niveau de l'authentification des domaines de destination

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



Si WPAD est activés sur l'interface réseau, les utilisateurs utiliseront directement Squid pour accéder à ces sites.

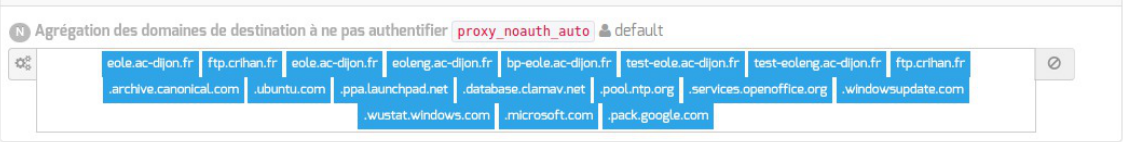
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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`.

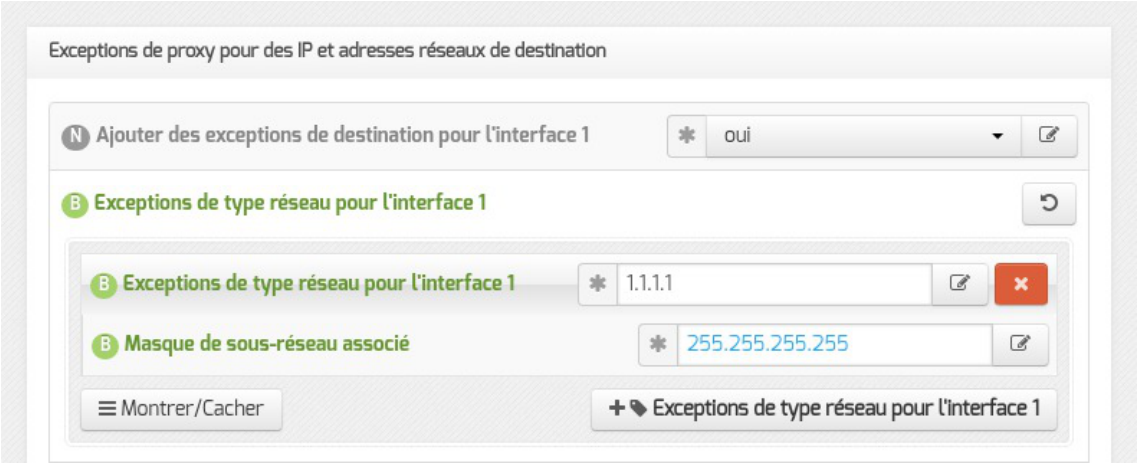
Il est possible de l'afficher dans l'onglet `Exceptions proxy` de l'interface de configuration du module en activant le mode Debug.



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

Exceptions de proxy pour des IP et adresses réseaux de destination

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.

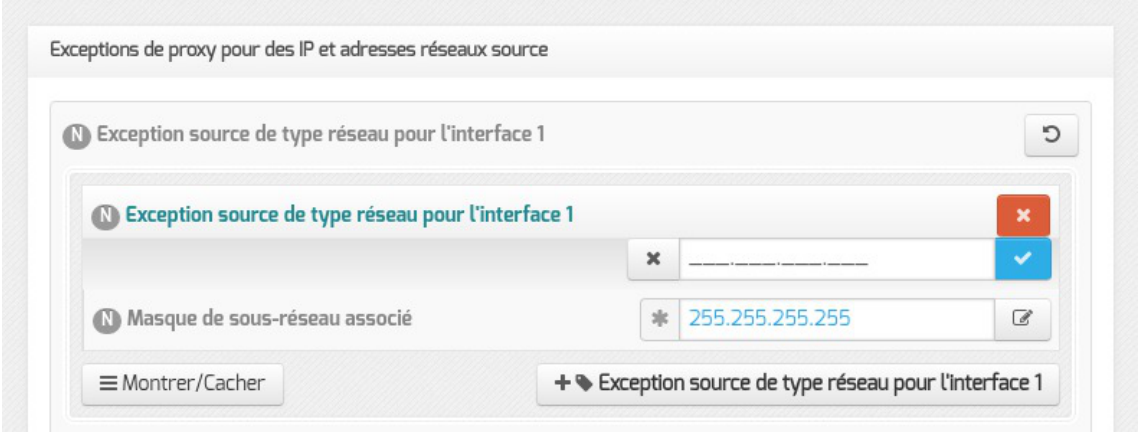


Le bouton `Exceptions de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.

Exceptions de proxy pour des IP et adresses réseaux source

Cette exception spécifique à ERA permet de déclarer une adresse IP ou une plage d'adresses IP **source** pour laquelle on ne passe pas par le proxy.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

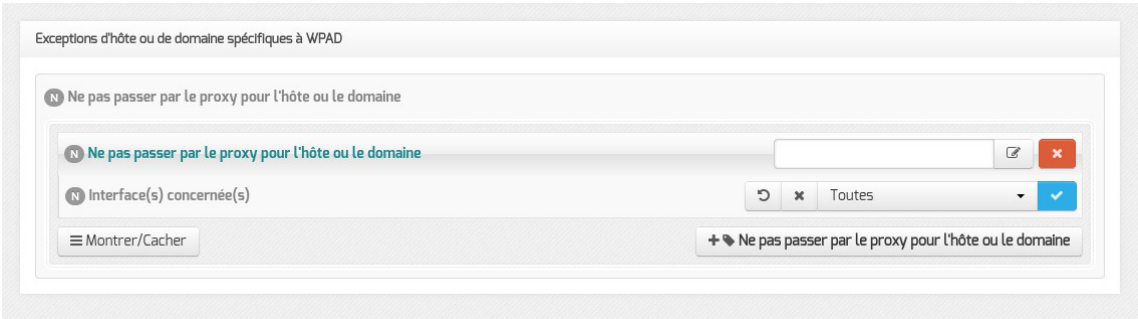


Le bouton `+ Exception source de type réseau pour l'interface n` permet d'ajouter plusieurs exceptions sur une même interface.

Cette fonctionnalité permet à une machine de contourner le proxy ce qui constitue un non respect des règles légales de sécurité. Elle peut servir pour effectuer des tests de proxy et d'exceptions de filtrage.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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

3. Proxy non configuré dans le navigateur : redirection ou page d'information

Redirection transparente HTTP sur Amon

À partir d'EOLE 2.6, la redirection transparente HTTP est remplacée par une redirection vers une page d'information proposée par Nginx.

> Techniquement, cela se traduit par le remplacement de la redirection des accès directs HTTP (port 80) vers le proxy local (port 3128) par une redirection vers une adresse dédiée (port 81) dans les modèles ERA. On retrouve ainsi le même fonctionnement que pour la navigation HTTPS.

> Dans l'onglet `Exceptions proxy` de l'interface de configuration du module, il est possible de déclarer des adresses de destination qui ne passeront pas par 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. La page Nginx est également affichée également si la requête initiale est en HTTPS.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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
```

```
root@amon:~# cp /usr/share/eole/creole/distrib/nginx.no_proxy.html
  /usr/share/eole/creole/modif/nginx.no_proxy.html
root@amon:~# vim /usr/share/eole/creole/modif/nginx.no_proxy.html
[...]
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
root@amon:~# gen_patch

** Génération des patches à partir de modif **

Génération du patch nginx.no_proxy.html.patch

** Fin de la génération des patch **

root@amon:~# ls /usr/share/eole/creole/patch/
nginx.no_proxy.html.patch  variante
root@amon:~# reconfigure
[...]
root@amon:~# vim /var/www/index.html
```

Il est possible d'appeler des variables Creole comme par exemple `%%libelle_etab` et aussi d'ajouter des images en les ajoutant par exemple dans un dossier `/img` dans `/var/www/`.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
    <META http-equiv="Content-Type" content="text/html; charset=utf-8;">
    <head>
<title>Veuillez configurer le proxy de votre navigateur</title>
<style>
.main {
        background:#bbbbbb;
        text-align:center;
}
h1 {
    /* text-shadow: 0px 0px 7px rgba(0, 0, 0, 0.75);*/
    color: #91e842;
    font-size: 50px;
    text-align:center;
    text-shadow: 0 1px 0 #eee,
              0 2px 0 #e5e5e5,
              -1px 3px 0 #C8C8C8,
              -1px 4px 0 #C1C1C1,
              -2px 5px 0 #B9B9B9,
              -2px 6px 0 #B2B2B2,
              -2px 7px 2px rgba(0,0,0, 0.6),
              -2px 7px 8px rgba(0,0,0, 0.2),
              -2px 7px 45px rgba(0,0,0, 0.4);
}
.message {
    top:25%;
    text-align:center;
    margin-left: 50px;
    margin-right: 50px;

    padding: 40px;
    background: #d2ff52;
    border: 1px solid #000000;

    border-radius: 10px;
    -moz-border-radius: 10px;
    -webkit-border-radius: 10px;

    box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
    -moz-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
    -webkit-box-shadow: 5px 7px 10px 6px rgba(119, 119, 119, 0.75);
}
</style>
    </head>
    <body class='main'>
    <img src="./img/logoEolePt.png">
    <h1>%%libelle_etab</h1>
    <h2>Votre navigateur n'est pas correctement configuré !!</h2>
    <div class="message">Pour naviguer sur internet, un proxy doit être déclaré dans votre navigateur.<br />
Si vous accédez à la présente page, c'est que votre navigateur n'est pas configuré pour utiliser le proxy. Veuillez contacter le service informatique de l'établissement.</div>
    </body>
</html>

```



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`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 du module AmonEcole, l'adresse du proxy sera l'adresse IP réservée pour le proxy sur le réseau local de la structure. Le port sera celui de e2guardian (`3128` par défaut), ce qui donne par exemple :

- proxy sur le réseau local 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`). Par contre pour le DNS, il faut utiliser la même adresse IP que celle du proxy.

Double authentification

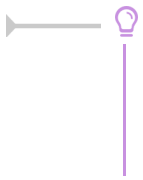
Si la double authentification est configurée, le port à utiliser pour le second proxy sera le porte d'écoute de la troisième configuration e2guardian, le port d'écoute pour le 3ème filtre web, (`3129` par défaut), ce qui donne par exemple :

- proxy2 sur le réseau eth1 Amon : `adresse ip eth1:3129`
- proxy2 sur le réseau local 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) ;



À partir d'EOLE 2.8.1, lorsque l'authentification est configurée en mode `NTLM/KERBEROS`, les postes hors domaine peuvent utiliser directement le proxy authentifié.

La mise en œuvre du proxy NTLM n'est donc plus utile dans cette version.

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 par défaut sur le port 3129, port d'écoute de la seconde instance de Squid.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 10

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 complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. Services liés aux bases de données

1.1.1. eole-annuaire

Le paquet `eole-annuaire` permet la mise en place d'un service d'annuaire 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, AmonEcole, 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)`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Sur le module AmonEcole, 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, WordPress, Cdt...).

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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.1.4. eole-interbase

Le paquet `eole-interbase` permet la mise en place d'un serveur de base de données Interbase[p.716].

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)`.
En mode conteneur, 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[p.721].

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 le module AmonEcole, 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 [p.727].

Logiciels et services

Le paquet `eole-postgresql` s'appuie principalement sur le service postgresql.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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-ad-dc

Le paquet `eole-ad-dc` permet la mise en place d'un serveur Samba Active Directory[p.702] pouvant être soit contrôleur de domaine, soit membre d'un domaine existant.

Logiciels et services

Le paquet `eole-ad-dc` permet de gérer les services suivants :

- samba-ad-dc en mode contrôleur de domaine ;
- smbd, nmbd et winbind en mode serveur membre.

http://www.samba.org/

Historique

Le service a été créé spécifiquement pour le nouveau module 2.6 nommé Seth.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.2.2. eole-fichier-primaire

Le paquet `eole-fichie-primaire` permet la mise en place d'un serveur de fichiers PDC[p.726] complet.

Logiciels et services

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le paquet `eole-fichie-primaire` permet de gérer les services suivants :

- smbd, nmbd (serveur de fichiers) ;
- nscd (cache) ou winbind.

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 le module AmonEcole, 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`).

1.2.3. eole-cups

Le paquet `eole-cups` permet la mise en place d'un serveur d'impression.

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 le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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[p.712].

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 le module AmonEcole, 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[p.708] local et/ou d'un serveur PXE[p.728].

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 (modules Scribe et Horus) ainsi que sur le serveur de clients légers Eclair, ceci avec des configurations hétérogènes et très limitées.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 le module AmonEcole, il est installé dans le groupe de conteneurs : `partage (id=52)`.

Remarques

Ne pas confondre ce paquet avec le paquet `eole-dhcrelay` qui est pré-installé sur le module Amon.

1.2.6. Partages avec NFS

Historiquement, le paquet `eole-nfs` a été créé pour les besoins du serveur de clients légers Eclair.

Mais, le partage de fichiers NFS[p.722] proposé peut être mis en œuvre pour d'autres besoins (sauvegarde, partage de données, ...).

Configuration du partage de fichiers sur le module Scribe

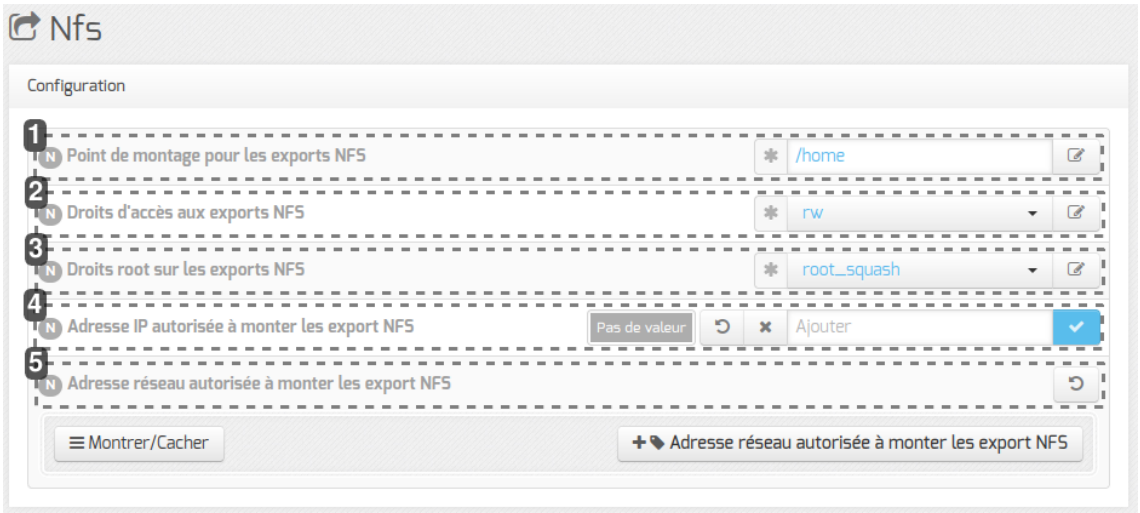
Sur le module, il faut installer le paquet `eole-nfs` :

```
# apt-eole install eole-nfs
```

L'installation du paquet ajoute :

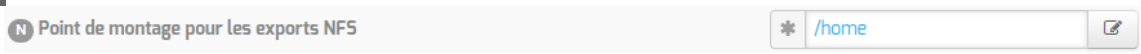
- un nouveau service dans l'onglet `Services` de l'interface de configuration du module : `Activer le serveur NFS` est par défaut à `oui`
- un nouvel onglet nommé `Nfs`

Il faut ensuite autoriser le serveur de clients légers ou les clients à monter les export NFS du module. Pour cela, se rendre dans l'interface de configuration du module, dans l'onglet `Nfs` et saisir l'adresse IP (Interface-0) du serveur cible ou les adresses des clients GNU/Linux dans le champ `Adresse IP autorisée à monter les exports NFS`.



Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1



Point de montage

Indiquer le chemin du point de montage pour les exports NFS

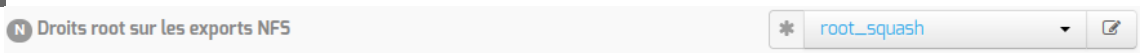
2



Droits d'accès

Choix des droits d'accès (ro ou rw) sur les exports NFS

3



Droits root

Autoriser ou non l'utilisateur distant à être root sur le serveur dans le partage NFS.

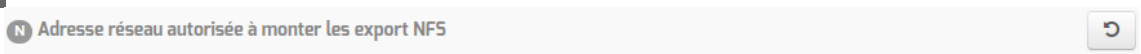
4



Adresse IP autorisée

Indiquer une ou plusieurs adresses IP de postes ou serveurs distants autorisées à monter les export NFS

5



Adresse réseau autorisée

Indiquer un ou plusieurs réseaux autorisés à monter les export NFS



Si vous n'indiquez pas d'adresse IP, ou de réseau autorisé pour le montage des exports NFS, la configuration ne sera pas effective.

Il faut ensuite procéder à la reconfiguration du module avec la commande `reconfigure`.

Test manuel de montage sur Scribe

Pour le support du système de fichiers NFS sur le client il faut installer le paquet `nfs-common` :

```
# apt-get install nfs-common
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

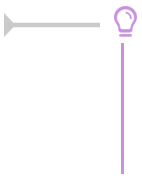
Pour tester la prise en charge il est possible de procéder à un montage manuelle d'une partition distante :

```
# mdkir /mnt/montage
```

```
# mount -t nfs -o auto,nouser,rsize=8192,wsize=8192,timeo=14,intr,acl,nolock,async scribe:/home/ /mnt/montage
```

Pour démonter la partition :

```
# umount /mnt/montage
```



Si le test de montage renvoie la ligne suivante c'est qu'il faut autoriser l'adresse IP du client dans l'onglet Nfs du module Scribe :

```
mount.nfs: access denied by server while mounting scribe:/home/
```

Configuration pour le montage à la connexion

Pour permettre à PAM de monter des volumes pour une session utilisateur il faut installer la bibliothèque libpam-mount :

```
root@pclinux:/home/eole# apt-get install libpam-mount
```

1.3. Services liés au 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 les applications phpMyAdmin ou Adminer (selon les versions d'EOLE).

http://www.phpmyadmin.net/

https://www.adminer.org/

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le service est configuré pour s'installer dans le conteneur : `web (id=15)`.

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `reseau (id=51)`.

Remarques

Ce paquet sert de brique de base pour toutes les applications web empaquetées 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.722], peut également faire office de serveur web.

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Initialement conçu pour les modules Amon et AmonEcole, ce service est pré-installé sur tous les modules à partir de la version 2.6.1 d'EOLE.

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.734]).

Le logiciel utilisé, Nginx[p.722], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Ce service étaient auparavant inclus dans le paquet `eole-reverseproxy`. Il peut désormais être

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

installé de façon indépendante.
Le paquet `eole-wpad` est pré-installé sur les modules Amon et AmonEcole.

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[p.731] Exim[p.711].

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, 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Conteneurs

Le service est configuré pour s'installer dans le conteneur : `mail (id=13)`.
Sur le module 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[p.727] / IMAP[p.715].

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 le module 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.
L'accès au service IMAP peut être facilité par la mise en œuvre de la messagerie web Roundcube.

Voir aussi...

> Roundcube : interface pour le courrier électronique

1.4.4. eole-sympa

Le paquet `eole-sympa` permet la mise en place d'un serveur de listes de diffusion.

Logiciels et services

Le paquet `eole-sympa` s'appuie principalement sur le service sympa.
Son interface d'administration nécessite un serveur web apache2.

http://www.sympa.org/

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 le module AmonEcole, ils sont installés dans le groupe de conteneurs : `reseau (id=51)`.

1.5. Services liés au proxy et à l'authentification

1.5.1. eole-proxy

Le paquet `eole-proxy` permet la mise en place d'un serveur proxy complet.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les logiciels et services suivants :

- Squid[p.731] : proxy cache ;
- e2guardian[p.710] : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM[p.723] ou Kerberos[p.717].

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 le module AmonEcole, 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Afin d'assurer les authentifications 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.728].

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 système hôte (maître).

1.6. Services liés à la virtualisation

1.6.1. eole-libvirt

Le paquet `eole-libvirt` permet la mise en place de la gestion de la virtualisation.

Logiciels et services

Le paquet `eole-libvirt` s'appuie sur le service libvirt[p.718].

http://libvirt.org/

Historique

Utilisé à la base sur les modules Hâpy et Hâpy Node, le paquet `eole-libvirt` est installable sur n'importe quel module EOLE.

Conteneurs

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le service s'installe sur le système hôte (maître).

1.6.2. eole-one-frontend

Le paquet `eole-one-frontend` permet la mise en place de l'interface de gestion des machines virtuelles, OpenNebula Sunstone[p.732].

Logiciels et services

Le paquet `eole-one-frontend` s'appuie sur le service opennebula-sunstone.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy , le paquet `eole-one-frontend` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.6.3. eole-one-node

Le paquet `eole-one-node` permet la mise en place de la gestion d'un nœud de calcul (nœud de travail).

Logiciels et services

Le paquet `eole-one-node` s'appuie sur le service opennebula-node.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy et Hâpy Node, le paquet `eole-one-node` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.6.4. eole-one-singlenode

Le paquet `eole-one-singlenode` permet la mise en place de l'interface de gestion des machines virtuelles.

Logiciels et services

Le paquet `eole-one-singlenode` s'appuie sur le service opennebula-node.

http://opennebula.org/

Historique

Utilisé à la base sur les modules Hâpy , le paquet `eole-one-singlenode` est installable sur n'importe quel module EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7. Autres services réseau

1.7.1. 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 et clamav-freshclam.

http://www.clamav.net/

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 le module AmonEcole, le service clamav-daemon est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.

C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>eole-antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.7.2. 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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.7.3. eole-bareos

Le paquet `eole-bareos` permet d'installer et de configurer la solution de sauvegarde Bareos[p.704].

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).

1.7.4. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS[p.709] local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.705].

http://www.isc.org/downloads/bind/

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)`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Sur le module AmonEcole, il est installé dans le groupe de conteneurs : `internet (id=53)`.

1.7.5. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP[p.708].

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 système hôte (maître).

1.7.6. eole-ltsp-server

Le paquet `eole-ltsp-server` permet la mise en place d'un serveur de clients légers LTSP[p.727].

Logiciels et services

Le paquet `eole-ltsp-server` s'appuie sur les service NBD[p.722] et LDM[p.717].

http://ltsp.org/

Historique

Ce paquet, initialement conçu pour le module Eclair 2.3 intègre désormais les fonctionnalités apportées par l'ancien paquet `eole-ltsp-fichier`.

Conteneurs

Contrairement à la version proposée sur EOLE 2.3, le service s'installe sur le système hôte (maître).

1.7.7. eole-nut

Le paquet `eole-nut` permet la mise en place de la gestion des onduleurs.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.8. eole-open-iscsi

Le paquet `eole-open-iscsi` permet de mettre en œuvre l'accès à un réseau de stockage SAN[p.730].

Logiciels et services

Le paquet `eole-open-iscsi` s'appuie sur les services open-iscsi et multipath.

http://www.open-iscsi.com

Historique

Ce service n'est pré-installé sur aucun module.

Initié grâce à une contribution de Karim Ayari de l'académie de Lyon, a été repris par l'équipe EOLE pour répondre à des besoins exprimés par le ministère de l'écologie.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.9. eole-pacemaker

Le paquet `eole-pacemaker` permet la mise en place d'un service de haute disponibilité[p.714].

Logiciels et services

Le paquet `eole-pacemaker` s'appuie principalement sur le service Corosync[p.707].

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

http://clusterlabs.org/

Historique

A la base, le service de haute disponibilité était uniquement disponible sur le module Sphynx via le service Heartbeat. Celui-ci se fait maintenant via les logiciels Corosync et Pacemaker. Le service a été adapté afin d'être installé sur n'importe quel module EOLE, y compris en *mode une carte*.

Conteneurs

Le service s'installe sur le système hôte (maître).

1.7.10. eole-snmpd

Le paquet `eole-snmpd` permet d'installer et de configurer un serveur SNMP[p.731].

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 système hôte (maître).

1.7.11. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN[p.728].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.732].

http://www.strongswan.org/

Historique

Ce paquet est pré-installé sur les modules Amon et AmonEcole ainsi que sur le module Sphynx.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Conteneurs

Le service s'installe sur le serveur maître.

2. Personnalisation du serveur à l'aide de Creole

Creole[p.708] 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.726]** : permet de modifier un template[p.733] fourni par EOLE ;
- le **dictionnaire[p.709] 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.733] 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `/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/` : librairies 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
[…]
```



Le nom du patch doit impérativement être celui du nom du fichier template à modifier suivi de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

l'extension `.pacth`.

Exemple : `smb.conf.patch`

Sont concernés par la procédure de patch uniquement les fichiers déjà présents dans le répertoire des templates et référencés dans les dictionnaires fournis par l'équipe EOLE.

Pour les autres fichiers, l'utilisation de dictionnaires locaux et de templates personnalisés est recommandée.

Le répertoire `/usr/share/eole/creole/` contient les répertoires suivants :

- **./distrib/** : templates originaux fournis principalement par le paquet conf d'un module ;
- **./modif/** : endroit où doivent être copiés et modifiés les templates souhaités ;
- **./patch/** : fichiers patch générés à partir des différences entre les deux répertoires précédents.

Le répertoire `/var/lib/creole/` comprend les templates finaux, c'est à dire les templates initiaux avec éventuellement des patchs.

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 susceptible 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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.733] 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.709] :
> 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.375]

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

```
<creole>
    <files>
    </files>
    <containers>
        <all>
            <host hostlist='web' name='web_url' ip='adresse_ip_br0' instance_mode='when_container' comment="Serveur web sur l'IP de l'interface 0" />
            <file filename='/etc/fichier_cible' instance_mode='when_container' />
        </all>
        <container name='web' id='15'>
            [...]
        </container>
        <container name='reseau' id='51'/>
        <!-- affectation du conteneur web au groupe de conteneurs reseau -->
        <container name='web' group='reseau'/>
    </containers>
    [...]
```

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>**.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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'appeller 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 **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 les services : systemd (par défaut), apache et restartonly ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 **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).

Gestion des services

`systemd` est, dorénavant, la seule méthode valide pour la gestion des services Linux.

À partir d'EOLE 2.7.2, la méthode `restartonly` a été introduite afin de redémarrer les services de base qui nécessitent une continuité, tels que networkd, rsyslog, ssh, cron...

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) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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>squid</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 optionnel **mount_point** permet de définir le point de montage à l'intérieur du conteneur, par défaut c'est la valeur de l'attribut **name** ;
- si l'attribut **mount_point_type** vaut SymLinkOption cela indique que le chemin sera défini dans la variable indiquée dans l'attribut **mount_point** ;
- l'attribut optionnel **options** permet de définir les options de montage ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.732] 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`s et `service restriction` doit être renseigné avec le nom de la `servicelist` associée

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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`

```
<service_access service='sshd'>
    <port>22</port>
    <tcpwrapper>sshd</tcpwrapper>
</service_access>
<service_restriction service='sshd'>
    <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
    <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
    <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
    <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
    <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
</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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`<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` (calcule 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`

```
<service_access service='genconfig'>
    <port>7000</port>
</service_access>
<service_restriction service='genconfig'>
    <ip interface='eth0' netmask='netmask_ssh_eth0' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth0</ip>
    <ip interface='eth1' netmask='netmask_ssh_eth1' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth1</ip>
    <ip interface='eth2' netmask='netmask_ssh_eth2' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth2</ip>
    <ip interface='eth3' netmask='netmask_ssh_eth3' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth3</ip>
    <ip interface='eth4' netmask='netmask_ssh_eth4' netmask_type='SymLinkOption' ip_type='SymLinkOption'>ip_ssh_eth4</ip>
</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	✓	

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

when_no_container		✓
always (default)	✓	✓

Les balises acceptant l'attribut instance_mode sont actuellement :

- package ;
- file ;
- service ;
- host ;
- fstab.

Exemple récapitulatif

Fichiers templates, paquets et services locaux ou dans un conteneur

```
<containers>
  <!-- dans le conteneur mon_reverseproxy -->
  <container name="mon_reverseproxy" id='101'>
    <package>nginx</package>
    <service servicelist="myrevprox">nginx</service>
    <file filelist='myrevprox' name='/etc/nginx/sites-enabled/default' source='nginx.default'/>
    <file filelist='myrevprox' name='/var/www/nginx-default/nginx.html' rm='True'/>
  </container>
</containers>
<files>
<!-- sur le maître-->
  <service>ntp</service>
  <file name='/etc/ntp.conf/>
  <file name='/etc/default/ntpdate' owner='ntp' group='ntp' mode='600'/>
  <file name='/etc/strange/host' source='strangehost.conf' mkdir='True'/>
</files>
```

Voir aussi...

Choisir le mode du module

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>

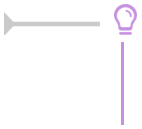
Un conteneur famille permet d'avoir des catégories de variables. Celle-ci correspond à un onglet dans l'interface. Les familles sont incluses obligatoirement dans une balise *<variables>*.

Une famille `Squid` pour gérer toutes les variables relatives a *Squid*.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 basique 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://fortawesome.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='envelope'>
<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 a 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*) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 ;
- 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 forcement 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 forcement être du type alpha. Le '.' est obligatoire. Minimum 2 et maximum 255 caractères ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- *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 forcement 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" ;
- *password* : la valeur de la variable est masquée dans l'interface une fois le champ validé. Elle est affichée en clair lorsque le champ est édité. Aucune contrainte n'est associée à ce type de variable.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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>
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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>* ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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.733] ;
- 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>
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- *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>
```

  Si l'une des valeurs passées à la fonction est vide, elle renverra une liste vide.

  À partir d'EOLE 2.6.2, il est possible de modifier ce comportement en ajoutant la balise suivante : `<param name='allow_none'>True</param>`.

- *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_calculee'>
    <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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.733] ;
- 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.

```
1 <check name="valid_ipnetmask" target="adresse_netmask_eth0" level=
  "warning">
2     <param type='eole'>adresse_ip_eth0</param>
3 </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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
<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 des règles de pare-feu (type='*service_accesslist*')
- d'activer/désactiver la templatisation de fichiers (*type='filelist'*)

en fonction d'un ensemble de conditions.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
<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>
```

La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la variable source est renseignée ou non.

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.

Gestion des variables inexistantes ou désactivées

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>
```

Désactivation de variables entre esclaves du même groupe

À partir de la version 2.6.1 d'EOLE, il est possible de gérer la désactivation d'une variable esclave en fonction de la valeur d'une autre variable esclave du même groupe.

Dans les versions précédentes, il était possible de désactiver totalement une variable esclave mais pas de le faire pour une seule de ses valeurs.

Dictionnaire avec conditions de désactivation entre variables esclaves

```
<?xml version="1.0" encoding="utf-8"?>
<creole>
    <files/>
    <variables>
        <family name='famille_demo'>
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
            <variable name='ma_master' type='string' description='Je suis une variable maitre' multi="True"/>
            <variable name='ma_slave1' type='oui/non' description='Je suis une variable esclave qui cache'>
                <value>oui</value>
            </variable>
            <variable name='ma_slave2' type='string' description='Je suis une variable esclave qui peut être caché'/>
            <variable name='ma_slave3' type='string' description='Je suis une variable esclave qui peut être caché aussi'/>
        </family>
    </variables>
    <constraints>
        <group master='ma_master'>
            <slave>ma_slave1</slave>
            <slave>ma_slave2</slave>
            <slave>ma_slave3</slave>
        </group>
        <condition name='disabled_if_in' source='ma_slave1'>
            <param>non</param>
            <target type='variable'>ma_slave2</target>
        </condition>
        <condition name='disabled_if_in' source='ma_slave1'>
            <param>oui</param>
            <target type='variable'>ma_slave3</target>
        </condition>
    </constraints>
    <help/>
</creole>
```

Template associé au dictionnaire

```
%for %%master in %%ma_master
pour %%master :
%if %%master.ma_slave1 == 'oui'
* ma_slave2 : %%master.ma_slave2
%else
* ma_slave3 : %%master.ma_slave3
%end if
%end for
```

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>
```

La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la variable source est renseignée ou non.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Gestion des variables inexistantes ou désactivées

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.

mandatory_if_in et mandatory_if_not_in

Les conditions *mandatory_if_in* et *mandatory_if_not_in* permettent passer une variable en mode obligatoire (une valeur doit être renseignée par l'utilisateur) en fonction d'un ensemble de conditions.

```
<condition name='mandatory_if_not_in' source='mode_zephir'>
    <param>non</param>
    <target type='variable'>nom_carte_eth0</target>
    <target type='variable'>nom_zone_eth0</target>
</condition>
```

La syntaxe `<param></param>` permet de mettre en place une condition sur le fait que la variable source est renseignée ou non.

Gestion des variables inexistantes ou désactivées

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.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
# -*- 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 importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptible 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 premiere 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`

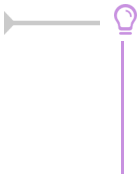
Et qu'on a dans un template source le contenu suivant :

```
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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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**.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



```
%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]
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
%end while
```

La déclaration repeat

Syntaxe : `%repeat EXPR`

```
%end repeat
```

La déclaration unless

```
%unless EXPR
%end unless
```

peut être utile si une variable est dans le dictionnaire Creole pour "'ne pas"' executer une action :

```
%unless %%alive
do this
%end unless
```

La syntaxe d'inclusion

il est possible d'inclure des fichiers à l'aide de la déclaration suivante :

```
%include "includeFileName.txt"
```

ou bien à partir du nom long du fichier à inclure (le nom de fichier étant ici renseigné dans une variable Creole :

```
%include source=%%myParseText
```

Effacement des retours chariots : slurp

Exemple d'utilisation :

```
%for %%i in range(15)
%%i-%slurp
%end for
```

donnera :

```
1-2-3-4-5-6...
```

sur une seule ligne (gobe les retours chariots)

remarquons que dans ce cas là, `slurp` n'est pas nécessaire et il est possible d'écrire le end sans sauter de ligne :

```
%for %%i in range(15)
%%i-%end for
```

exemple 2 :

```
%if %%dns_nameservers != ['']
dns_nameservers %slurp
%for %%name_server in %%dns_nameservers %%name_server %slurp
%end for
%end if
#
```

générera :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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]
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
%else
la variable est vide
%end if
```

Concaténation des éléments d'une liste : custom_join

La fonction `%%custom join` permet de concaténer facilement les éléments d'une variable multi-valuée.
Cela permet d'éviter le recours à une boucle `%for` et l'utilisation du l'instruction `%slurp` qui est souvent source d'erreurs.
Il est possible de spécifier le séparateur à utiliser en le passant comme paramètre à la fonction.
En l'absence de ce paramètre, le séparateur utilisé est l'espace.



```
%%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 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'
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
%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 in %%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_chaine)` ;
- encodage d'une chaîne en ISO-8859-1 (au lieu d'UTF-8) : `%%to_iso(%%ma_chaine)` ;
- transformation d'un masque réseau (ex : *255.255.255.0*) en classe d'adresse (ex : *24*) : `%%calc_classe(%%mask)` ;

Fonctions de tests

- vérification que la variable est une adresse IP (et pas un nom DNS) : `%%is_ip(%%variable)` ;
- vérification de l'existence d'un fichier : `%%is_file(%%fichier)`.

Déclaration de fonctions locales

Pour un traitement local et répétitif, il peut être pratique de déclarer une fonction directement dans un template avec `%def` et `%end def`.

Cependant, la syntaxe à utiliser dans ces fonctions est assez complexe (on ne sait jamais quand mettre le caractère `%` !) et ce genre de déclaration ne facilite pas la lisibilité du template.

Les fonctions déclarées localement s'utilisent de la même façon que les fonctions déjà prédéfinies.



```
%def nombre_points(chaine)
    %return chaine.count('.')
%end def
Il y a %%nombre_points(%%ma_variable) points dans ma variable.
```

Ajout de fonctions personnalisées

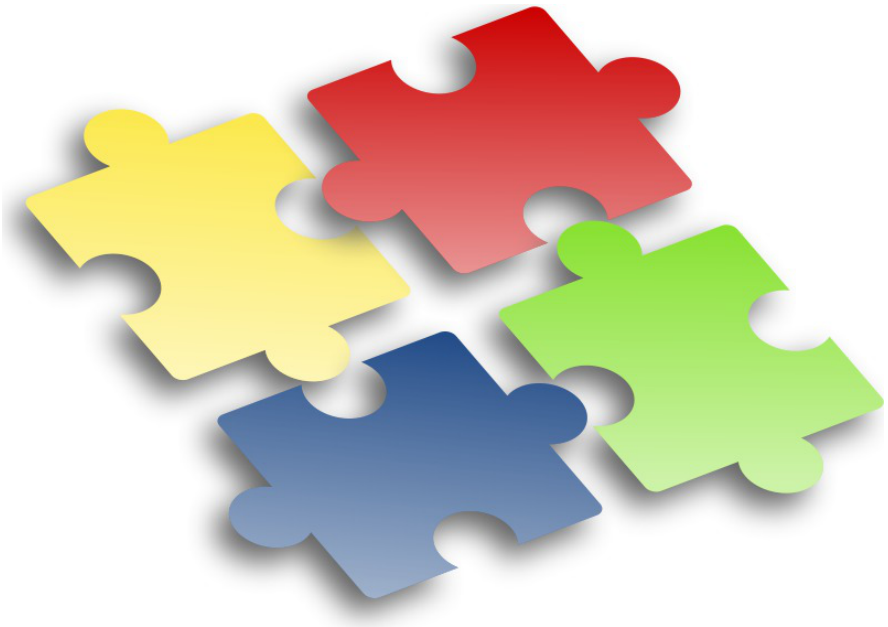
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 importez des librairies python dans un fichier de fonctions personnalisées, ne les importez pas en début de fichier. Les imports doivent être faits dans la fonction de calcul elle-même.



Les adaptations que vous pouvez réaliser sur l'un de vos serveurs EOLE sont susceptible 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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.711].

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 eolesso_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']
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
%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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

CreoleLint et CreoleCat [p.623]

2.5. Le fichier de configuration Creole

Le fichier de configuration principal d'un module EOLE est enregistré dans `/etc/eole/config.eol`.

Ce fichier est au format JSON[p.716].



Bien que ce fichier semble simple et lisible, il est fortement déconseillé de l'éditer sans passer par l'interface de configuration du module.

Version du fichier

Depuis EOLE 2.4, le numéro de sous-version du module EOLE sur lequel a été enregistré le fichier de configuration est stocké dans celui-ci.

Il est associé au mot-clé réservé : **___version___**.

Exemple : `"___version___": "2.6.1"`.

Représentation des variables et des valeurs associées

Seules les variables modifiées par l'utilisateur et celles faisant l'objet d'un enregistrement obligatoire sont stockées dans le fichier sous forme d'un dictionnaire.

Les noms des différentes variables Creole sont les mot-clés du dictionnaire.

La valeur associée est elle-même un dictionnaire qui contient le propriétaire (stocké dans le mot-clé **owner**) et la valeur de la variable (stockée dans le mot-clé **val**).

En fonction du type Creole de la variable, la valeur représentée peut-être :

- une chaîne de caractère : `"numero_etab": {"owner": "gen_config", "val": "0000000A"}` ;
- un entier (si type='number') : `"vm.swappiness": {"owner": "creoleset", "val": 0}` ;
- aucune valeur (possible pour certaines variables à enregistrement obligatoire) : `"test_autosave": {"owner": "forced", "val": null}` ;
- une liste (si multi='True') : `"ip_admin_eth0": {"owner": "gen_config", "val": ["192.168.230.0", "194.18.20.0"]}`.

Depuis la version EOLE 2.6, les valeurs des variables esclaves sont indexées :

`"netmask_admin_eth0": {"owner": {"1": "gen_config", "0": "gen_config"}, "val": {"1": "255.255.255.0", "0": "255.255.255.0"}`

Origine des valeurs enregistrées

Le nom de l'application et/ou de l'action ayant modifié en dernier la valeur de l'une des variable est associé au mot-clé : **owner**.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Exemple : `"serveur_maj": {"owner": "gen_config", "val": ["test-eole.ac-dijon.fr"]}`

- `default` : valeur par défaut et/ou calculée (n'est jamais enregistrée dans le fichier config.eol) ;
- `forced` : valeur par défaut enregistrée d'office pour les variables à verrouillage automatique (**auto_freeze**) ou à enregistrement obligatoire (**auto_save**) ;
- `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.

2.6. 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.707] ;
- CreoleLock permettant de placer, enlever ou vérifier les verrous Creole.

2.6.1. 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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` ;
- `condition_without_target` : recherche des conditions sans cible associée (EOLE >=2.6.2) ;
- `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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.tmpl -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.tmpl`

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.

2.6.2. 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

```
# CreoleGet --list | grep release
eole_release="2.8.1"
```

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=
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
service0.name="networking"
service1.name="cron"
service10.name="exim4"
service11.name="eoleflask"
service12.name="nginx"
service13.name="ead3"
service14.name="genconfig"
service15.name="bastion"
service16.name="z_stats"
service2.name="rng-tools"
service3.name="ntp"
service4.name="nut-server"
service5.name="salt-api"
service6.name="salt-master"
service7.name="salt-minion"
service8.name="ead-server"
service9.name="ead-web"
root@eolebase:~#
```

Recharger les variables et/ou la configuration creoled avec CreoleGet

À partir de la version EOLE 2.6.1, deux nouvelles options permettent de demander le rechargement du service creoled[p.708].

- `CreoleGet --reload` : recharge toute la configuration Creole (dictionnaires et valeurs) ;
- `CreoleGet --reload-eol` : recharge uniquement les valeurs de configuration Creole.

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.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

2.6.3. 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.707].

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.

2.6.4. CreoleLock

CreoleLock est un utilitaire permettant de placer, enlever ou vérifier les verrous Creole.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.726] 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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]
```

2.6.5. 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

```
#!/bin/bash
echo "mon adresse IP est $(CreoleGet adresse_ip_eth0)"
echo "La base Ldap est stockée dans $(CreoleGet container_path_annuaire) /var/lib/ldap"
echo "Le conteneur annuaire a l'adresse : $(CreoleGet container_ip_annuaire)"
CreoleRun "ls /var/lib/ldap" annuaire
CreoleService slapd restart -c annuaire
```

Script compatible EOLE 2.3 et supérieur

```
#!/bin/bash
if [ -f /usr/bin/ParseDico ];then
  RunCmd=RunCmd
  . /usr/bin/ParseDico
  . /etc/eole/containers.conf
  . /usr/share/eole/FonctionsEoleNg
else
  RunCmd=CreoleRun
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
    # récupération des variables nécessaires
    container_path_web=$(CreoleGet container_path_web)
    nom_machine=$(CreoleGet nom_machine)
fi
touch "${container_path_web}/etc/${nom_machine}.conf"
$RunCmd "chown www-data /etc/${nom_machine}.conf" web
ls -al "${container_path_web}/etc/${nom_machine}.conf"
```

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['eolesso_ldap.eolesso_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')
  ```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`manage_service('restart', '<service>', '<conteneur>')`

Petit script Python

```
#!/usr/bin/env python3
# -*- coding: UTF-8 -*-
from creole.client import CreoleClient
creole_client = CreoleClient()
print ("mon adresse IP est {0}".format(creole_client.get_creole(
'adresse_ip_eth0')))
print ("La base Ldap est stockée dans {0}/var/lib/ldap".format(
creole_client.get_creole('container_path_annuaire')))
print ("Le conteneur annuaire a l'adresse : {0}".format(creole_client.
get_creole('container_ip_annuaire')))
from pyeole.process import system_code
system_code(['ls', '/var/lib/ldap'], container='annuaire')
from pyeole.log import init_logging
from pyeole.service import manage_services
init_logging(level='info')
manage_services('restart', 'slapd', 'annuaire')
```

Script compatible EOLE 2.3 et supérieur *(modulo le nom de l'interpréteur python)*

```
#!/usr/bin/env python3
# -*- coding: UTF-8 -*-
from pyeole.process import system_code
try:
    from creole import parsedico
    from creole.eosfunc import load_container_var
    variables = parsedico.parse_dico()
    variables.update(load_container_var())
except:
    from creole.client import CreoleClient
    variables = CreoleClient().get_creole()
fichier = open('{0}/etc/{1}.conf'.format(variables['container_path_web'],
variables['nom_machine']), 'a')
fichier.close()
system_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.

```
#!/usr/bin/env python3
# -*- coding: UTF-8 -*-
from creole.loader import creole_loader, config_save_values
config = creole_loader(rw=True)
config.creole.interface_0.ssh_eth0 = u'oui'
config.creole.interface_0.ip_ssh_eth0.netmask_ssh_eth0[0] =
u'255.255.255.255'
config.creole.interface_0.ip_ssh_eth0.ip_ssh_eth0[0] = u'192.168.1.1'
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
8 config_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.733], 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
```

2.7. 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/postemplate` : exécution entre la templatisation des fichiers et le redémarrage des services ;
- `/usr/share/eole/postservice` : exécution après le redémarrage des services.

Chacun des scripts doit respecter les contraintes exigées par l'outil `run-parts`, et, en particulier :

- être exécutable ;
- être sans extension.

L'ensemble de ces scripts se jouent de façon alphanumérique.

Les scripts fournit 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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
#!/bin/bash
if [ "$1" == "instance" ]; then
    echo "ce code n'est exécuté qu'à l'instance"
elif [ "$1" = "reconfigure" ] ;then
    echo "ce code n'est exécuté qu'au reconfigure"
fi
```



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 :

```
#!/bin/bash
# <<< SCRIPT >>>
exit 0
```

Voir aussi...

Indications pour la programmation [p.630]

2.8. 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 librairies EOLE, mais vous pouvez créer vos propres fonctions pour vos besoins spécifiques.

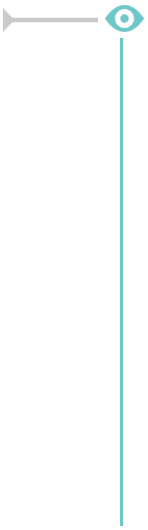
Généralement, le test affiche *Ok* si le service est fonctionnel et *Erreur* en cas de problème.

Voici quelques fonctions disponibles dans la librairie `/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 ;
- *TestHTTPPage* : teste l'ouverture d'une session HTTP ;
- *TestWeb* : teste le téléchargement d'une page HTTP ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- *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 TestHTTPPage
if [ $(CreoleGet activer_apache) = "oui" ];then
        TestHTTPPage "Web local" "http://$(CreoleGet adresse_ip_eth0)/"
fi
```

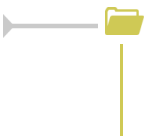
Voir aussi...

Indications pour la programmation [p.630]

2.9. Gestion des noyaux Linux

Noyau Linux utilisé

Les modules EOLE 2.8 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.



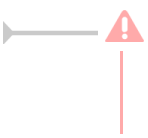
Sur les dernières versions d'Ubuntu, le noyau utilisé est `linux-image-generic`.
Pour plus d'informations, consulter la page : http://doc.ubuntu-fr.org/ltsenablementstack



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

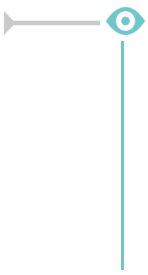
Tous les noyaux sont purgés à l'`instance` et au `reconfigure` à l'exception :

- 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-5.4.0-47-generic** il faut ajouter le numéro de version du noyau 5.4.0-47 dans le fichier `/usr/share/eole/noyau/local` :

```
# echo 5.4.0-47 > /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.

2.10. 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.

Depuis la version 2.5 d'EOLE, `eole-schedule` est géré depuis Tiramisu[p.733].

Le principe est le suivant :

- si aucune sauvegarde n'est prévue, c'est cron[p.708] qui lance `eole-schedule` ;
- si une sauvegarde est prévue, c'est Bareos[p.704] qui lance `eole-schedule`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Gestion des tâches planifiées

Lister ce qui est programmé

```
# manage_schedule -l
```

Ajouter une tâche planifiée

```
# manage_schedule -a daily -s majblacklist
```

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` .

Si vous venez de créer ou d'installer les fichiers XML décrivant les tâches planifiées que vous souhaitez manipuler, il peut être nécessaire de recharger les dictionnaires au préalable à l'aide de la commande : `systemctl restart creoled.service`

Gestion des tâches uniques (once)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Les scripts lancés pour une nuit sont gérés totalement différemment et les informations associées ne sont pas conservées dans Tiramisu.

Ajouter une une tâche planifiée unique

```
# manage_schedule -a once -s majauto
```

Supprimer une une tâche planifiée unique

```
# manage_schedule -d once -s majauto
```

La prise en compte des tâches uniques est instantanée.

L'appel à la méthode `--apply` n'est donc pas nécessaire.

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

```
# python3 -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
```

```
# manage_schedule --apply
```

ou :

```
# python3 -c "from creole import maj; maj.enable_maj_auto(); print(maj.maj_enabled())"
```

Désactivation de la mise à jour hebdomadaire :

```
# manage_schedule -d majauto
```

```
# manage_schedule --apply
```

ou :

```
# python3 -c "from creole import maj; maj.disable_maj_auto(); print(maj.maj_enabled())"
```

Si la fréquence des tâches `Schedule` est personnalisée dans l'interface de configuration du module, c'est cette dernière qui prévaut et l'activation/désactivation de la mise à jour hebdomadaire via l'EAD ou la commande `manage_schedule` n'est plus possible.

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`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
root@amon:~# /usr/share/eole/schedule/schedule cron
Démarrage de pre schedule daily
pre schedule daily accompli
Démarrage de post schedule daily
.  Test de http://eole.orion.education.fr/maj/blacklists => Ok
Téléchargement des bases
Rien à faire pour blacklists.tar.gz
Rien à faire pour le fichier weighted
eole-schedule - run-parts: executing
/usr/share/eole/schedule/daily/post/majblacklist daily
post schedule daily accompli
Démarrage de pre schedule once
pre schedule once accompli
Démarrage de post schedule once
post schedule once accompli
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.

```
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```



Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
root@eole:~# rm /etc/eole/extra/schedule/config.eol
rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

À partir d'EOLE 2.7.0, il est possible de fixer le jour et l'heure de la mise à jour hebdomadaire à l'aide de la commande `CreoleSet`.



Pour paramétrer la mise à jour hebdomadaire le mercredi matin à 3h30, il faut exécuter les commandes suivantes :

```
root@eole:~# CreoleSet .schedule.schedule.weekday 3
root@eole:~# CreoleSet .schedule.schedule.hour 3
root@eole:~# CreoleSet .schedule.schedule.minute 30
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> Le jour choisi devra cependant être différent de celui choisi pour le "Jour des tâches mensuelles la première semaine du mois" (`.schedule.schedule.monthday`).

Déclarer une nouvelle tâche planifiée

Les tâches `eole-schedule` se composent de deux éléments :

- un fichier XML décrivant la tâche planifiée
- le script à exécuter

Les fichiers XML décrivant les tâches planifiées ont un format proche de celui des dictionnaires[p.709] Creole.

Exemple du fichier : `/usr/share/eole/creole/extra/schedule/01_majauto.xml`

```
<?xml version="1.0" encoding="utf-8"?>

<creole>
    <variables>
        <family name='majauto'>
            <variable name="description" type="string"><value>Mise à jour du serveur</value></variable>
            <variable name="day" type="schedule"><value>weekly</value></variable>
            <variable name="mode" type="schedulemod"><value>post</value></variable>
        </family>
    </variables>
</creole>
```

Le nom du script à exécuter doit correspondre exactement au nom de la famille : `majauto`, dans l'exemple.

Le script doit être exécutable et sans extension. Il doit être placé dans le répertoire `/usr/share/eole/schedule/scripts`.

C'est `eole-schedule` qui se charge de créer des liens symboliques en fonction de la planification souhaitée.

2.11. Gestion du pare-feu eole-firewall

Introduction

`eole-firewall` est conçu pour gérer les flux réseau d'un module EOLE.

Il permet d'autoriser des connexions :

- de l'extérieur vers le maître ;
- de l'extérieur vers un conteneur.

Techniquement, ces autorisations se traduisent par des règles *iptables* et, si nécessaire, des connexions TCP Wrapper[p.732] et l'activation de modules noyau.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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

```
#!/bin/bash
/sbin/iptables -A eth0-root -p icmp --icmp-type destination-unreachable -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type network-unreachable -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type source-quench -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type fragmentation-needed -j ACCEPT
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
/sbin/iptables -A eth0-root -p icmp --icmp-type time-exceeded -j ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type parameter-problem -j
ACCEPT
/sbin/iptables -A eth0-root -p icmp --icmp-type echo-reply -j ACCEPT
/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.589]

2.12. Gestion de drapeaux eole-flag

Un drapeau est un fichier servant de marqueur d'un état du système. Un drapeau, par sa présence ou son absence, permet d'identifier deux états différents.

Une gestion de drapeaux est apparue utile pour des raisons d'automatisation de leur création et suppression.

La gestion des drapeaux est accessible via l'installation du paquet optionnel `eole-flag` disponible à partir de la version 2.7.2.



Le premier cas d'usage est celui du conditionnement du comportement d'un programme en fonction d'un planning.

C'est le cas mis en place pour la messagerie dont une coupure peut être souhaitée à certaines heures de la journée

Principe de fonctionnement

La gestion de drapeau retenue s'articule autour des points suivants :

- un emplacement dédié géré par `systemd-tmpfiles` impliquant que les drapeaux ne doivent pas être perçus comme persistants ;
- un nom correspondant au nom du fichier créé ;
- une méthode d'automatisation.

L'automatisation est pensée comme l'application d'un planning, au moins une fois par jour via un timer déclenchant l'interprétation d'un planning et termes de tâches `at`. Seules les tâches du jour sont programmées.

Un planning est propre à chaque drapeau quoiqu'un même planning puisse être utilisé pour l'automatisation de plusieurs drapeaux.

Un planning est constitué de la déclaration d'une série de plages avec, notamment, une heure de début et une heure de fin. Ces plages sont utilisées pour programmer la création et la suppression des drapeaux.

Pour des raisons d'ergonomie de saisie des plannings, il est possible de choisir si une plage correspond à la présence ou à l'absence du drapeau.



Examinons la configuration nécessaire à la coupure de la messagerie en dehors des plages

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> de travail.
>
> D'un côté, Exim peut être configuré pour interdire l'envoi de courriel si un fichier spécifique est présent dans le système de fichiers. De l'autre côté, on peut automatiser la création et la suppression de ce fichier spécifique via un planning d'évènements.
>
> Il est possible d'utiliser les événements comme marqueur de la présence du fichier ou comme marqueur de son absence. La différence tient au nombre d'événements nécessaires pour représenter les plages de fermeture au cours d'une journée. Dans le cas classique envisagé ici, il faut un évènement si celui-ci marque l'absence du fichier verrouillant l'envoi de courriels ou deux évènements si ceux-ci marquent la présence de ce fichier.

Méthodes d'automatisation

Deux méthodes sont actuellement implémentées :

- manuelle
- fichier

La méthode manuelle n'est pas, à proprement parler, une méthode d'automatisation. Toutefois, la déclaration d'un drapeau géré manuellement permet de pouvoir recenser ce dernier.

La méthode d'automatisation basée sur un fichier permet de fournir le planning sous forme de fichier et, ainsi, d'exploiter les possibilités de dépôt du module Zéphir.

Actuellement, le fichier doit contenir le planning au format json dont un exemple est fourni ci-après.

Le planning peut servir à déclarer des plages qui ont différentes périodes de répétition :

- weekly : plages d'une semaine type ;
- monthly : plages répétées à des jours précis tous les mois ;
- yearly : plages répétées à des jours précis tous les ans ;
- unique: plages propres à des jours précis de l'année.

Chaque plage est déclarée en indiquant une date, une étiquette, une heure de début et une heure de fin.

L'étiquette est `off` est utilisée en opposition à l'étiquette `on`. Elle permet d'annuler un événement d'une période moins prioritaire.

Les heures de début et de fin de plages sont à la minute près et sont interprétées en heure locale.

La date adopte un format différent selon le contexte :

weekly : jour de la semaine (de 1 à 7, du lundi au dimanche) ;

monthly : numéro du jour du mois (les dépassements sont ignorés par le traitement) ;

yearly : numéros du mois et du jour sans mention de l'année (MM-JJ) ;

unique : date complète (AAAA-MM-JJ).

```
{
    "monthly": [
        [1, "on", "07:30", "17:30"],
        [4, "on", "07:30", "17:30"]
    ],
    "weekly": [
        [1, "on", "08:00", "17:00"],
        [2, "on", "08:00", "17:00"],
        [3, "on", "08:00", "17:00"],
        [4, "on", "08:00", "17:00"],
        [5, "on", "08:00", "17:00"]
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
    ],
    "yearly": [
        ["12-25", "off", "00:00", "24:00"]
    ],
    "unique": [
        ["2024-07-04", "off", "00:00", "24:00"],
        ["2024-06-27", "off", "00:00", "24:00"],
        ["2024-07-06", "off", "00:00", "24:00"]
    ]
}
```

La priorité des plages déclarées est fonction du contexte. Seules les plages du contexte le plus prioritaire sont prises en compte. Du plus prioritaire au moins prioritaire, les contextes sont ordonnés de la façon suivante en fonction de leur spécificité :

1. unique,
2. yearly,
3. monthly,
4. weekly.

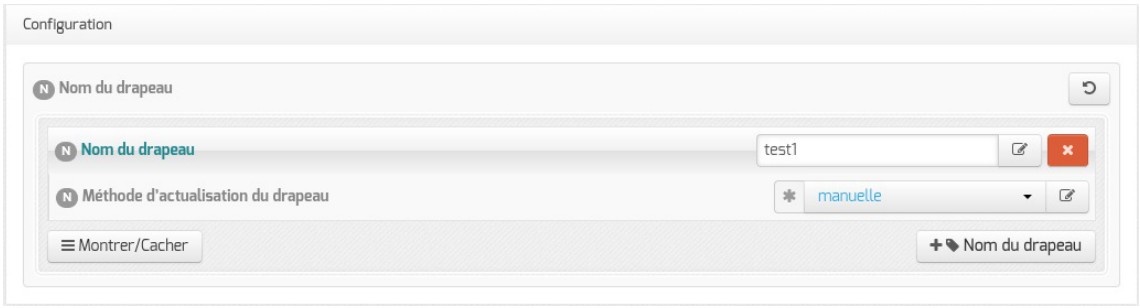
Configuration

La configuration de la gestion des drapeaux est regroupée dans l'onglet spécifique `Drapeaux`.



Les variables de configuration disponibles dépendent de la méthode d'actualisation sélectionnée.

- `Nom du drapeau` : nom du fichier qui sera créé sur le système de fichier (pas de chemin absolu) ;
- `Méthode d'actualisation du drapeau` : manuelle ou fichier, indique quel mécanisme mettre en œuvre pour la création des tâches de gestion du drapeau (si manuelle, aucun mécanisme n'est mis en place).

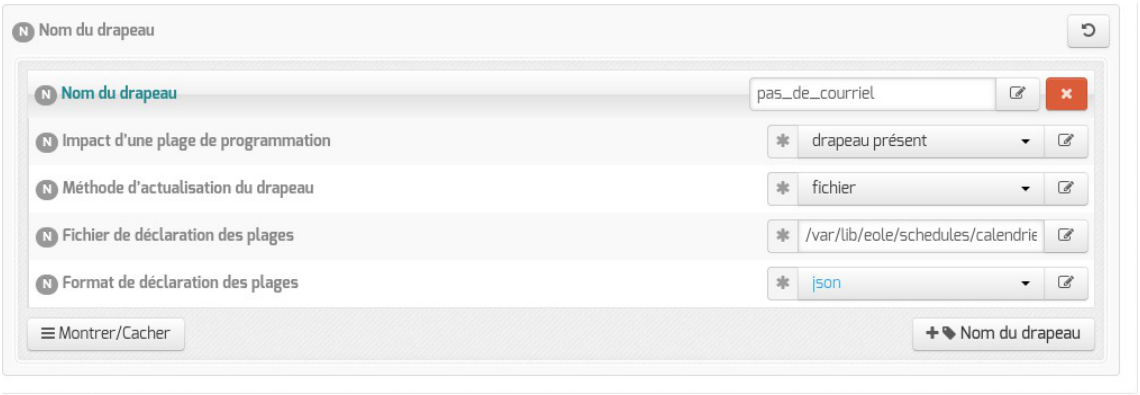


Les variables suivantes sont disponibles pour la méthode d'actualisation basée sur un fichier.

- `Impact d'une plage de programmation` : drapeau présent ou drapeau absent, indique si la plage doit être interprétée comme une plage de présence du fichier ou une plage d'absence du fichier ;
- `Fichier de déclaration des plages` : emplacement du fichier de planning sur le système de fichier local (le fichier peut y être déposé par n'importe quel moyen à la disposition de l'administrateur) ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- `Format de déclaration des plages` : format du planning (actuellement, seul un planning au format json respectant le modèle décrit précédemment est pris en charge).



Utilisation en ligne de commande

Le paquet installe un timer flag-switch.timer, un service flag-switch.service ainsi qu'une commande flag-switch.

Le service interprétant le planning pour le traduire sous forme de tâche pour la commande `at` est déclenché via un timer quotidien lancé à 00:00 au délai d'exécution près.

Le service peut également être lancé à la demande via la commande `systemctl start flag-switch.service`. C'est notamment utile dans le cas où le fichier de planning aurait été mis à jour après exécution du timer.

Enfin, la commande `flag-switch` peut être utilisée en dehors du contexte du service pour, notamment, supprimer les programmations relatives aux drapeaux ou supprimer tous les drapeaux en place.

Pour éviter les tâches en doublon, l'application d'un planning s'accompagne toujours de la suppression, au préalable, des tâches précédemment programmées.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 11

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

⚠ Cette partie de la documentation est en cours d'écriture ou de réécriture...



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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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 IUti% 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 ...
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

```
# mkdir /media/partition
# mount /dev/sda2 /media/partition
mount: type inconnu de système de fichiers 'LVM2_member'
```

Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
# vgscan
Reading all physical volumes. This may take a while...
Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
# vgchange -a y eolebase-vg
4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
# ll /dev/mapper/
total 0
drwxr-xr-x  2 root root     160 févr.  8 11:53 ./
drwxr-xr-x 19 root root    4460 févr.  8 11:53 ../
crw-------  1 root root 10, 236 févr.  8 11:53 control
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-home -> ../dm-4
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-root -> ../dm-0
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-swap_1 -> ../dm-1
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-var -> ../dm-3
```

ou

```
# lvdisplay
  --- Logical volume ---
  LV Path                /dev/eolebase-vg/swap_1
  LV Name                swap_1
  VG Name                eolebase-vg
  LV UUID                OO47WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
  LV Write Access        read/write
  LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
  LV Status              available
  # open                 2
  LV Size                1,09 GiB
  Current LE             280
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:1
[...]
```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 évolues régulièrement.

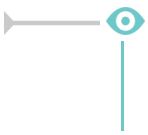


Une documentation thématique dédiée réuni les FAQ de tous les modules.

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` (examinateur de paquets)
- `nmap` (scanneur de ports)
- `tcpcheck` (testeur de port)

Les archives des listes de discussion

Les listes de discussion du projet sont archivés 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.

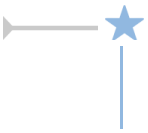
https://pcll.ac-dijon.fr/listes/lists

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

https://pcll.ac-dijon.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'activer 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'envoie de messages sur une liste de discussion, merci de les respecter.

  http://fr.wikipedia.org/wiki/Nétiquette

Documentation externe

La plupart des logiciels fournit avec les modules EOLE sont largement utilisés en dehors de l'Éducation nationale.

Des documentations plus spécifiques à l'utilisation de la plupart des logiciels utilisés sont disponibles sur Internet (ex. http://doc.ubuntu-fr.org/cups).

Dans le cas de la mise en place d'une configuration avancée de l'un des logiciels, il est tout à fait indiqué de consulter sa documentation officielle (ex. http://www.cups.org/documentation.php).



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.708]) 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Les annonces

La publication des paquets fait 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://pcll.ac-dijon.fr/eole/ ;
- envoi d'un message sur les principales listes de diffusion du projet : https://pcll.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/Journaux290 pour EOLE 2.9.0).

Quelques références

- Site officiel du Pôle de Compétences Logiciels Libres : https://pcll.ac-dijon.fr ;
- Site web officiel de la distribution : https://pcll.ac-dijon.fr/eole/ ;
- Le blog : http://pcll.ac-dijon.fr/eole/blog/ ;
- Les listes de discussion : https://pcll.ac-dijon.fr/listes ;
- 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

RGPD
Si vous souhaitez échanger des données avec le Pôle de Compétences à des fins d'expertise, vous pouvez être amené à transférer des journaux, des mots de passe, des fichiers confidentiels qui contiennent beaucoup d'informations concernant les utilisateurs (personnels administratif, enseignants, élèves, parents d'élèves). Nous attirons votre attention sur les informations nominatives suivantes : nom, prénom, date de naissance, email, coordonnées des responsables. Il est de votre responsabilité de vérifier tous les contenus et de les anonymiser. Vous devez avoir l'aval du Responsable des données de votre organisation avant d'effectuer l'envoi. Si vous utilisez la procédure `gen_rpt` présentée ci-dessous, l'archive sera chiffrée avec une clé détenue par le seul PCLL. Cette procédure, vous permet de transférer d'autres fichiers en les incluant dans l'archive. Le PCLL et le Ministère de l'Éducation nationale ne peuvent être tenus responsables de la mauvaise application de cette procédure.

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 (`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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 (selon le module) ;
- le rapport de sauvegarde (selon le module) ;
- le contenu du répertoire `/root/gen_rpt` (à partir de la version 2.7.2).

Le répertoire /root/gen_rpt peut être utilisé pour ajouter à l'archive des fichiers complémentaires utiles au diagnostic.

La commande `gen_rpt` crée les archives dans le répertoire courant.

L'archive nommée <module>-<numéro-etab>.tar.gz, non chiffrée, peut être envoyée à n'importe qui.

À partir de la version 2.7.2, une archive chiffrée nommée `<module>-<numéro-etab>.tar.gz.gpg` est également générée. Seule l'équipe EOLE possède la clé nécessaire pour déchiffrer cette archive. Si vous voulez envoyer le rapport à l'équipe EOLE, envoyez cette archive chiffrée nommée `<module>-<numéro-etab>.tar.gz.gpg`.



Si une passerelle de courrier a été définie sur le serveur, il est possible d'envoyer l'archive par courriel.

Celui-ci pourra être immédiatement envoyée à l'équipe EOLE (merci de ne pas en abuser) ou à l'adresse de votre choix.

À partir de la version 2.7.2, l'envoi immédiat à l'équipe EOLE utilise la version chiffrée de l'archive. Dans le cas d'un envoi vers une autre adresse, il faut choisir quelle version de l'archive envoyer : normale ou chiffrée (mais dans ce dernier cas, uniquement lisible par l'équipe EOLE).

Si aucune passerelle de courrier n'a été définie sur le serveur, les deux versions de l'archive sont créées. Vous avez alors le choix de la version à récupérer pour un envoi depuis un autre poste.



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 aiderons 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 ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 certain 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'envoie 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`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'activer 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 certain 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.

Vous pouvez nous rejoindre sur le canal `#eole` hébergé sur irc://irc.oftc.net:6667 ou grâce à l'interface https://webchat.oftc.net.

- Il est demandé de mettre son nom réel dans les paramètres du client. ;
- La Nétiquette décrit un certain nombre de règles lors de l'envoi de messages sur une liste de discussion, merci de les respecter.

  http://fr.wikipedia.org/wiki/Nétiquette

Le Pôle de Compétences Logiciels Libres utilisait Freenode depuis 2008 comme réseau IRC.

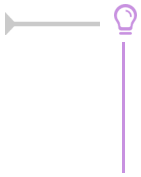
Suite aux changements des conditions d'usages de Freenode, la gestion du canal `#eole` nous a été enlevé sans préavis. Vous avez pu constater que les lignes d'accueil ont disparu. Maintenant, les utilisateurs doivent créer un compte (SSO) pour accéder à notre canal.

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 12

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[p.712]) :

- **<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 contenants des mises à jour correctives non critiques ;
- **<version>-security** : paquets contenants 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 2.8 sont disponibles à l'adresse suivante :

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

Les dépôts proposent pour chaque version d'EOLE plusieurs catégories de paquets (les fichiers *.deb) :

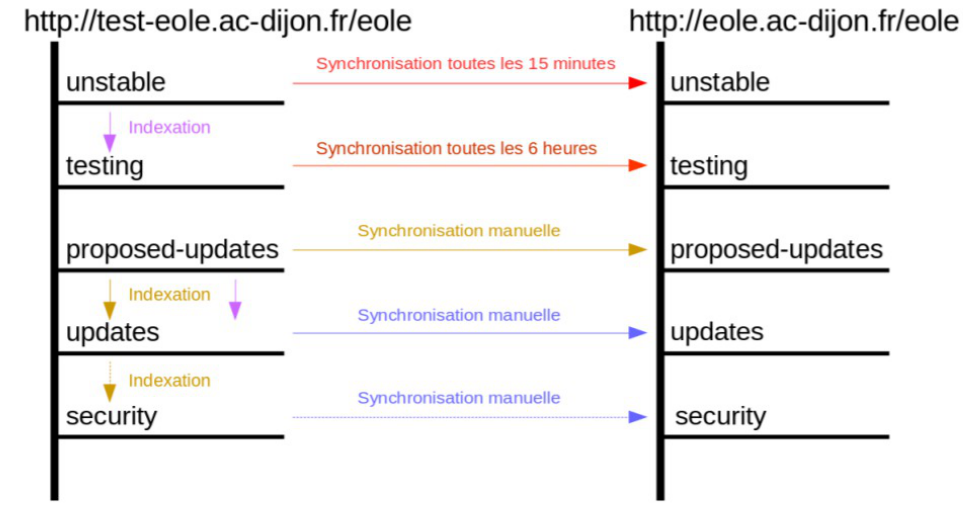
- **eole-2.8-unstable** : paquets de développement pouvant contenir des évolutions fonctionnelles, des corrections de sécurité ou de dysfonctionnement ;
- **eole-2.8-testing** : paquets candidats (correspondant aux images RC de la distribution) qui sont éligibles pour passer en version stable après validation ;
- **eole-2.8-proposed-updates** : paquets candidats qui sont éligibles pour passer en version update après validation (dysfonctionnement, régression, etc.) ;
- **eole-2.8-updates** : paquets contenant des mises à jour correctives non critiques ;
- **eole-2.8-security** : paquets contenant des mises à jour de sécurité ;
- **eole-2.8** : 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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. Ils sont utilisés durant le développement et lors des tests de mises à jour avant diffusion.



Publication des paquets candidats toutes les 3 semaines
Publication des paquets stables 2 semaines après les paquets candidats
Publication d'une image ISO

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

- **eole-2.8-unstable** : dépôt synchronisé toutes les 15 minutes ;
- **eole-2.8-testing** : dépôt synchronisé toutes les 6 heures ;
- **eole-2.8.x-proposed-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.8.x-updates** : synchronisation manuelle avec annonce préalable ;
- **eole-2.8.x-security** : synchronisation manuelle avec annonce préalable ;
- **eole-2.8.x** : aucune modification sur ce dépôt.

Les miroirs académiques sont en principe synchronisés toutes les nuits.

Architectures supportées

Depuis la version 2.7, seule l'architecture 64 bits[p.703] (x86_64) est supportée 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 ;
- **amd64** : paquets compilés spécifiquement pour l'architecture 64 bits.

Signature des paquets EOLE

La clé GPG[p.713] publique de la clé signant les paquets EOLE est disponible à l'adresse : http://eole.ac-dijon.fr/eole/project/eole-2.8-repository.key

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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-journ

Note technique de l'ANSSI[p.703] 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 :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 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 au 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

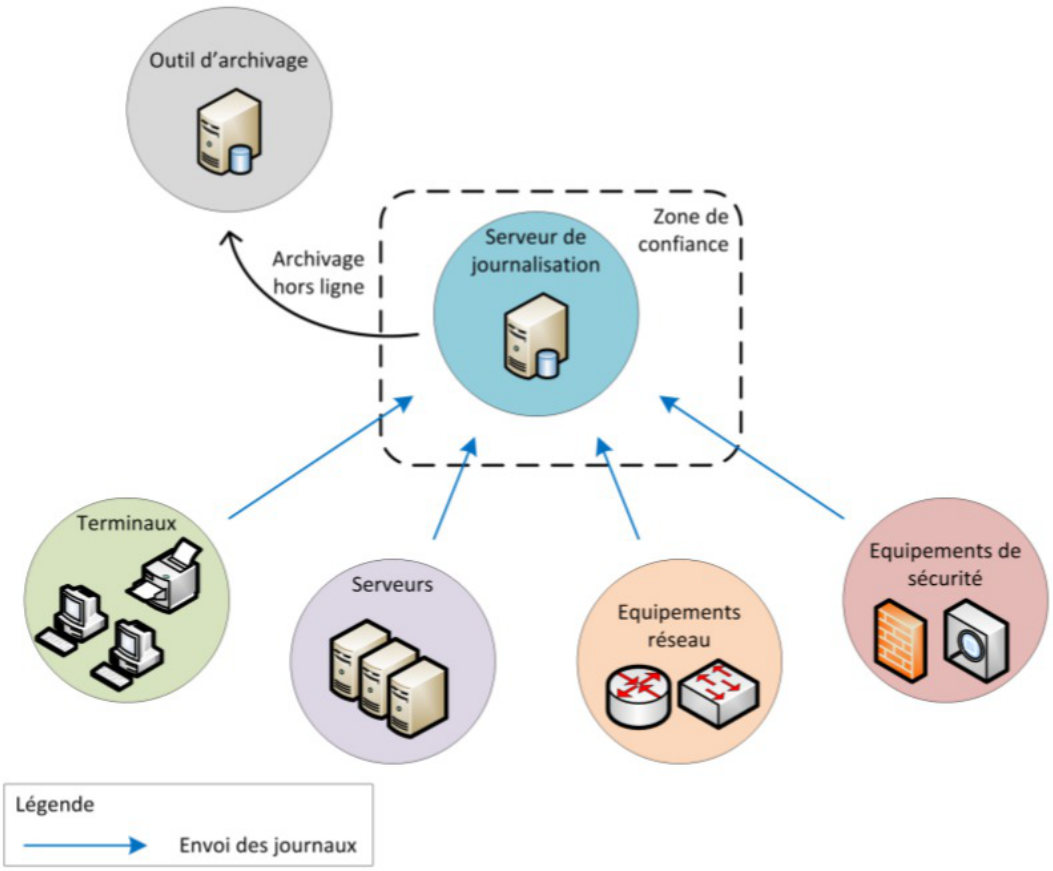
- l'estimation de l'espace de stockage nécessaire à la conservation locale des journaux doit être prise

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

en compte dans le dimensionnement des équipements,

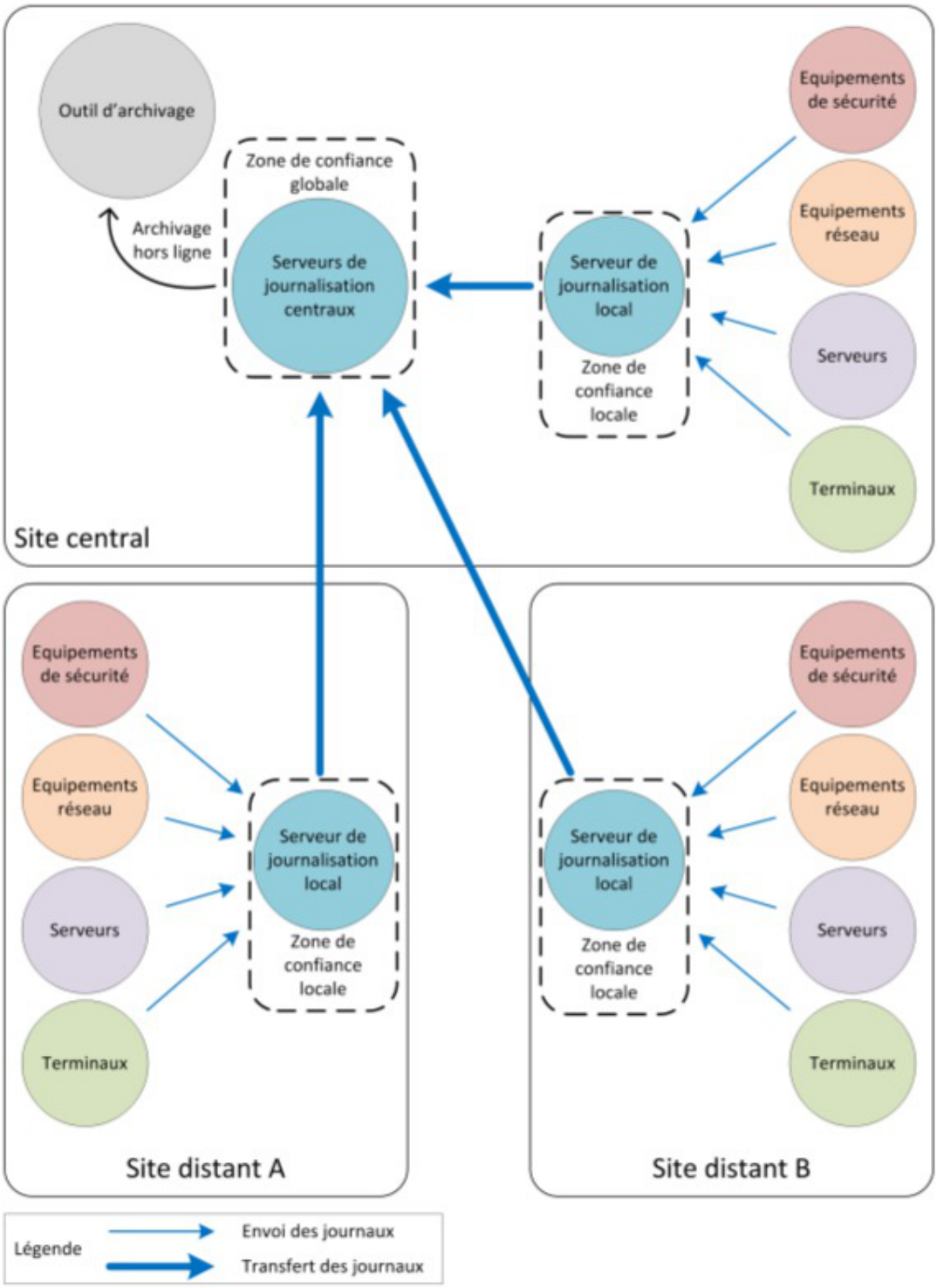
Recommandations d'architecture et de conception

- Les journaux doivent être automatiquement exportés sur une machine physique différente de celle qui les a générés ;
- centralisation des journaux 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)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 complétement indépendante.

Un module EOLE peut donc être considéré comme un ensemble de services choisis et adaptés à des usages précis.

Des services peuvent être ajoutés sur les modules existants (exemple : installation du paquet `eole-dhcp` sur le module Amon) et il est également possible de fabriquer un module entièrement personnalisé en installant les services souhaités sur une installation Eolebase.

1.1. eole-antivirus

Le paquet `eole-antivirus` permet la mise en place d'un serveur antivirus.



Ne pas confondre ce paquet avec `eole-antivir` qui permet la mise en place de la gestion d'un antivirus centralisé de type OfficeScan de Trend Micro.

http://dev-eole.ac-dijon.fr/projects/eole-antivir

http://eole.ac-dijon.fr/presentations/2011%20novembre/eole-antivir.pdf

Logiciels et services

Le paquet `eole-antivirus` s'appuie sur les services clamav-daemon et clamav-freshclam.

http://www.clamav.net/

Historique

A la base, les services clamav et freshclam étaient déjà sur la plupart des modules afin de servir à d'autres services tels que le serveur de fichiers, le serveur FTP, le serveur SMTP, le proxy (filtrage du contenu), ...

La mise en commun a permis de rendre les configurations homogènes.

Conteneurs

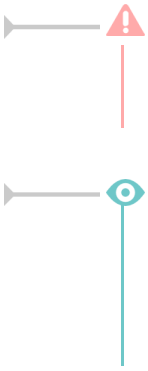
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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 le module AmonEcole, le service clamav-daemon est pré-installé dans les groupes de conteneurs :

- `partage (id=52)` ;
- `internet (id=53)` ;
- `reseau (id=51)`.



C'est au paquet du service qui souhaite utiliser le serveur antivirus de gérer son installation, sa configuration et son démarrage dans le conteneur souhaité.

Activation de clamav dans un conteneur

```
<container name='xxx'>
    <package>eole-antivirus-pkg</package>
    <service>clamav-daemon</service>
    <file filelist='clamav' name='/etc/clamav/clamd.conf'/>
</container>
```

1.2. eole-dhcrelay

Le paquet `eole-dhcrelay` permet la mise en place d'un relais DHCP[p.708].

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 système hôte (maître).

1.3. eole-dns

Le paquet `eole-dns` permet la mise en place d'un serveur DNS[p.709] local.

Logiciels et services

Le paquet `eole-dns` s'appuie principalement sur le service bind9[p.705].

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

http://www.isc.org/downloads/bind/

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 le module AmonEcole, 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[p.731] Exim[p.711].

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, 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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

http://www.networkupstools.org/

Historique

Ce paquet est pré-installé sur tous les modules.

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.

Logiciels et services

Le paquet `eole-proxy` s'appuie sur les logiciels et services suivants :

- Squid[p.731] : proxy cache ;
- e2guardian[p.710] : filtrage web ;
- Lightsquid : analyseur de logs ;
- smbd, nmbd, winbind, krb5 : authentification NTLM[p.723] ou Kerberos[p.717].

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 le module AmonEcole, 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 les authentifications en mode NTLM/KERBEROS, ce paquet fournit des configurations

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.728].

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 système hôte (maître).

1.8. eole-reverseproxy

Le paquet `eole-reverseproxy` permet la mise en place d'un serveur proxy inverse.

Le logiciel utilisé, Nginx[p.722], peut également faire office de serveur web.

Logiciels et services

Le paquet `eole-reverseproxy` s'appuie sur le serveur Nginx.

http://nginx.org/

Historique

Initialement conçu pour les modules Amon et AmonEcole, ce service est pré-installé sur tous les modules à partir de la version 2.6.1 d'EOLE.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

1.9. eole-vpn

Le paquet `eole-vpn` permet la mise en place d'un VPN[p.728].

Logiciels et services

Le paquet `eole-vpn` s'appuie principalement sur le logiciel strongSwan[p.732].

http://www.strongswan.org/

Historique

Ce paquet est pré-installé sur les modules Amon et AmonEcole ainsi que sur le module Sphynx.

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.734]).
Le logiciel utilisé, Nginx[p.722], se charge de distribuer les fichiers `wpad.dat` adaptés à chacun des sous-réseaux.

Logiciels et services

Le paquet `eole-wpad` s'appuie sur le serveur Nginx.

http://nginx.org/

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 et AmonEcole.

Conteneurs

Le service s'installe sur le système hôte (maître).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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)
- 53/tcp+udp : Dnsmasq
- 68/udp : dhclient
- 123/udp : ntpd
- 465/tcp : smtps (Exim4)
- 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 utilisés par l'EAD3

- 4300/tcp : nginx (reverse proxy EAD3 dans le cas où apache est activé)

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

- 4605/tcp : saltstack (publisher)
- 4606/tcp : saltstack (request server)
- 8880/tcp : saltsatck (api)

Ports spécifiques au module Amon

- 50/esp : IPsec
- 53/tcp+udp : bind (DNS)
- 67/udp : dhcrelay
- 500/udp : charon (VPN)
- 953/tcp : bind (RNDC)
- 1340/tcp : e2guardian (mode ICAP)
- 1342/tcp : e2guardian2 (mode ICAP)
- 1812/udp : radius
- 1813/tcp+udp : radius accounting
- 3128/tcp : squid (proxy)
- 3129/tcp : squid2 (proxy)
- 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)
- 9990/tcp : e2guardian
- 9992/tcp : e2guardian2

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)
- 83/tcp : nginx (interdiction proxy http e2guardian)
- 84/tcp : nginx (interdiction proxy https e2guardian)
- 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

La correspondance entre un service et un numéro de port standard peut être trouvée dans le fichier `/etc/services`.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Chapitre 14

Questions fréquentes

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



1. Questions fréquentes communes aux modules

CAS Authentication failed !

Le message ***`CAS Authentication failed ! You were not authenticated.`*** *(ou* ***`Authentification CAS infructueuse ! Vous n'avez pas été authentifié(e).`*** *)* peut apparaître si des modifications ont été faites dans l'interface de configuration.

Les paramètres constituant un certificat ont été modifiés récemment dans l'interface de configuration du module

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom de établissement, numéro RNE, etc...) suivie d'une reconfiguration du module ne régénère pas les certificats. Un message explicite le signale lors de l'étape de reconfiguration.

Après changement des paramètres il est nécessaire de supprimer le certificat :

```
# rm -f /etc/ssl/certs/eole.crt
```

puis lancer la reconfiguration du module :

```
# reconfigure
```

Plutôt qu'une suppression, il est possible d'utiliser la commande `gen_certif.py` avec l'option `-f` pour forcer la régénération (cependant, il faut que cette commande soit précédée d'une reconfiguration du module pour que les templates de configuration des certificats soient à jour).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`# 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

Il faut ajouter le nom alternatif dans le certificats pour que le certificat le prenne en compte. Pour cela dans l'onglet `Certificats ssl` en mode expert il faut remplir les champs `Nom DNS/IP alternatif 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`

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Dans un terminal

```
python3 -c "from creole import maj; print(maj.get_maj_day())"
```

Pour activer/désactiver la mise à jour hebdomadaire il est possible de passer par l'EAD ou par un terminal.

Via l'EAD

Pour l'afficher il faut se rendre dans la section `Système` / `Mise à jour` de l'EAD.

Dans un terminal

Activation de la mise à jour hebdomadaire :

```
/usr/share/eole/schedule/manage_schedule post majauto weekly add
```

ou :

```
python3 -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 :

```
python3 -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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Il faut supprimer le certificat du gestionnaire de certificats du navigateur et recharger la page.

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`.

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.734] 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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
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
```

Source : http://blog.remibergsma.com/2012/04/30/rrdtool-moving-data-between-32bit-and-64bit-archite

Comment débloquer les message en file d'attente ?

Un nombre de messages apparaissent comme étant *Frozen* dans le retour de la commande `diagnose`.

```
*** Messagerie
. Courrier SMTP => Ok
. File d'attente => 1 message(s)
. Messages "Frozen" => 1 message(s)
```

Une solution consiste à récupérer les identifiants des messages :

```
root@scribe:~# exim4 -bp
10h 2.5K 1abJaX-00036S-Bu <> *** frozen ***
touser@ac-test.fr
```

Il est ensuite possible de récupérer les journaux spécifiques message par message :

```
root@scribe:~# exim4 -Mvl 1abJaX-00036S-Bu
2016-03-03 04:06:05 Received from <> R=1abJaX-00036L-8j
U=Debian-exim P=local S=2525
2016-03-03 04:06:05 SMTP error from remote mail server after RCPT
TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr
[192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address
rejected: Access denied
2016-03-03 04:06:05 touser@ac-test.fr R=satellite_route
T=remote_smtp: SMTP error from remote mail server after RCPT
TO:<touser@ac-test.fr>: host socrate.in.ac-dijon.fr
[192.168.57.212]: 554 5.7.1 <touser@ac-test.fr>: Recipient address
rejected: Access denied
*** Frozen (delivery error message)
```

Dans cet exemple, le message d'erreur est `Recipient address rejected: Access denied`, l'expéditeur n'est pas autorisé à transiter par la passerelle configurée dans l'interface de configuration du module.

Comment changer le jour de mise à jour d'un serveur EOLE ?

Le jour tiré au hasard pour les mises à jour ne me convient pas et je souhaiterais le changer.

```
1 root@eole:~# manage_schedule -l
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le vendredi à 05:35 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

Une solution consiste à supprimer le fichier de configuration `/etc/eole/extra/schedule/config.eol`.

```
root@eole:~# rm /etc/eole/extra/schedule/config.eol
rm : supprimer fichier '/etc/eole/extra/schedule/config.eol' ? y
root@eole:~# manage_schedule -l
Tâches planifiées EOLE :
 * les tâches hebdomadaires se feront le jeudi à 04:12 (hors sauvegarde)
  - après sauvegarde
   + Mise à jour du serveur (majauto)
root@eole:~#
```

À partir d'EOLE 2.7.0, il est possible de fixer le jour et l'heure de la mise à jour hebdomadaire à l'aide de la commande `CreoleSet`.

Pour paramétrer la mise à jour hebdomadaire le mercredi matin à 3h30, il faut exécuter les commandes suivantes :

```
root@eole:~# CreoleSet .schedule.schedule.weekday 3
root@eole:~# CreoleSet .schedule.schedule.hour 3
root@eole:~# CreoleSet .schedule.schedule.minute 30
```

Le jour choisi devra cependant être différent de celui choisi pour le "Jour des tâches mensuelles la première semaine du mois" (`.schedule.schedule.monthday`).

Le proxy empêche les mises à jour

Les modifications apportées au proxy transparent à partir de la version 2.6.1 provoquent le blocage de certaines mises à jour aussi, la déclaration du proxy est nécessaire pour effectuer les mises à jour d'un module EOLE qui serait protégé par un module Amon.

```
root@scribe:~# Maj-Auto
Mise à jour le lundi 20 mars 2017 11:47:52
*** scribe 2.6.1 ***

Maj-Auto - (VERSION CANDIDATE) - Augmenter le niveau de mise à jour peut empêcher de
revenir au niveau de mise à jour stable.
Voulez-vous continuer ? [oui/non]
[non] : oui
pyeole.pkg - Pas de configuration du miroir Ubuntu avec eole.ac-dijon.fr qui semble
inaccessible : Impossible d'obtenir la version pour le dépôt :
http://eole.ac-dijon.fr/ubuntu/dists/xenial/main/binary-amd64/Release
pyeole.pkg - Pas de configuration du miroir Ubuntu avec ftp.crihan.fr qui semble
inaccessible : Impossible d'obtenir la version pour le dépôt :
http://ftp.crihan.fr/ubuntu/dists/xenial/main/binary-amd64/Release
Maj-Auto - Impossible de configurer les sources APT pour Ubuntu
```

La déclaration du proxy s'effectue dans l'onglet `Général` de l'interface de configuration du

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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=`

```
root@eolebase:~# CreoleGet .containers.services|grep \.name=
service0.name="networking"
service1.name="cron"
service10.name="exim4"
service11.name="eoleflask"
service12.name="nginx"
service13.name="ead3"
service14.name="genconfig"
service15.name="bastion"
service16.name="z_stats"
service2.name="rng-tools"
service3.name="ntp"
service4.name="nut-server"
service5.name="salt-api"
service6.name="salt-master"
service7.name="salt-minion"
service8.name="ead-server"
service9.name="ead-web"
root@eolebase:~#
```

Questions propres au partitionnement

Accéder aux partitions du module depuis un Live Linux

Lorsqu'on a recours à un live CD ou USB, il n'est pas possible d'accéder directement aux partitions.

```
# mkdir /media/partition
# mount /dev/sda2 /media/partition
mount: type inconnu de système de fichiers 'LVM2_member'
```

Installer LVM et procéder au montage

Sur des Linux Live ne gérant pas par défaut les volumes logiques il faut installer le paquet LVM :

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
# apt-get install lvm2
```

Afficher les groupes de volumes :

```
# vgscan
Reading all physical volumes. This may take a while...
Found volume group "eolebase-vg" using metadata type lvm2
```

Changer les attributs d'un groupe de volumes spécifiques

```
# vgchange -a y eolebase-vg
4 logical volume(s) in volume group "eolebase-vg" now active
```

2 méthodes pour lister les volumes logiques

```
# ll /dev/mapper/
total 0
drwxr-xr-x  2 root root     160 févr.  8 11:53 ./
drwxr-xr-x 19 root root    4460 févr.  8 11:53 ../
crw-------  1 root root 10, 236 févr.  8 11:53 control
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-home ->
../dm-4
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-root ->
../dm-0
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-swap_1 ->
../dm-1
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-tmp -> ../dm-2
lrwxrwxrwx  1 root root       7 févr.  8 11:53 eolebase--vg-var -> ../dm-3
```

ou

```
# lvdisplay
  --- Logical volume ---
  LV Path                /dev/eolebase-vg/swap_1
  LV Name                swap_1
  VG Name                eolebase-vg
  LV UUID                OO47WX-fpNm-5Ydq-9fSF-8rXN-iPYP-T3rCmm
  LV Write Access        read/write
  LV Creation host, time eolebase, 2017-02-06 21:48:52 +0100
  LV Status              available
  # open                 2
  LV Size                1,09 GiB
  Current LE             280
  Segments               1
  Allocation             inherit
  Read ahead sectors     auto
  - currently set to     256
  Block device           252:1
[...]
```

Montage de la partition :

```
# mount /dev/mapper/eolebase--vg-root /media/partition
```

Ajouter de l'espace disque à un volume LVM

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

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



Après avoir créé la nouvelle partition `/dev/sdb1` il peut être nécessaire de redémarrer le

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> 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` :

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

root@scribe:/dev/mapper#
```

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

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

Agrandir le volume logique

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

```
# lvextend -l +100%FREE /dev/scribe-vg/var
# e2fsck -f /dev/scribe-vg/var
# resize2fs /dev/scribe-vg/var
```

Redimensionner un volume LVM

Sur un serveur où une partition est saturée.

```
root@scribe:~# df -h
Sys. de fichiers            Taille Utilisé Dispo Uti% Monté sur
udev                          1,5G       0  1,5G   0% /dev
tmpfs                         301M     52M  250M  18% /run
/dev/mapper/scribe--vg-root   9,1G    2,6G  6,0G  30% /
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
tmpfs                          1,5G     28K  1,5G   1% /dev/shm
tmpfs                          5,0M       0  5,0M   0% /run/lock
tmpfs                          1,5G       0  1,5G   0% /sys/fs/cgroup
/dev/sda1                      687M    107M  531M  17% /boot
/dev/mapper/scribe--vg-tmp     1,8G    3,4M  1,7G   1% /tmp
/dev/mapper/scribe--vg-var     8,1G      8G  0,1G  99% /var
/dev/mapper/scribe--vg-home     18G    149M   18G   1% /home
tmpfs                          301M       0  301M   0% /run/user/0
root@scribe:~#
```

La partition `/var` est occupée à 99% alors que la partition `/home`, est occupée à 1%.
Réduire la partition `/home` de 1Go permet d'ajouter d'ajouter 1Go à `/var`.

Pour démonter le périphérique :

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

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

```
# lsof | grep home
```

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

Vérifier le support

Pour vérifier le support, lancer la commande :

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

Diminuer la taille de la première partition

Réduire le système de fichiers :

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

Réduire la partition logique :

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

Vérifier l'intégrité du système du système de fichiers :

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

Vérifier l'espace libéré

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

```
# vgdisplay
```

```
root@scribe:~# vgdisplay
  --- Volume group ---
  VG Name               scribe-vg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  6
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                5
  Open LV               5
  Max PV                0
  Cur PV                1
  Act PV                1
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

```
  VG Size               39,30 GiB
  PE Size               4,00 MiB
  Total PE              10060
  Alloc PE / Size       10060 / 39,30 GiB
  Free  PE / Size       0 / 0
  VG UUID               hcuPgd-tSEe-xu20-Q3XP-hrwU-5qfU-41Fkf3

root@scribe:~#
```

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

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

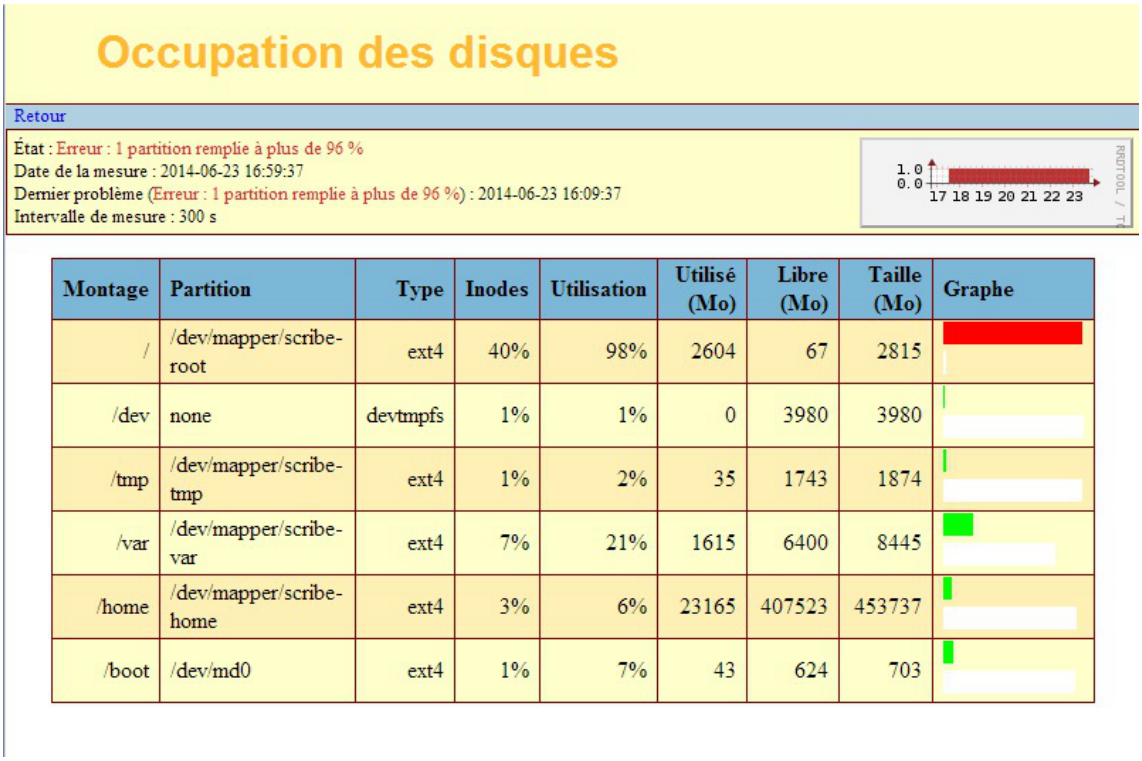
Procéder au montage du périphérique avec la commande `mount` :

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

Pensez à redémarrer les services qui ont précédemment été arrêtés.

Partition saturée

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

1.0
0.0
17 18 19 20 21 22 23

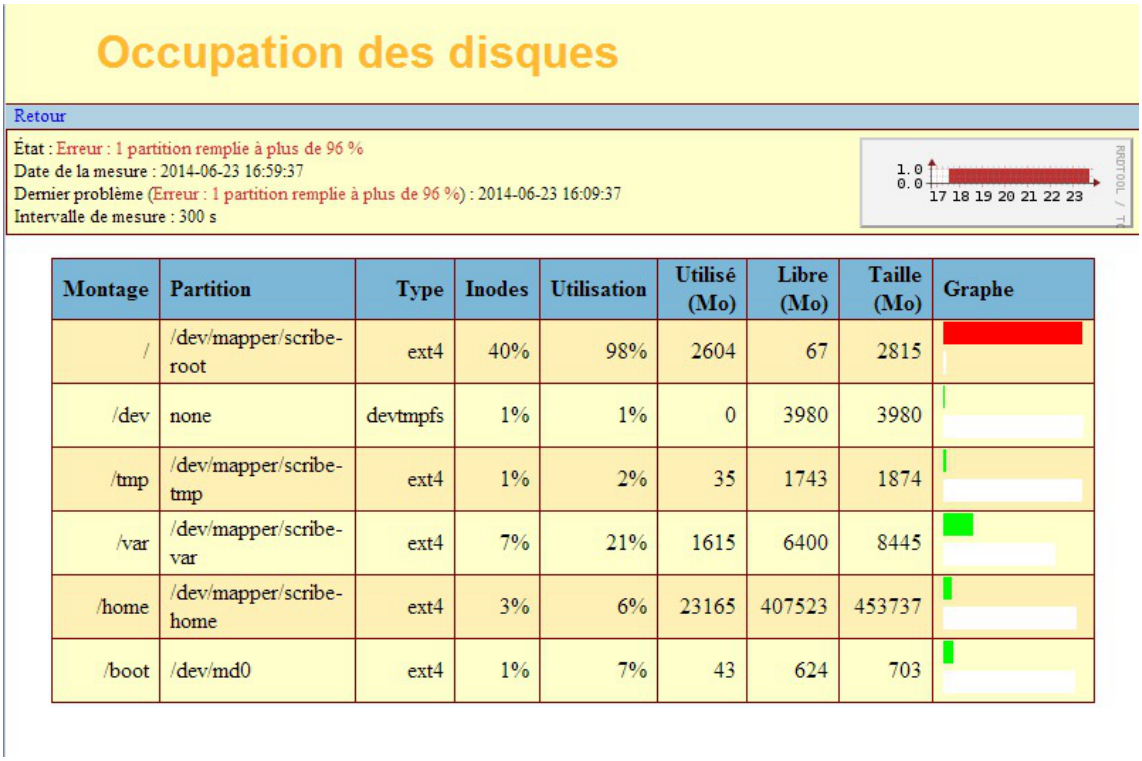
Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Une partition saturée apparaît en rouge dans l'EAD, la cause peut être :

- le manque de place disponible ;
- le manque d'inodes disponibles.

La cause de la saturation apparaît dans la page Occupation des disques, soit les inodes soit l'utilisation sont à un pourcentage élevé. La résolution du problème est différente selon le cas.

Partition / saturée



Occupation des disques

Retour

État : Erreur : 1 partition remplie à plus de 96 %
Date de la mesure : 2014-06-23 16:59:37
Dernier problème (Erreur : 1 partition remplie à plus de 96 %) : 2014-06-23 16:09:37
Intervalle de mesure : 300 s

1.0
0.0
17 18 19 20 21 22 23

Montage	Partition	Type	Inodes	Utilisation	Utilisé (Mo)	Libre (Mo)	Taille (Mo)	Graphe
/	/dev/mapper/scribe-root	ext4	40%	98%	2604	67	2815	
/dev	none	devtmpfs	1%	1%	0	3980	3980	
/tmp	/dev/mapper/scribe-tmp	ext4	1%	2%	35	1743	1874	
/var	/dev/mapper/scribe-var	ext4	7%	21%	1615	6400	8445	
/home	/dev/mapper/scribe-home	ext4	3%	6%	23165	407523	453737	
/boot	/dev/md0	ext4	1%	7%	43	624	703	

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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. 719]).

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. 719]).

Partition /var saturée en inode

Un nombre important de fichiers peut être du à un service mal configuré mais peut aussi être du à un fonctionnement normal. Il faut identifier le répertoire dans lequel il y a le plus de fichier.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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.

Questions propres à l'EAD

Problème d'accès à l'EAD avec un nom de domaine incorrect

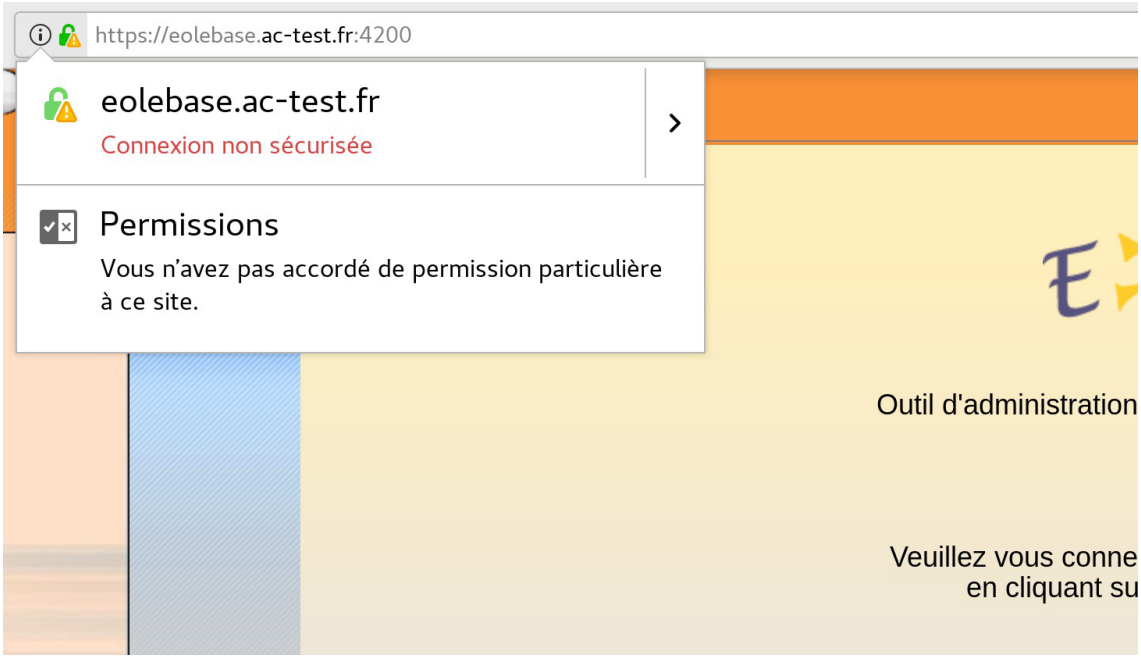
Pour avoir accès à l'EAD il faut impérativement que le nom de domaine soit présent dans le certificat SSL.

Il est notamment impossible de se connecter à l'EAD avec une simple adresse IP.

Il existe plusieurs méthodes pour connaître les noms de domaine présents dans le certificat SSL, par exemple il est possible d'utiliser un navigateur Internet.

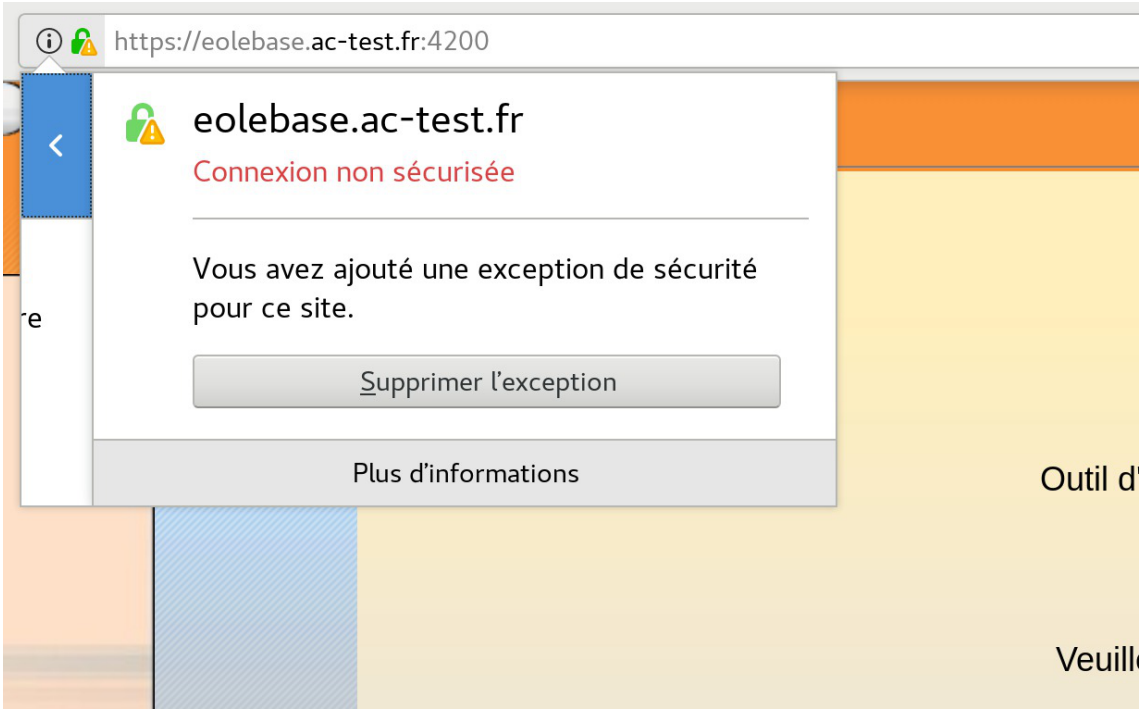
Exemple avec Firefox

- Cliquer sur le cadenas à côté de l'URL

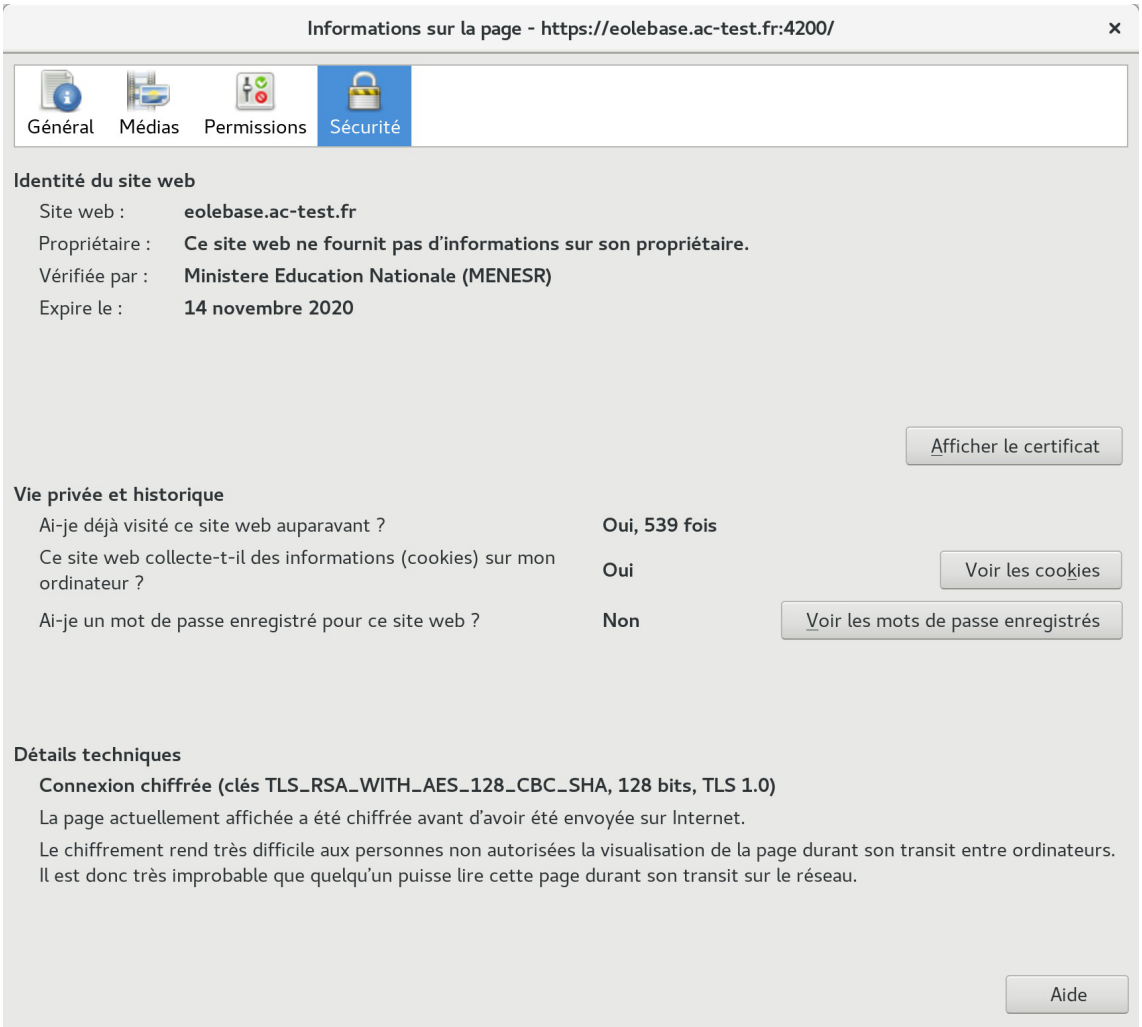


- Cliquer sur la flèche dirigée vers la droite pour afficher les détails de la connexion

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)



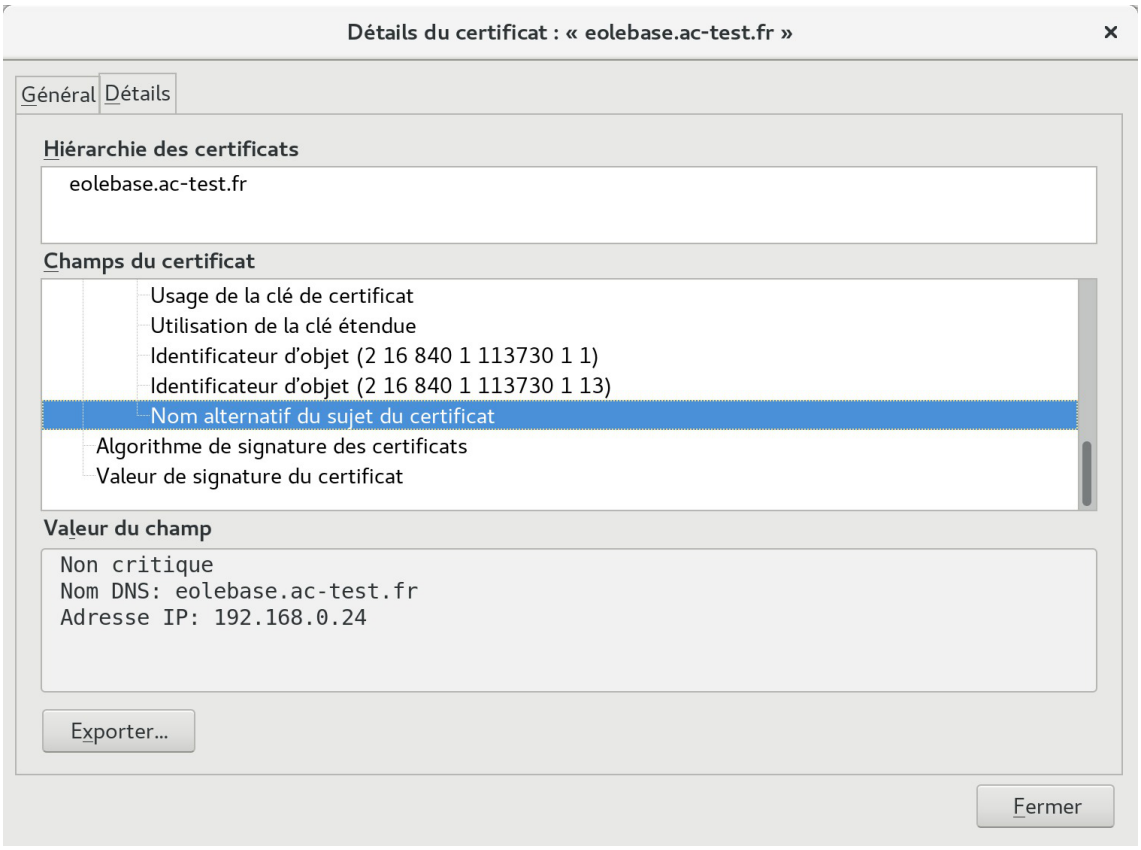
- Cliquer sur le bouton `Plus d'informations`, le nom de domaine principal du certificat apparaît alors dans la partie `Identité du site web` et `Site web`



- Il est possible que des noms alternatifs soient renseignés dans le certificat. Pour les retrouver, cliquer sur le bouton `Afficher le certificat`, puis sur l'onglet `Détails` et

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

sélectionner la ligne `Nom alternatif du sujet de certificat`, les noms alternatifs sont affichés dans la boîte `Valeur du champ`.



Attention, même si la bonne adresse IP apparaît dans le certificat, elle ne sera pas prise en compte.

Si le nom de domaine n'apparaît pas et que le certificat est de type autosigné, il faut le rajouter dans l'onglet `Certificats ssl` de l'interface de configuration du module en mode expert.

La modification, dans l'interface de configuration du module, de l'un des paramètres constituant un certificat (nom d'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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

> `# 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`

Services et journaux

Les fichiers journaux associés aux services EAD sont les suivants :

- `/var/log/rsyslog/local/ead-server/ead-server.info.log`
- `/var/log/rsyslog/local/ead-web/ead-web.info.log`

Si le service `ead-server` ne démarre plus ou si des actions EAD ne se chargent plus et que la consultation des fichiers journaux n'apportent pas d'informations pertinentes, le service peut être exécuté manuellement à l'aide des commandes suivantes :

```
service ead-server stop
cd /tmp
export PYTHONPATH=/usr/share
twistd3 -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, le service peut être exécuté manuellement à l'aide des commandes suivantes :

```
service ead-web stop
cd /tmp
export PYTHONPATH=/usr/share
twistd3 -noy /usr/share/ead2/frontend/frontend.tac
```

La combinaison de touches `ctrl+c` permet d'arrêter le programme.

La mire de connexion de l'EAD3 n'affiche pas les informations de contexte, il est impossible de se connecter

La mire de connexion s'affiche mais le domaine, le nom du module et de la machine ne s'affiche pas. Il est de plus impossible de se connecter.

> **Vérifier le certificat et l'acceptation du certificat.**
>
> Pour fonctionner la connexion à l'EAD3 a besoin d'un certificat valide et reconnue par la navigateur. Le cache du navigateur peut faire que la mire peut s'afficher alors que le certificat n'est plus reconnu.

Questions propres à l'interface de configuration du module

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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

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>/genconfig/`

ou : `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.eol.bak` est sauvegardé dans le répertoire `/etc/eole/` à la fin de l'instanciation et à la fin de la reconfiguration du serveur.

Cela permet de conserver la dernière configuration fonctionnelle du serveur.

À chaque reconfiguration du serveur un fichier `config.eol.bak.1` est généré. Celui-ci est une copie de la configuration fonctionnelle de l'état précédant.

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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

`/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.733] 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.713].



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.

2. Questions fréquentes propres au module Amon

Le service rvp est introuvable

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Le service rvp est introuvable :

```
root@amon:~# service rvp start
 Failed to start rvp.service: Unit rvp.service not found.
root@amon:~#
```

Les opérations du service *rvp* ont été intégrées dans le service *strongswan*, il faut donc l'utiliser en remplacement :

```
root@amon:~# service strongswan start
```

et

```
root@amon:~# service strongswan stop
```

Le service agregation est introuvable

Le service agregation est introuvable :

```
root@amon:~# service agregation status
● agregation.service
   Loaded: not-found (Reason: No such file or directory)
   Active: inactive (dead)
root@amon:~#
```

Les opérations du service *agregation* ont été déplacées dans un script, celui-ci peut être exécuté comme suit :

```
root@amon:~# agregation status
le service Agregation n'est pas démarré
root@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 squid stop
# rm -rf $(CreoleGet cache_dir)/*
# squid -f /etc/squid/squid.conf -z -N
# service squid 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)/*
# squid -f /etc/squid/squid2.conf -z -N
# service squid3-2 start
```


Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Problèmes avec le protocole HTTPS

La règle de pare-feu par défaut redirige le trafic Internet directement vers le proxy local.

C'est le mécanisme de proxy transparent.

Cette méthode ne permet toutefois pas de laisser passer le flux chiffré (HTTPS) par ce même mécanisme.

Pour accéder aux sites en HTTPS, il est nécessaire de configurer le proxy sur les postes clients (par exemple : avec ESU sur le module Scribe).

L'option `Destinations non redirigées sur le proxy` disponible en mode expert dans l'onglet `Interface-1` permet, à l'inverse, de déclarer des exceptions.

Lenteur lors de la navigation web

Un filtrage web e2guardian est en place et la navigation web est très lente.

Dans les logs apparaissent des erreurs Squid à répétition (`TCP_DENIED/407`) :

```
Mar  01  10:36:01  amon  (squid):  1363253761.503  51  192.168.10.10 TCP_DENIED/407 4006 GET http://linuxfr.org/ - NONE/- text/html
```

Augmenter le nombre de processus e2guardian maximum dans le filtre

Avant d'augmenter le nombre de processus, on peut vérifier la valeur configurée dans l'interface de configuration du module. Celle-ci est fixée à `256` par défaut et se trouve dans l'onglet `Filtrage web` en mode expert.

Une commande rudimentaire permet de se rendre compte du nombre de processus effectivement exécutés sur le serveur mais elle ne permet pas de distinguer à quelle instance appartiennent les processus et renvoie aussi les processus qui servent a contrôler les autres processus :

```
# ps ax | grep -c guardian
```

La commande `diagnose` permet de connaître précisément le nombre de processus e2guardian exécutés par instance :

```
*** Filtre web
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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Compatibilité du module Sphynx avec les différentes versions du module Amon

Un serveur Sphynx 2.7 est-il en mesure d'établir des tunnels VPN avec des serveurs Amon 2.8 ?

Inversement, un Sphynx 2.8 est-il en mesure d'établir des tunnels VPN avec des serveurs Amon 2.7 et 2.6 ?

Pour les connexions VPN, la compatibilité est assurée par strongSwan

Actuellement toutes les versions maintenues du module Sphynx peuvent établir des tunnels VPN 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.732] 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/.

Quant-au serveur Sphynx utilisé pour la gestion des VPN dans l'application ARV, il est impératif d'utiliser une version EOLE supérieure ou égale à la version des serveurs Amon/Amonecole/Sphynx importés dans l'application via Zéphir.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Glossaire

Active Directory *= AD*	Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Source Wikipédia : https://fr.wikipedia.org/wiki/Active_Directory
Adressage statique	Les adresses IP statiques (ou fixes) sont définies manuellement, elles ne changeront pas sauf si elles sont modifiées manuellement.
adresse MAC *= Media Access Control*	Une adresse MAC, parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés (tablette tactile, smartphone,consoles de jeux). Une adresse MAC est généralement représentée sous la forme hexadécimale en séparant les octets par un double point. Par exemple 5E:FF:56:A2:AF:15. Source Wikipédia : http://fr.wikipedia.org/wiki/Adresse MAC
Agent Zéphir	Les agents Zéphir sont des sondes qui génèrent divers statistiques et rapports sur les modules EOLE. 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. 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.
Agrégation de liens Ethernet *= Bonding*	L'agrégation de liens (niveau 2) est une technique utilisée dans les réseaux informatiques, permettant le regroupement de plusieurs ports réseau et de les utiliser comme s'il s'agissait d'un seul. Le but est d'accroître le débit au-delà des limites d'un seul lien, et éventuellement de faire en sorte que les autres ports prennent le relais si un lien tombe en panne (redondance). Source Wikipedia : https://fr.wikipedia.org/wiki/Agrégation_de_liens [https://fr.wikipedia.org/wiki/Agr%C3%A9gation_de_liens]
Agrégation de routes IP	L'agrégation de routes IP (niveau 3) permet la mise en place d'une répartition de charge ou d'une haute disponibilité pour les sorties Internet.
AGRIATES	De responsabilité partagée entre les collectivités locales et les

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

= Accès Généralisé aux Réseaux Internet Académiques et Territoriaux pour les Établissements Scolaires	académies, ces réseaux de concentration des établissements scolaires couvrent à ce jour l'ensemble de lycées et collèges et devraient s'étendre aux secteurs du primaire. L'interconnexion des réseaux AGRIATES de chaque académie forme une partie du réseau RACINE. Par extension, les applications AGRIATES sont les applications Intranet accessibles aux établissements connectés au réseau AGRIATES, à savoir essentiellement, mais pas uniquement, les applications internet à usage des services administratifs des établissements. RACINE-AGRIATES a pour objectif la fourniture d'un support sécurisé pour les échanges d'information (VPN) entre le réseau de l'administration des établissement et leur rectorat de rattachement. L'organisation utilisée pour RACINE-AGRIATES est celle mise en place pour le réseau RACINE. http://www.igc.education.fr/agriates/agriates.htm C'est à la fois une zone de confiance sur le réseau des rectorats et un ensemble de contraintes techniques auxquelles doivent répondre les dispositifs d'accès des établissements. RACINE-AGRIATES fait partie du projet réseau RACINE, dont l'objectif consiste à fournir un support sécurisé pour les échanges d'information (ou Réseau Virtuel Privé (RVP)) entre entités du ministère en s'appuyant sur des infrastructures réseau ouvertes. RACINE-AGRIATES a ainsi pour objectif la fourniture d'un support sécurisé pour les échanges d'information (RVP) entre le réseau de l'administration des établissements et leur rectorat de rattachement. RACINE-AGRIATES rassemble dans une même "zone de confiance" académique les établissements scolaires et les services académiques. Ce nouveau réseau privé virtuel sécurisé est l'Intranet académique.
AMD64	AMD64 est le nom d'une architecture processeur développée par la société AMD. Cette architecture est compatible avec le standard 32 bits x86 d'Intel.
ANSSI *= Agence nationale de la sécurité des systèmes d'information*	Service à compétence nationale, l'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale. Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. Source : https://www.cert.ssi.gouv.fr/a-propos/
Anti-spoofing *= Anti-usurpation d'adresse IP*	L'usurpation d'adresse IP est une technique utilisée en informatique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	L'anti-spoofing sont des réglages du noyau et du réseau qui permettent de lutter contre l'usurpation d'adresse IP.
APT *= Advanced Packaging Tool*	APT est un ensemble d'outils fondamentaux au cœur de Debian. Il permet : • d'installer des applications ; • de supprimer des applications ; • de garder les applications à jour ; • et encore bien d'autres choses... APT, qui essentiellement résout les problèmes de dépendances et récupère les paquets désirés, fonctionne avec `dpkg`, 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.
ARV *= Administration de Réseaux Virtuels*	ARV permet de construire un modèle de configuration RVP. C'est un logiciel qui permet de générer des configurations RVP pour strongSwan. http://www.strongswan.org/
Autorité de Certification *= CA : Certification Authority*	AC est l'acronyme de Autorité de Certification. Une autorité de certification est une société ou un service administratif chargé de créer, de délivrer et de gérer des certificats électroniques.
Balise méta	Information sur la nature et le contenu d'une page web, ajoutée dans l'en-tête de la page HTML.
Bareos	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. 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.
bastion	bastion est un service qui récupère les règles par défaut des zones réseaux utilisées par le module ainsi que toutes les règles personnalisées : • les règles optionnelles de l'EAD ; • les postes et les groupes de postes interdits ou restreints dans l'EAD ; • les règles sur les horaires de l'EAD ; • les règles ipsets (exceptions sur une directive) ; • les règles de la QOS ; • les règles tcpwrapper (host allow et hosts deny).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	Le service bastion gère également les règles iptables dans les conteneurs lorsque le module en est pourvu. La liste des actions du service se trouve dans le script `/usr/share/era/bastion.sh`. Le service bastion met en cache les règles mais ne les régénère pas à chaque fois. À partir de la version 2.6.1, seules les commandes `reconfigure` et `bastion regen` régénèrent les règles.
BIND *= Berkeley Internet Name Domain*	BIND est un serveur DNS libre. C'est le plus utilisé sur Internet. http://www.isc.org/downloads/bind/
broadcast	le broadcast désigne une méthode de transmission de données à l'ensemble des machines d'un réseau. 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. Source : http://fr.wikipedia.org/wiki/Broadcast_(informatique)
CAS *= Central Authentication Service*	CAS est un système d'authentification unique créé par l'université de Yale : on s'authentifie sur un site Web, et on est alors authentifié sur tous les sites Web qui utilisent le même serveur CAS. Il évite de s'authentifier à chaque fois qu'on accède à une application en mettant en place un système de ticket.
CERT-FR *= Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*	Le CERT-FR (anciennement CERTA) est une des composantes curatives complémentaires des actions préventives assurées par l'ANSSI. En tant que CERT (Computer Emergency Response Team) national, il est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il assure une permanence de ses activités 24h/24, 7j/7.S Ses principales missions peuvent se décliner ainsi : • détecter les vulnérabilités des systèmes, au travers notamment d'une veille technologique ; • piloter la résolution des incidents, si besoin avec le réseau mondial des CERT ; • aider à la mise en place de moyens permettant de se prémunir contre de futurs incidents ; • organiser la mise en place d'un réseau de confiance. Source : https://www.cert.ssi.gouv.fr/

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

CETIAD *= Centre d'Études et de Traitements Informatiques de l'Académie de Dijon*	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 du Général Delaborde dans les nouveaux locaux du rectorat de l'académie de Dijon en novembre 2012.
CIDR *= Classless Inter-Domain Routing*	La notation CIDR permet de diminuer la taille de la table de routage contenue dans les routeurs. Elle donne le numéro du réseau suivi par une barre oblique (/) et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau. Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19 (19 bits à la valeur 1, suivis de 13 bits 0). Source : http://fr.wikipedia.org/wiki/Sous-réseau
CN *= Common Name*	Valeur permettant d'identifier le serveur dans le certificat.
Cntlm	Cntlm proxy d'authentification NTLM rapide écrit en C. Il s'intercale entre le poste client et le proxy. Il oblige l'utilisateur à renseigner son identifiant/mot de passe dans une fenêtre surgissante (popup). Il ouvre une socket en écoute et gère la transmission de chaque requête au proxy parent. Si une connexion au proxy parent est créée à nouveau et authentifiée, la connexion précédente est mise en cache et est réutilisée pour une plus grande efficacité. Cntlm intègre également la redirection transparente de port TCP/IP. Il existe de nombreuses fonctions avancées telles que le support de NTLMv2, la protection de mot de passe, le hachage de mot de passe,etc. Il est peu gourmand en terme de ressources. http://cntlm.sourceforge.net/
Commutateur réseau *= switch*	Un commutateur réseau (en anglais switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage. Dans les réseaux locaux (LAN), il s'agit le plus souvent d'un boîtier disposant de plusieurs ports Ethernet (entre 4 et plusieurs centaines), il a donc la même apparence qu'un concentrateur (hub) mais peut être configuré pour un accès direct à Internet, ce qui n'est pas possible pour un hub. Il existe aussi des commutateurs pour tous les types de réseau en mode point à point comme pour les réseaux ATM, relais de trames, etc. Source : http://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau
Consistent Network Device Naming	Le nommage des interfaces réseau en ethX n'était pas assez fiable. Si on insérait une carte réseau supplémentaire dans le système, la

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	nouvelle carte réseau pouvait remplacer eth0 et la déplacer en eth1. Le nom des interfaces est fonction de leur attachement au système et non plus simplement de l'ordre matériel. Consistent Network Device Naming est une convention pour le nommage des cartes réseau sous GNU / Linux. Cette convention a été implémentée au travers du module kernel biosdevname par la société Dell. Le schéma de nommage de biosdevname respecte les conventions suivantes : • em[1−N] pour les cartes physiques embarquées, le numéro correspond à l'emplacement interne de la carte sur la carte mère (numéro renvoyé par la commande `lspci`) ; • p<numeroEmplacement>p<numeroEmplacementPhysique> pour les cartes PCI, le numéro de l'emplacement physique commençant à 1 ; • un suffixe _vf est ajouté au matériel NPAR et SR-IOV, le numéro dépend du nombre de partitions ou des fonctions de virtualisation utilisées et sur quel port ; • d'autres conventions comme les suffixes vlan et alias sont inchangées et reste applicables. Source : http://en.wikipedia.org/wiki/Consistent_Network_Device_Naming systemd/udev utilisent leur propre schéma de nommage similaire à biosdevname. Les principales différences sont supportées nativement par udev : • carte embarquée et numéro interne de l'emplacement de la carte (numéro renvoyé par la commande `lspci`) (exemple: eno1) ; • carte PCI Express et numéro interne de l'emplacement de la carte (exemple: ens1) ; • carte et localisation du connecteur au niveau du matériel (exemple: enp2s0) ; • carte avec l'adresse MAC (exemple: enx78e7d1ea46da) ; • pour les cartes nommées nativement dans le kernel (exemple: eth0).
Conteneur	Un conteneur est une zone isolée à l'intérieur du système qui a un espace spécifique du système de fichiers, un réseau, des processus, des allocations mémoires et processeurs, comme s'il s'agissait de plusieurs serveurs physiques séparés. Contrairement à la virtualisation, une seule instance du noyau est présente pour l'ensemble des conteneurs et du maître.
Corosync Cluster Engine	Corosync Cluster Engine est un moteur libre de cluster. C'est un

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

= Corosync	système de communication avec des fonctionnalités supplémentaires pour la mise en œuvre de la haute disponibilité dans les applications. Le projet fournit quatre fonctionnalités principales : • 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 ; • un système de notification qui se déclenche lorsque un quorum est atteint ou perdu. Sources : https://fr.wikipedia.org/wiki/Corosync_Cluster_Engine et http://clusterlabs.org/
CPU *= Central Processing Unit*	Le CPU , ou en français UCT pour Unité Centrale de Traitement, désigne le ou les microprocesseurs d'un ordinateur. C'est lui qui exécute les programmes informatiques.
Creole *= Création EOLE*	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.
creoled	creoled est un service permettant d'effectuer des requêtes sur la configuration Creole depuis la boucle locale sur le maître et dans les conteneurs.
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 *= Comma-separated values*	Le CSV est un format informatique ouvert représentant des données tabulaires sous forme de valeurs séparées par des virgules. Il est souvent utilisé pour l'interopérabilité entre applications.
DHCP	Dynamic Host Configuration Protocol (DHCP) est un protocole réseau

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

= Dynamic Host Configuration Protocol	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 `active_tags` 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.
DMZ *= Demilitarized Zone*	En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local. Source Wikipédia : http://fr.wikipedia.org/wiki/Zone démilitarisée (informatique)
DN *= Distinguished Name*	Identifiant unique dans le cadre des annuaires LDAP.
DNS *= Domain Name System*	Un DNS est un service permettant de traduire un nom de domaine en informations de plusieurs types. L'usage le plus fréquent étant la traduction d'un nom de domaine en adresses IP. Source : http://fr.wikipedia.org/wiki/Dns
Dstat	Dstat est un outil polyvalent de statistiques des ressources. Il peut remplacer vmstat, iostat et ifstat. Dstat surmonte certaines des limitations de ces programmes et ajoute quelques fonctionnalités supplémentaires.
DTD *= Document Type Definition*	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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	document parce qu'on peut former avec un texte complet. Une DTD décrit les documents à deux niveaux : • la structure logique, que l'on peut assimiler à la syntaxe abstraite ; • la structure physique, que l'on peut assimiler à la syntaxe concrète. Source : http://fr.wikipedia.org/wiki/Document_Type_Definition
e2guardian	e2guardian est un fork de DansGuardian. La dernière version stable de DansGuardian est sortie depuis un très long moment (2009) et plus récemment, suite au désengagement du créateur originel Daniel Barron, le projet a été migré sur la plateforme sourceforge et repris en main par un nouveau mainteneur. DansGuardian devait devenir un projet plus communautaire mais après diverses versions alpha le projet n'a pas réellement repris vie. Depuis 2012 le travail a repris pour incorporer toutes les évolutions et corrections proposées par de nombreux contributeurs et le logiciel est publié sous le nom de e2guardian. http://e2guardian.org
EAD *= EOLE ADmin*	L'EAD est l'interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse `https://<adresse_module>:4200`. L'authentification peut être locale et/ou au travers d'EoleSSO (authentification unique). L'EAD est composé de deux parties : • un serveur de commandes (service ead-server), présent et actif sur tous les modules ; • une interface web (service ead-web), présent et actif sur tous les modules. Chaque module dispose d'une interface utilisateur EAD. Certains modules (Zéphir, Sphynx, ...) ne disposent que de la version de base qui permet d'effectuer les tâches de maintenance (mise à jour du serveur, diagnostic, arrêt du serveur, ...). Une version plus complète existe pour les autres modules (Horus, Scribe, Amon, ...) incluant des fonctionnalités supplémentaires.
EAD3 *= EOLE ADmin 3*	L'EAD3 est une interface d'administration des modules EOLE. Il s'agit d'une interface web, accessible uniquement en HTTPS avec un navigateur web à l'adresse https://<serveur>/ead/. Les briques de l'EAD3 sont préinstallées sur les modules à partir de la version EOLE 2.6.1, mais non activées. Certaines de ses fonctionnalités ne sont accessibles que sur la version d'EOLE en cours de développement.
ELF	

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

= Executable and Linkable Format	ELF est un format de fichier binaire utilisé pour l'enregistrement de code compilé
Envole	Envole est un Espace Numérique Personnel pour l'Éducation. Il propose une interface de type portail Web 2.0 qui permet l'interaction entre un utilisateur et son environnement numérique résultant de l'utilisation de services hétérogènes. Il centralise dans une seule interface l'ensemble des applications de l'utilisateur : mail, agenda, dossier personnel, B2I, blog, gestion de notes, gestion des absences, etc ... 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/
eole-schedule	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. Sur un module instancié, la commande suivante permet d'obtenir la liste des tâches planifiées : `manage_schedule -l`.
ERA *= Éditeur de Règles pour le module Amon*	ERA est une application graphique de génération et de gestion de règles de sécurité adaptée au module pare-feu Amon. À partir du fichier XML de description du pare-feu, un script de règles iptables pour Netfilter est généré de manière à implémenter ces règles sur le module pare-feu Amon. La génération directe de règles iptables est également possible, permettant d'utiliser ERA pour d'autres types de serveurs sous GNU/Linux.
Erlang	Erlang est un langage de programmation, supportant plusieurs paradigmes : concurrent, temps réel, distribué. Son cœur séquentiel est un langage fonctionnel à évaluation stricte, affectation unique, au typage dynamique fort. Sa couche concurrente est fondée sur le modèle d'acteur. Il possède des fonctionnalités de tolérance aux pannes et de mise à jour du code à chaud, permettant le développement d'applications à très haute disponibilité. Erlang est conçu pour s'exécuter sur une machine virtuelle spécifique appelée BEAM. Source Wikipédia : http://fr.wikipedia.org/wiki/Erlang_%28langage%29
Exim	Exim est un serveur de messagerie électronique (ou Mail Transfer Agent en anglais) utilisé sur de nombreux systèmes de type UNIX. Il est l'un des serveurs de messagerie électronique (MTA) les plus

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	flexibles et robustes. Exim est hautement configurable : il possède des fonctionnalités manquantes dans les autres serveurs de courriel. http://www.exim.org/
Extrémité	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.
Fichier DEB	Un fichier DEB est un package permettant d'installer une application sous les systèmes Linux Debian. La distribution Debian propose un outil de gestion de package permettant d'automatiser l'installation, la configuration et la mise à jour des logiciels installés par ce biais.
Filtrage syntaxique	Système de pondération détectant des mots interdits dans une page et lui assignant un score en fonction de la gravité et du nombre de mots détectés. Le proxy bloquera les pages dont le score dépasse un certain seuil.
Flux	Lien entre deux zones.
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".
FOG *= Free OpenSource Ghost*	FOG est un logiciel libre de déploiement d'OS. FOG est installable facilement sur le module EoleBase versions 2.8 et supérieures. https://pcll.ac-dijon.fr/eole/installation-de-fog-sur-eolebase-2-8/ https://fogproject.org/
FTP *= File Transfert Protocol*	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. La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS. FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande). FTP, qui appartient à la couche application du modèle OSI et du

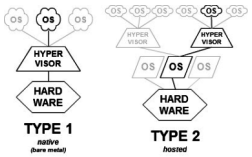
Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	modèle ARPA, utilise une connexion TCP. Par convention, deux ports sont attribués (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990. Ce protocole peut fonctionner avec IPv4 et IPv6. (Source : http://fr.wikipedia.org/wiki/File_Transfer_Protocol)
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 *= GNU is Not Unix*	GNU est l'acronyme récursif de GNU is Not Unix. Projet fondé en 1984, il vise à produire un OS complet de type Unix. Le noyau propre au projet n'étant pas fini, GNU est le plus souvent utilisé avec Linux. On parle alors de système GNU/Linux.
GNU GRUB *= GRand Unified Bootloader*	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 *= GnuPG*	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
GPO *= Group Policy Objects* *= stratégies de groupe*	Les stratégies de groupe (ou GP pour Group Policy) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection de dossiers ainsi que la gestion des fichiers en mode déconnecté. Les stratégies de groupe sont gérées à travers des objets de stratégie de groupe communément appelés GPO (Group Policy Objects). https://fr.wikipedia.org/wiki/Strat%C3%A9gies_de_groupe
Gunicorn *= Green Unicorn (Licorne Verte)*	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.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	Source Wikipédia : http://fr.wikipedia.org/wiki/Gunicorn_(HTTP_server)
Haute Disponibilité *= High Availability ou HA*	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 : • 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 *= HyperText Transfer Protocol - protocole de transfert hypertexte*	HTTP est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (le S signifiant sécurisé) est la variante du HTTP sécurisée par l'usage des protocoles SSL ou TLS. HTTP est un protocole de la couche application. Dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS).
https://cloud-init.io/	Cloud-init fournit un environnement et un outil pour configurer et personnaliser les instances de machines virtuelles pour les plateformes de nuages de type infrastructure en tant que service (IaaS). Il peut par exemple régler une locale et un nom d'hôte par défaut, créer des clés d'hôtes SSH privées, installer des clés publiques SSH pour se connecter à un compte par défaut, mettre en place des points de montage éphémères et lancer des scripts fournis par l'utilisateur. Diverses méthodes sont prises en charge pour envoyer des données vers l'instance au démarrage, dont les interfaces standard de plateformes multiples. https://cloud-init.io/
Hyperviseur	Un hyperviseur est une plate-forme de virtualisation qui permet à plusieurs systèmes d'exploitation de travailler sur une même machine physique en même temps. Les hyperviseurs sont classés actuellement en deux catégories : • Type I, natif : un hyperviseur de Type 1 est un logiciel qui s'exécute directement sur une plateforme matérielle ; cette plateforme est alors considérée comme outil de contrôle de système d'exploitation. Un système d'exploitation secondaire peut, de ce fait, être exécuté au-dessus du matériel ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	• Type II : un hyperviseur de Type 2 est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation. Un système d'exploitation invité s'exécutera donc en troisième niveau au-dessus du matériel. Les systèmes d'exploitation invités n'ayant pas conscience d'être virtualisés, ils n'ont pas besoin d'être adaptés.  Source Wikipédia : http://fr.wikipedia.org/wiki/Hyperviseur
ICAP *= Internet Content Adaptation Protocol*	ICAP est un protocole mis au point en 2000 par un consortium comprenant entre autres les sociétés Network Appliance, Akamai Technologies et Novell. L'objectif du protocole est de fournir une interface générique pour la communication avec les solutions de filtrage de contenu sur Internet. Source : https://fr.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol
ICMP *= Internet Control Message Protocol*	Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.
IGC/A *= Infrastructure de Gestion de la Confiance de l'Administration*	L'infrastructure de gestion de la confiance de l'administration, dite « IGC/A », est une infrastructure de gestion de clés cryptographiques (IGC) opérée par l'Agence nationale de la sécurité des systèmes d'information, l'autorité de certification racine de l'État français. Les certificats émis par l'IGC/A permettent d'identifier officiellement les autorités de certification des administrations de l'État français. Ils attestent également de la qualité des pratiques de gestion des clés publiques mises en œuvre par ces autorités. Ils sont délivrés au terme d'un audit et peuvent être révoqués en cas de défaillance. Source : https://www.ssi.gouv.fr/administration/services-securises/igca/
Image ISO *= Image disque*	Une image ISO est une archive proposant la copie conforme d'un disque optique ou magnétique. L'opération de gravure de l'image ISO consiste à recopier cette structure sur un disque optique.
IMAP *= Internet Message Access Protocol*	IMAP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Mais contrairement au protocole POP, il permet de laisser les messages sur le serveur, ce qui présente un gros avantage pour consulter sa messagerie depuis plusieurs postes équipés de clients lourds.
INI	Un fichier INI est un fichier de configuration dans un format de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	données introduit par les systèmes d'exploitation Windows en 1985. Par convention les noms de ces fichiers portent l'extension « `.ini` ». Les fichiers INI sont des fichiers texte qui peuvent être manipulés avec un logiciel courant de type éditeur de texte. La valeur de chaque paramètre de configuration est indiquée par une formule : paramètre = valeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Fichier_INI
instance *= instanciation, instancier*	Instancier un serveur correspond à la troisième étape de mise ne œuvre d'un module EOLE. Cette phase permet d'écrire les fichiers de configuration et de lancer ou de redémarrer les services d'après les valeurs renseignées lors de l'étape de configuration. L'instanciation prépare le système en vue de sa mise en production et s'exécute à l'aide de la commande `instance`.
InterBase	InterBase est un moteur de base de données. Il a été choisi par le ministère de l'Éducation nationale pour supporter les bases de données utilisées par les logiciels nationaux (comme GFC et SELENE, par exemple). Source Wikipédia : http://fr.wikipedia.org/wiki/InterBase
iptables	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. 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.
Jinja2	Jinja2 est un moteur de templates pour le langage de programmation Python. http://jinja.pocoo.org/docs/2.9/
journald *= systemd-journald*	journald est un service système chargé de collecter et de stocker les journaux des applications. Source : https://www.freedesktop.org/software/systemd/man/systemd-journald.se
JSON *= JavaScript Object Notation*	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. 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. Un document JSON ne comprend que deux types d'éléments structurels : • des ensembles de paires nom / valeur ;

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	• des listes ordonnées de valeurs. Ces mêmes éléments représentent trois types de données : • des objets ; • des tableaux ; • des valeurs génériques de type tableau, objet, booléen, nombre, chaîne ou null. Source Wikipédia : http://fr.wikipedia.org/wiki/JavaScript_Object_Notation
Kerberos	Kerberos est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes (chiffrement symétrique) et l'utilisation de tickets, et non de mots de passe en clair, évitant ainsi le risque d'interception frauduleuse des mots de passe des utilisateurs. Source Wikipédia : http://fr.wikipedia.org/wiki/Kerberos_(protocole)
Keycloak	Keycloak est un outil libre et moderne de gestion d'identité et des accès (IAM).
KVM *= Kernel-based Virtual Machine*	KVM est un hyperviseur libre natif (Type I) pour Linux. KVM est une instance modifiée de QEMU pour être prise en charge en tant que module kernel kvm. KVM est intégré dans le noyau Linux depuis la version 2.6.20. Lorsqu'on parle de KVM, on parle généralement de l'ensemble : version modifiée de QEMU et module kvm. Source : http://fr.wikipedia.org/wiki/Kernel-based_Virtual_Machine
L'expérience à tâtons	Ne pouvant établir avec certitude qui de l'équipe a introduit ce type d'expérience dans la documentation du module Amon en version 2.2, l'équipe dans son intégralité revendique la paternité du concept.
LDAP *= Lightweight Directory Access Protocol*	À l'origine un protocole permettant l'interrogation et la modification des services d'annuaire, LDAP a évolué pour représenter une norme pour les systèmes d'annuaires.
LDM *= LTSP Display Manager*	LDM est le gestionnaire d'affichage spécialement écrit pour LTSP.
LemonLDAP *= LemonLDAP::NG*	LemonLDAP::NG est une infrastructure d'authentification unique distribuée (SSO – Single Sign On) avec gestion centralisée des droits. Il se présente sous la forme d'une suite logicielle libre reposant sur le serveur web Apache. Source : http://www.starxpert.fr/lemon-ldap/
Let's Encrypt *= LE*	Let's Encrypt est une autorité de certification qui fournit des certificats gratuits X.509 pour le protocole cryptographique TLS au moyen d'un processus automatisé destiné à se passer du processus complexe actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	des sites internet. Source Wikipédia : https://fr.wikipedia.org/wiki/Let's_Encrypt
libvirt	libvirt est une bibliothèque, une API, un daemon et des outils en logiciel libre de gestion de la virtualisation. Elle est notamment utilisée par KVM, Xen, VMware ESX, QEMU et d'autres solutions de virtualisation. Elle est notamment utilisée par la couche d'orchestration des hyperviseurs. Source : http://fr.wikipedia.org/wiki/Libvirt
Licence CeCILL	Acronyme pour CEa Cnrs Inria Logiciel Libre. C'est une licence libre de droit français compatible avec la licence GNU GPL.
Linux *= Kernel Linux*	Le noyau Linux est un noyau de système d'exploitation de type Unix. Le noyau Linux est un logiciel libre développé initialement par Linus Torvalds. Il a officiellement vu le jour en 1991. Formellement, « Linux » est le nom du seul noyau, mais dans les faits, on appelle souvent « Linux » l'ensemble du système d'exploitation, aussi appelé « GNU/Linux », voire l'ensemble d'une distribution Linux.
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.
live CD	Un live CD, ou CD autonome en français, est un CD qui contient un système d'exploitation exécutable sans installation, qui se lance au démarrage de l'ordinateur. On désigne par live CD le système d'exploitation présent sur un support externe amorçable. Le support de stockage peut être un CD, un DVD ou encore une clé USB. Source : https://fr.wikipedia.org/wiki/Live_CD
LTS *= Long Term Support*	Certaines versions d'Ubuntu sont estampillées LTS. Ces versions, publiées tous les deux ans au mois d'avril, sont soutenues pour une durée prolongée de 60 mois (5 ans). Le label LTS : • la récupération des paquets de Debian se fait de manière plus conservatrice, synchronisée depuis Debian testing plutôt que Debian unstable ; • la stabilisation de la distribution commence tôt dans le cycle de développement en limitant le nombre de nouveautés. L'équipe d'Ubuntu fait une sélection entre les paquets qui doivent être inclus dans une distribution maintenue sur une durée d'au plus 5 ans et ceux qui pourront être optionnellement installés par les

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	utilisateurs ; • les changements structurels majeurs sont le plus possible évités, comme le changement des applications incluses par défaut dans la distribution, la transition vers d'autres bibliothèques ou les changements des couches basses du système. Une version LTS est : • tournée vers les entreprises : ces versions sont pensées pour le déploiement dans des parcs de serveurs et de postes de travail dont la durée de vie est longue et où les changements sont peu fréquents ; • compatible avec les nouveaux matériels : des révisions sont publiées à intervalles réguliers (une point release) pour ajouter la prise en charge de nouveaux matériels pour serveurs et postes de travail ; • davantage testée : la phase de développement alpha est réduite, afin d'étendre davantage la période de stabilisation bêta pour récolter le plus de retours d'expérience et de rapports de bogues et pour stabiliser l'ensemble de la distribution. Clairement, une version LTS n'est pas : • une version incluant de nombreuses nouveautés : l'effort est surtout tourné vers la stabilisation et le renforcement des fonctionnalités existantes. Si des exceptions sont accordées à certains projets, elles sont documentées et leur intégration dans une version LTS doit être complétée pour la version bêta 1 du cycle de développement ; • une version d'avant-garde : plutôt que d'importer les paquets de Debian depuis sa version unstable, ceux-ci sont tirés depuis la version testing de Debian. Même si certaines nouveautés ne sont pas incluses dans ces paquets, il y a plus de bénéfices à importer des paquets testés qui introduisent moins de bogues et moins de régressions.
LVM *= Logical Volume Management*	La gestion par volumes logiques est à la fois une méthode et un logiciel. Elle permet le découpage, la concaténation, le redimensionnement et l'utilisation des espaces de stockage. Le logiciel permet de gérer, de sécuriser et d'optimiser de manière souple les espaces de stockage sur les systèmes d'exploitation de type UNIX.
LXC *= Linux Containers*	LXC, contraction de l'anglais Linux Containers, est un système de virtualisation au niveau système d'exploitation utilisé pour faire fonctionner de multiples environnements Linux isolés les uns des autres sur un seul et même système hôte. Le conteneur LXC n'est pas une machine virtuelle mais uniquement un environnement virtualisé qui dispose de ses propres processus et de son propre réseau (isolés

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	du système physique hôte).
man in the middle *= homme du milieu*	L'attaque de l'homme du milieu (HDM) ou man in the middle attack (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion à Internet de l'internaute lambda. L'attaquant doit d'abord être capable d'observer et d'intercepter les messages d'une victime à l'autre. Source Wikipédia : http://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
MD5 *= Message Digest 5*	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
MEEM *= Ministère de l'Environnement, de l'Énergie et de la Mer*	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. 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 : • 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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	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). • Ministère de l'Environnement, de l'Énergie et de la Mer (depuis 2016) Le ministère devient Ministère de l'Environnement, de l'Énergie et de la Mer (MEEM) et est chargée des relations internationales sur le climat. Source Wikipédia : http://fr.wikipedia.org/wiki/Minist%C3%A8re_de_l'Environnement,_de_l http://fr.wikipedia.org/wiki/Liste_des_ministres_fran%C3%A7ais_des_T
Modèle	ERA enregistre la description d'un pare-feu dans un fichier XML situé par défaut dans un répertoire nommé `/usr/share/era/modeles/`. Ce fichier est souvent dérivé d'un modèle livré de base, fichiers de référence présent dans le dossier `/usr/share/era/modeles` sur lequel se base l'utilisateur. Par extension, un modèle est n'importe quel fichier de description de pare-feu dans ERA.
Mode promiscuité *= Promiscuous mode*	Le mode promiscuité se réfère à une configuration de la carte réseau qui lui permet d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.
MSS *= Maximum Segment Size*	Le MSS désigne la quantité de données en octets qu'un ordinateur ou tout équipement de communication peut contenir dans un paquet seul et non fragmenté. Pour obtenir le meilleur rendement possible, la taille du segment de données et de l'en-tête doivent être inférieures au MTU. Pour plus d'information : https://fr.wikipedia.org/wiki/Maximum_Segment_Size
MTU *= Maximum Transmission Unit*	Le MTU définit la taille maximum d'un paquet (en octets) pouvant être transmis sur le réseau sans fragmentation. Source Wikipédia : http://fr.wikipedia.org/wiki/Maximum_Transmission_Unit
MySQL	MySQL est un système de gestion de base de données (SGBD). Il fait partie des logiciels de gestion de base de données les plus utilisés au monde. C'est un serveur de bases de données relationnelles SQL développé dans un souci de performances élevées en lecture, il est davantage orienté vers le service de données déjà en place plutôt que vers celui de mises à jour fréquentes et fortement sécurisées. Il est multi-thread et multi-utilisateur.
NAS *= Network Attached Storage*	Un NAS est un serveur relié à un réseau dont la principale fonction est

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	le stockage de données en un volume centralisé pour des clients réseau hétérogènes.
NAS *= Network Access Server*	Un Network Access Server (NAS), ici un switch, fonctionne comme un client RADIUS. Au sein d'un réseau, le premier équipement qui prend en charge un client (machine ou utilisateur) est un équipement d'accès (switch, point d'accès Wifi). Ces équipements jouent un rôle crucial car ce sont eux qui détectent la présence d'un équipement qui essaye de rejoindre le réseau. Ils interviennent donc dans le processus d'authentification. Dans la terminologie RADIUS, ces équipements d'accès sont appelés NAS (Network Access Server), ou clients Radius : ce sont ces équipements qui interagissent avec le serveur RADIUS en utilisant le protocole du même nom. Ils devront d'ailleurs être configurés pour cela (ils doivent connaître l'adresse IP du serveur Radius). Source : http://juboite.hd.free.fr/doku.php?id=tuto:radius:freeradius
NAT *= Network Address Translation*	Le NAT est un mécanisme informatique permettant de faire communiquer un réseau local avec l'Internet. En réseau informatique, on dit qu'un routeur fait de la traduction d'adresse réseau lorsqu'il fait correspondre les adresses IP internes non-uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4. Source Wikipédia : http://fr.wikipedia.org/wiki/Network_address_translation
NBD *= Network Block Devices*	Network Block Devices (NBD) est un composant du kernel permettant de monter un fichier distant via ethernet, en TCP, comme s'il s'agissait d'un périphérique de bloc local.
Netfilter	Netfilter est un outil de filtrage de paquets sous linux. Le logiciel qui lui est associé est iptables.
NFS *= Network File System*	NFS est est un protocole développé par Sun Microsystems qui permet à un ordinateur d'accéder à des fichiers via un réseau. Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX. Des implémentations existent pour Macintosh et Microsoft Windows. NFS est compatible avec IPv6 sur la plupart des systèmes.
Nginx *= Engine-x*	Nginx est un logiciel de serveur Web ainsi qu'un proxy inverse. Le serveur est de type asynchrone par opposition aux serveurs synchrones où chaque requête est traitée par un processus dédié. Donc au lieu d'exploiter une architecture parallèle et un multiplexage

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	temporel des tâches par le système d'exploitation, Nginx utilise les changements d'état pour gérer plusieurs connexions en même temps. Le traitement de chaque requête est découpé en de nombreuses tâches plus petites ce qui permet de réaliser un multiplexage efficace entre les connexions. Pour tirer parti des ordinateurs multiprocesseurs, le serveur permet de démarrer plusieurs processus. Ce choix d'architecture se traduit par des performances très élevées, une charge et une consommation de mémoire particulièrement faibles comparativement aux serveurs Web classiques, tels qu'Apache.
Niveau de sécurité	Nombre entier (entre 0 et 100) permettant d'ordonner les zones par ordre croissant.
Nom de domaine	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. Un domaine est un ensemble d'ordinateurs reliés à Internet et possédant une caractéristique commune. Voici des exemples de domaine : 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 ténue dans certains cas) avec la France ; le domaine paris.fr est l'ensemble des ordinateurs hébergeant des activités pour la ville de Paris. 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. Source Wikipédia : http://fr.wikipedia.org/wiki/Nom_de_domaine
NTLM *= NT Lan Manager*	NTLM est un protocole d'identification utilisé dans diverses implémentations des protocoles réseau Microsoft. Il est aussi utilisé partout dans les systèmes de Microsoft comme un mécanisme d'authentification unique SSO.
NTP *= Network Time Protocol*	NTP est un protocole permettant de synchroniser les horloges des systèmes informatiques.
NUT *= Network UPS Tools*	NUT est un ensemble d'outils permettant de monitorer un système relié à un ou des onduleurs. Il se compose de plusieurs éléments : • le démon `nut` lancé au démarrage du système ; • le démon `upsd` qui permet d'interroger l'onduleur, il est lancé

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	sur le PC relié à l'onduleur ; • le démon `upsmon` qui permet de monitorer et lancer les commandes nécessaires sur le réseau ondulé (arrêt de machines ...) ; • différents programmes pour envoyer des commandes manuellement à l'onduleur. `upsd` peut communiquer avec plusieurs onduleurs si nécessaire. `upsmon` interroge à intervalle régulier la machine du réseau sur laquelle est lancée `upsd`.
OpenNebula	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/
OpenSSL	OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, openssl. Source : https://fr.wikipedia.org/wiki/OpenSSL
OpenVZ	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, qualifiées de serveurs privés virtuels (VPS) ou environnements virtuels (VE). Source Wikipédia : https://fr.wikipedia.org/wiki/OpenVZ
OSPF *= Open Shortest Path First*	Open Shortest Path First (OSPF) est un protocole de routage interne IP de type « à état de liens ». Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages Link-state advertisements (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens Link-State Database (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, Shortest Path First (SPF) pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB. Le bon fonctionnement d'OSPF requiert donc une complète

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire. En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur. Source Wikipédia : http://fr.wikipedia.org/wiki/Open_Shortest_Path_First
OTP *= One-time password*	Un Mot de passe unique (OTP) est un mot de passe qui n'est valable que pour une session ou une transaction. Les OTP permettent de combler certaines lacunes associées aux traditionnels mots de passe statiques, comme la vulnérabilité aux attaques par rejeu. Cela signifie que, si un intrus potentiel parvient à enregistrer un OTP qui était déjà utilisé pour se connecter à un service ou pour effectuer une opération, il ne sera pas en mesure de l'utiliser car il ne sera plus valide. En revanche, les OTP ne peuvent pas être mémorisé par les êtres humains, par conséquent, ils nécessitent des technologies complémentaires afin de s'en servir. Source : http://fr.wikipedia.org/wiki/Mot_de_passe_unique
PAM *= Pluggable Authentication Modules*	PAM est un mécanisme permettant d'intégrer différents schémas d'authentification de bas niveau dans une API de haut niveau, permettant de ce fait de rendre indépendants du schéma les logiciels réclamant une authentification. PAM est une création de Sun Microsystems et est supporté en 2006 sur les architectures Solaris, Linux, FreeBSD, NetBSD, AIX et HP-UX. L'administrateur système peut alors définir une stratégie d'authentification sans devoir recompiler des programmes d'authentification. PAM permet de contrôler la manière dont les modules sont enfichés dans les programmes en modifiant un fichier de configuration. Les programmes qui donnent aux utilisateurs un accès à des privilèges doivent être capables de les authentifier. Lorsque vous vous connectez sur le système, vous indiquez votre nom et votre mot de passe. Le processus de connexion vérifie que vous êtes bien la personne que vous prétendez être. Il existe d'autres formes d'authentification que l'utilisation des mots de passe, qui peuvent d'ailleurs êtres stockés sous différentes formes.
Pare-feu *= firewall*	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. 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).

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	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. Le filtrage se fait selon divers critères. Les plus courants sont : • 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	Les modules EOLE sont livrés avec un ensemble de templates de fichiers de configuration qui seront copiés vers leur emplacement de destination à l'instance ou à chaque reconfigure. Il est possible de personnaliser ces fichiers de configuration à l'aide d'un patch. La procédure pour réaliser des patchs est expliquée dans la rubrique **Personnalisation du serveur à l'aide de Creole** dans les documentations complètes ou dans la documentation partielle dédiée nommée **PersonnalisationEOLEAvecCreole**.
PDC *= Primary Domain Controller*	Un contrôleur principal de domaine appartient à une technologie d'annuaire et de réseau pour Windows NT. C'est un serveur qui dans un domaine (un groupe d'ordinateur appelé aussi «forêt») Windows gère et contrôle l'accès à une variété de ressources. Le contrôleur principal de domaine a un compte d'administration générale qui a le contrôle total des ressources du domaine. Un domaine a au moins un contrôleur de domaine principal et a souvent un ou plusieurs contrôleurs de domaine de sauvegarde (BDC). Si un contrôleur de domaine principal tombe en panne, l'un des contrôleurs secondaires peuvent ensuite être promu pour prendre sa place.
PID *= Process IDentifier*	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). Wikipédia : https://fr.wikipedia.org/wiki/Identifiant_de_processus
Podman	Podman est un logiciel libre permettant de lancer des applications dans des conteneurs logiciels. Il s'agit d'une alternative à Docker, qui permet de lancer les commandes sans les permissions root.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	https://fr.wikipedia.org/wiki/Podman
Politique de filtrage	Une politique de filtrage permet de définir une suite d'autorisation et d'interdiction dans les accès web.
POP *= Post Office Protocol*	POP est un protocole qui permet de récupérer les courriers électroniques présents sur un serveur de messagerie. Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. C'est cette dernière qui a cours actuellement.
PostgreSQL	PostgreSQL est un système de gestion de base de données relationnelle et objet (SGBDRO). Il est fondé sur une communauté mondiale de développeurs et d'entreprises.
PPPoE *= Point-to-Point Protocol over Ethernet*	PPPoE est un protocole d'encapsulation de PPP sur Ethernet. Il permet de bénéficier des avantages de PPP et du contrôle de la connexion (débit, etc.), sur un réseau 802.3. Il est beaucoup employé par les connexions haut débit à Internet par ADSL et câble destinées aux particuliers, bien qu'une connexion utilisant un pont Ethernet-Ethernet soit souvent plus stable et plus performante. Il pose également des problèmes de MTU.
Préfixe binaire	Les préfixes binaires (kibi-, mébi-, gibi-, tébi-, pébi- et exbi-) sont souvent utilisés lorsqu'on a affaire à de grandes quantités d'octets. Ils sont dérivés, tout en étant différents, des préfixes du système international (kilo-, méga-, giga- et ainsi de suite). La raison d'être de ces préfixes binaires est d'éviter la confusion de valeur avec les préfixes du système international. http://fr.wikipedia.org/wiki/Préfixe_binaire
Projet LTSP *= Linux Terminal Server Project*	Linux Terminal Server Project (LTSP) est un ensemble de programmes permettant à plusieurs personnes d'utiliser le même ordinateur. Cela est réalisé par la mise en place d'un réseau informatique composé d'un serveur sous GNU/Linux et de clients légers. http://www.ltsp.org/
Pronote	Pronote est un logiciel privateur de gestion de vie scolaire créé en 1999. C'est au départ un client lourd, mais il existe, depuis 2003, une extension permettant d'utiliser une version Web.
Proxy sibling *= proxy frère*	Hiérarchiquement, un cache interrogé peut être un de niveau supérieur (parent) ou de niveau égal (frère ou sibling). Les serveurs parents sont d'ordinaire plus proches du serveur hébergeant l'objet recherché que les serveurs fils. Si un serveur fils ne peut trouver l'objet, la requête est en général relayée vers un serveur de cache parent qui va rapporter, mémoriser (mettre en cache) et finalement transmettre la requête au demandeur.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	Les serveurs frères (siblings) sont des serveurs de cache d'un niveau hiérarchique égal, dont le but est de répartir la charge. http://fr.wikipedia.org/wiki/Internet_Cache_Protocol
PUA *= Potentially Unwanted Applications*	Applications potentiellement indésirables.
PXE *= Pre-boot eXecution Environment*	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 : • 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 *= QOS*	Régulation des flux du trafic sur un réseau, définition de Wikpedia [http://fr.wikipedia.org/wiki/QoS]
RADIUS *= Remote Authentication Dial-In User Service*	RADIUS est un protocole client-serveur permettant de centraliser des données d'authentification. Source : http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Servic
Ramsese *= Répertoire académique et ministériel sur les établissements du système éducatif*	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 : • Nomenclature utilisée : code RNE • Niveau géographique : commune • Type de source : fichier de gestion
RELP *= Reliable Event Logging Protocol*	Reliable Event Logging Protocol ou RELP est un protocole définissant un service de journaux d'événements d'un système informatique. Il est supporté entre autres par Rsyslog.
Réseau virtuel Privé *= RVP ou VPN (Virtual Private Network) en anglais*	Le réseau virtuel privé permet de relier au travers d'Internet des sous réseaux entre eux, de façon sécurisée et chiffrée.
RIP *= Routing Information Protocol*	RIP, protocole d'information de routage, est un protocole de routage IP de type Vector Distance (à vecteur de distances) s'appuyant sur l'algorithme de détermination des routes décentralisé. Il permet à

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	chaque routeur de communiquer aux routeurs voisins la métrique, 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. Source Wikipédia : http://fr.wikipedia.org/wiki/Routing_Information_Protocol
Round-robin *= tourniquet*	Round-robin (RR) est un algorithme d'ordonnancement courant dans les systèmes d'exploitation. Ce dernier attribue des tranches de temps à chaque processus en proportion égale, sans accorder de priorité aux processus. Source Wikipédia : http://fr.wikipedia.org/wiki/Round-robin_(informatique)
Rsyslog	Rsyslog est un logiciel libre utilisé sur des systèmes d'exploitation de type Unix transférant les messages des journaux d'événements sur un réseau IP. Rsyslog implémente le protocole basique syslog qui centralise les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau. Il présente la particularité d'en étendre les fonctionnalités en permettant, notamment, de filtrer sur des champs, de filtrer à l'aide d'expressions régulières et l'utilisation du protocole TCP de la couche transport. Source : https://fr.wikipedia.org/wiki/Rsyslog
safe search *= recherche sécurisée*	Safe search est un terme utilisé pour évoquer un filtrage sur les contenus potentiellement offensant sur des plateformes de contenu ou des moteurs de recherche. Ce terme vient de la fonctionnalité SafeSearch implémentée sur le moteur de recherche Google.
SaltStack *= Salt*	Salt ou SaltStack est un logiciel de gestion de configuration écrit en Python, fonctionnant sur le principe client-serveur. SaltStack a pour but de rendre la gestion de configuration simple mais flexible. Il s'agit d'une alternative à Puppet, Ansible et Chef. On utilise les langages informatiques YAML, Jinja2 et Python pour configurer SaltStack. Source Wikipédia : https://fr.wikipedia.org/wiki/Salt_(logiciel) Le vocabulaire SaltStack : • Pillar : Dictionnaire des variables ; • States : Ordres à exécuter ; • Formula : Ensemble de States ; • Grains : Informations que retournent les minions au master-salt. La machine cliente SaltStack est appelé « minion », le serveur est

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	appelé « master ».
Samba *= SaMBa : Server Message Block*	Samba est une re-implémentation libre des protocoles SMB/CIFS sous GNU/Linux et d'autres variantes d'Unix. Son nom provient du protocole SMB, protocole standard de Microsoft. À partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Windows Server, soit en tant que contrôleur de domaine principal (PDC) ou en tant que membre d'un domaine. Il peut également faire partie d'un domaine Active Directory.
SAML *= Security assertion markup language*	SAML est un standard informatique définissant un protocole pour échanger des informations liées à la sécurité. Il est basé sur le langage XML. SAML suppose un fournisseur d'identité et répond à la problématique de l'authentification au-delà d'un intranet.
SAN *= Storage Area Network*	Un SAN, un réseau de stockage est un réseau spécialisé permettant de mutualiser des ressources de stockage. Un réseau de stockage se différencie des autres systèmes de stockage tels que le NAS (Network attached storage) par un accès bas niveau aux disques. Pour simplifier, le trafic sur un SAN est très similaire aux principes utilisés pour l'utilisation des disques internes (ATA, SCSI). C'est une mutualisation des ressources de stockage. Source Wikipédia : https://fr.wikipedia.org/wiki/R%C3%A9seau_de_stockage_SAN
SecurID	SecurID est un système de token, ou authentifieur, produit par la société RSA Security et destiné à proposer une authentification forte à son utilisateur dans le cadre de l'accès à un système d'information. Source : http://fr.wikipedia.org/wiki/SecurID
Service	Couple protocole et/ou port (ou plage de ports).
SHA-2 *= Secure Hash Algorithm*	SHA-2 est une famille de fonctions de hachage qui ont été conçues par la National Security Agency des États-Unis (NSA), sur le modèle des fonctions SHA-1 et SHA-0, elles-mêmes fortement inspirées de la fonction MD4 de Ron Rivest (qui a donné parallèlement MD5). Source : https://fr.wikipedia.org/wiki/SHA-2
SID *= Security Identifier*	Le SID est un identifiant de sécurité utilisé pour identifier les ressources et les personnes sur un réseau Microsoft. Le SID d'un domaine se présente sous la forme `S-1-5-21-nnnnnnnnnn-nnnnnnnnnn-nnnnnnnnnn`. Chaque serveur de fichiers possède son propre SID et celui-ci est utilisé lors de la création des comptes (utilisateurs, groupes, machines rattachées au domaine). Lors de l'installation de module Scribe, Samba génère aléatoirement

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	son propre SID. http://fr.wikipedia.org/wiki/Security_Identifier
SMTP *= Simple Mail Transfer Protocol*	SMTP est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
SNMP *= Simple Network Management Protocol*	SNMP est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance. https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol
Socle Interministériel de Logiciel Libre *= SILL*	Le secrétariat général pour la modernisation de l'action publique (SGMAP) relève du Premier ministre. 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. L'instance DISIC en charge des logiciels libres préconise une sélection de logiciels, sous la forme d'un socle interministériel de logiciels libres (SILL). 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. http://references.modernisation.gouv.fr/socle-logiciels-libres
Squid	Squid est un proxy (serveur mandataire en français) cache sous GNU/Linux. De ce fait il permet de partager un accès Internet entre plusieurs utilisateurs n'ayant qu'une seule connexion. Un serveur proxy propose également un mécanisme de cache des requêtes, qui permet d'accéder aux données en utilisant les ressources locales au lieu des ressources web, réduisant les temps d'accès et la bande passante consommée. Il est également possible aussi d'effectuer des contrôles de sites.
SSH *= Secure Shell*	Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
SSO *= Single Sign On, Authentification unique*	SSO est une méthode permettant de centraliser l'authentification afin de permettre à l'utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques. Les objectifs sont : • simplifier pour l'utilisateur la gestion de ses mots de passe : plus

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent ; • simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ; • simplifier la définition et la mise en œuvre de politiques de sécurité.
StartTLS	Dans certains cas, un même port est utilisé avec et sans SSL. Dans ce cas, la connexion est initiée en mode non chiffré. Le tunnel est ensuite mis en place au moyen du mécanisme StartTLS. C'est le cas, par exemple des protocoles de mails IMAP et SMTP ou LDAP.
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/
subiquity	Nouveau programme pour l'installation des serveurs Ubuntu (ubiquity pour serveur). https://github.com/canonical/subiquity
Sunstone	Sunstone est une interface graphique permettant de gérer OpenNebula. C'est une application Web qui permet de gérer et d'administrer les machines virtuelles et tout ce qui s'y rapporte. Depuis la version 2.7.2, l'accès à l'interface Sunstone s'effectue en https via un navigateur web : `https://<adresseServeur>`
Swap *= Verbe échanger*	En informatique le swap sert à étendre la mémoire utilisable par un système d'exploitation, par un fichier d'échange ou une partition dédiée ; c'est aussi une instruction de certains processeurs et une fonction de certains langages de programmation qui permet l'échange de deux variables.
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 *= Transmission Control Protocol*	TCP est le principal protocole réseau utilisé par les connexions Internet. C'est un protocole de transport qui travaille en mode connecté. Les données transmises sont donc vérifiées. Dans le modèle TCP/IP, il est entre la couche de transport (généralement IP) et la couche application.
TCP Wrapper	TCP Wrapper est une technique, propre à Unix, permettant de

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

= tcpd	contrôler les accès à un service (ou démon) suivant la source. Il se configure grâce au deux fichiers /etc/hosts.allow et /etc/hosts.deny. Tous les démons ne supportent pas la technique TCP Wrapper.
Telnet *= TErminal NETwork ou TELecommunication NETwork*	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 *= Modèle Creole*	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 *= Outil de gestion de configuration*	À cause de l'afflux de plus en plus grand des options de configuration des serveurs EOLE (plus de 1600 au dernier recensement), il était devenu de plus en plus difficile de correctement récupérer les options et de les utiliser là où elles devaient effectivement être employées. Pour remédier à ces difficultés, l'outil Tiramisu a été développé, il est utilisé comme moteur du générateur de configuration de la version EOLE 2.4. La documentation technique du projet : http://tiramisu.labs.libre-entreprise.org Les sources du projet Tiramisu : http://labs.libre-entreprise.org/projects/tiramisu/
TLS *= Transport Layer Security*	Le TLS et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le TLS est la poursuite des développements de SSL. Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
Type MIME	Un type MIME est une information permettant de connaitre le format d'un document sans se baser sur l'extension.
UEFI *= Unified Extensible Firmware Interface*	Le standard UEFI définit un logiciel intermédiaire entre le micrologiciel (firmware) et le système d'exploitation (OS) d'un ordinateur. Cette interface succède sur certaines cartes-mères au BIOS. Elle fait suite à EFI (Extensible Firmware Interface), conçue par Intel pour les processeurs Itanium. Source Wikipédia : https://fr.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

Unicode	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. Source Wikipédia : http://fr.wikipedia.org/wiki/Unicode
Unité organisationnelle *= OU*	Une Unité organisationnelle (Organizational Unit ; OU ; UO) est un objet conteneur, de la norme ldap, qui est utilisé pour hiérarchiser les annuaires.
URI *= Uniform Resource Identifier*	L'URI est une courte chaîne de caractères identifiant une ressource sur un réseau.
UTC *= Temps Universel Coordonné*	UTC, est une échelle de temps adoptée comme base du temps civil international par la majorité des pays du globe. Source Wikipédia : https://fr.wikipedia.org/wiki/Temps_universel_coordonné [https://fr.wikipedia.org/wiki/Temps_universel_coordonn%C3%A9]
UUID *= Universally Unique IDentifier*	Le but des UUID est de permettre à des systèmes distribués d'identifier de façon unique une information sans coordination centrale importante. Dans ce contexte, le mot « unique » doit être pris au sens de « unicité très probable » plutôt que « garantie d'unicité ». Source : http://fr.wikipedia.org/wiki/Universal_Unique_Identifier
Version admissible ou pre-release	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. Source Wikipédia : http://fr.wikipedia.org/wiki/Version_d%27un_logiciel#Version_admissibl
VLAN *= Réseau local virtuel*	Un VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.
VNC *= Virtual Network Computing*	VNC est un système de visualisation et de contrôle de l'environnement de bureau d'un ordinateur distant. Il permet au logiciel client VNC de transmettre les information de saisie du clavier et de la souris à l'ordinateur distant, possédant un logiciel serveur VNC à travers un réseau informatique. Il utilise le protocole RFB pour les communications.
WPAD *= Web Proxy Autodiscovery Protocol*	WPAD définit la façon selon laquelle un navigateur web se connecte à Internet. Ce protocole permet au navigateur d'utiliser automatiquement le proxy approprié à l'URL demandée. WPAD laisse le navigateur

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	découvrir l'emplacement du fichier PAC grâce aux services DHCP et DNS. Un fichier PAC est un fichier texte en JavaScript, qui contient entre autres la fonction FindProxyForURL(url, host). Cette fonction possède deux arguments associés : • URL : l'URL de l'objet • HOST : le nom de domaine dérivé de l'URL
Xen	Xen est un logiciel libre de virtualisation, plus précisément un hyperviseur de machine virtuelle.
XML *= Extensible Markup Language*	L'Extensible Markup Language (« langage de balisage extensible » en français) est un langage informatique de balisage générique qui dérive du SGML. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire, comme XHTML, XSLT, RSS, SVG... Elle est reconnaissable par son usage des chevrons (< >) encadrant les balises. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche...) entre systèmes d'informations hétérogènes (interopérabilité). Avec ses outils et langages associés une application XML respecte généralement certains principes : • la structure d'un document XML est définie et validable par un schéma, • un document XML est entièrement transformable dans un autre document XML. Source : http://fr.wikipedia.org/wiki/Xml
XML-RPC *= XML Remote procedure call*	XML-RPC est un protocole RPC (Remote procedure call), une spécification simple et un ensemble de codes qui permettent à des processus s'exécutant dans des environnements différents de faire des appels de méthodes à travers un réseau. XML-RPC permet d'appeler une fonction sur un serveur distant à partir de n'importe quel système (Windows, Mac OS X, GNU/Linux) et avec n'importe quel langage de programmation. Le serveur est lui même sur n'importe quel système et est programmé dans n'importe quel langage. Cela permet de fournir un Service web utilisable par tout le monde sans restriction de système ou de langage. Source : http://fr.wikipedia.org/wiki/XML-RPC
ZéphirLog	ZéphirLog était un module 2.2 qui permettait de stocker et d'archiver les journaux d'événements remontés par les différents serveurs EOLE.
Zone	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

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)

	zone la plus sécurisée (niveau 100). Chaque zone est définie par un nom, une adresse réseau, et un niveau de sécurité.

Documentation sous licence Creative Commons by-sa - EOLE (https://pcll.ac-dijon.fr/pcll/)