

EOLE 2.6

Panorama et nouveautés

Joël CUISSINAT
Daniel DEHENNIN

Pôle Logiciels Libres - EOLE

J-EOLE 2017

CC BY-SA 4.0



EOLE 2.6 : panorama

EOLE 2.6.0

- Présentation lors des J-EOLE 2016
- 4 versions β
- 3 versions RC
- 777 tests de qualification
- ISO stable le 2 décembre 2016

Architecture AMD64 uniquement

Panorama des modules EOLE 2.6.0

Dans l'ordre de démarrage de l'image ISO :

- | | |
|---------------------|------------------------|
| ① Eolebase | ⑥ ESBL |
| ② Horus | ⑦ Sphynx |
| ③ Scribe | ⑧ Zéhpír |
| ④ Seth Samba 4 AD | ⑨ Hâpy depuis 2.4 |
| ⑤ Eclair depuis 2.3 | ⑩ Hâpy Node depuis 2.4 |

Amon, AmonEcole, Thot et Seshat absents de la livraison

ECDL en expérimental

EOLE 2.6.1

- 4 versions β
- 4 versions RC
- 1366 tests de qualification
- ISO stable le [23 Mai 2017](#)

Panorama des modules EOLE 2.6.1

Dans l'ordre de démarrage de l'image ISO :

① Eolebase

② Amon

③ Horus

④ Scribe

⑤ Seth

⑥ Eclair

⑦ AmonEcole

⑧ ESBL

⑨ ECDDL

⑩ Sphynx

⑪ Seshat

⑫ Thot

⑬ Zéphir

⑭ Hâpy

⑮ Hâpy Node

Modifications communes

- Partitionnement personnalisé
- Agrégation de liens (*bonding*)
- Gestion des certificats [Let's Encrypt](#)
- Dépôts APT tiers
- reconfigure et bastion regen régénèrent les règles de pare-feu
- EAD3

Évolutions autour du proxy

- Exceptions de proxy pour adresses IP et réseaux sources
- L'authentification NTLM/SMB
 - Nécessite une intégration
 - Ne supporte pas le multi-domaine
- Mise à jour des règles « safe search »
- Gestion du « filtre web 3 » dans l'EAD
- Redirection de domaines pour le proxy inverse
- Intégration des contributions pour le proxy 1 carte

Tunnels IPSec

- Service RVP intégré à *StrongSwan*
- Gestion de la fragmentation IKEV2
- Gestion des configurations « Roadwarrior »

Applications Web (eole-web)

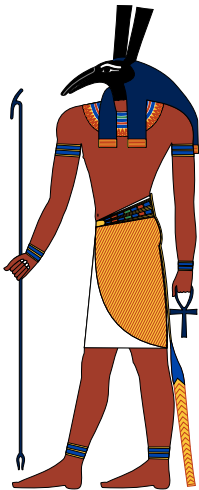
`web_url` n'accepte plus les adresses IP

Constellation Hâpy

- [OpenNebula 5.2.1](#)
- [Article de blog](#) sur la virtualisation de modules EOLE avec Hâpy

Seth

maître du tonnerre et de la foudre



© 2007 Jeff Dahl (source Wikipedia)

Seth

du nouveau depuis 2.6.0

- Samba 4.5 installé par mise à jour
- Gestion des sauvegardes
- Partages additionnels et corbeille
- Restriction d'accès par service (Samba-AD, LDAP, ...)

Eclair

plus de souplesse pour les clients

Paramétrage d'une ou deux images pour les clients :

- Client léger (*THIN*) ou semi lourd (*FAT*)
- Architecture I386 ou AMD64
- Choix du bureau des clients légers
 - [Mate \(en\)](#) par défaut
 - [Xfce4](#)

Nouveautés 2.6.1

Agrégation de liens ethernets

à deux c'est un minimum

- Accroître le débit
- Redondance entre cartes

Un même et unique commutateur sauf si extension propriétaire

Agrégation de liens ethernet

Configuration de l'interface

B Adresse IP de la carte	*	192.168.2.12	
B Masque de sous réseau de la carte	*	255.255.255.0	
E Nom de l'interface réseau	ens7 x ens8 x	ens4	
E Nom de l'interface réseau de la zone	*	ens4 ens7 ens8 ens9	
E Mode de bonding			
E Fréquence des MII link monitoring en millisecondes	*	100	
E Temps en millisecondes pour qu'une interface soit détectée down	*	200	
E Temps en millisecondes pour qu'une interface soit détectée comme active	*	200	
E Mode de connexion pour l'interface interne 1			

Agrégation de liens ethernet

Configuration de l'interface

B Adresse IP de la carte	* 192.168.2.12	
B Masque de sous réseau de la carte	* 255.255.255.0	
E Nom de l'interface réseau	* ens7 ens8 ens9	
E Nom de l'interface réseau de la zone	* bond1	
E Mode de bonding	balance-rr	
E Fréquence des MII link monitoring en millisecondes	* <input type="text"/>	
E Temps en millisecondes pour qu'une interface soit détectée down	* <input type="text"/>	
E Temps en millisecondes pour qu'une interface soit détectée comme	* <input type="text"/>	
E Mode de connexion pour l'interface interne 1	<input type="text"/>	

Partitionnement personnalisé

assouplir la gestion des volumes LVM

3 besoins fondamentaux :

- Créer de nouveaux volumes LVM
- Étendre un volume LVM existant sur tout l'espace libre
- Répartir l'espace libre entre plusieurs volumes

Utilisable par défaut sur Eolebase et ECDL

Nécessite un partitionnement manuel sur les autres modules

Partitionnement personnalisé

onglet *Système* : désactivé par défaut

Ajustement du partitionnement

E Ajuster le partitionnement

*

non



E Allouer l'espace restant

*

non



Partitionnement personnalisé

tout pour un

Ajustement du partitionnement

E Ajuster le partitionnement

* non



E Allouer l'espace restant

* oui



E Volume logique à étendre

* root



Partitionnement personnalisé

un peu pour plusieurs

Ajustement du partitionnement

E Ajuster le partitionnement

* oui

E Nom du volume à créer



E Nom du volume à créer

* root



E Taille du volume en pourcentage de l'espace disponible

* 30



E Format du système de fichiers



E Point de montage du volume logique



E Options du montage



☰ Montrer/Cacher

+ 🖱️ Nom du volume à créer

Certificats Let's Encrypt

pour celles et ceux sans IGC fixe

Slogan : *Encrypt the entire web*

- Distribution et renouvellement automatisé
- Gratuit

Prévu pour fonctionner avec des serveurs accessibles depuis Internet

Peut fonctionner à travers un proxy inverse

Certificats Let's Encrypt

onglet *Général*

B Types de certificats à utiliser

↻ × *

letsencrypt ✓

- autosigné
- letsencrypt
- manuel

Mise à jour

Certificats Let's Encrypt

onglet *Certificats SSL* : configuration du client

Paramètres du client Let's Encrypt

E Répertoire de configuration du client Let's Encrypt	*	<input type="text" value="/etc/ssl/letsencrypt/conf"/>	
E Répertoire de travail du client Let's Encrypt	*	<input type="text" value="/tmp/letsencrypt/work"/>	
E Répertoire de journalisation du client Let's Encrypt	*	<input type="text" value="/var/log/letsencrypt/"/>	
E Adresse du serveur Let's Encrypt		<input type="text"/>	
E Port d'écoute du serveur Let's Encrypt	*	<input type="text"/>	
E Mode de fonctionnement du client Let's Encrypt		<input type="text" value="webroot"/>	
E Port d'écoute pour la requête http-01	*	<input type="text" value="webroot"/> <input type="text" value="standalone"/>	
E Port d'écoute pour la requêt TLS-SNI	*	<input type="text" value="443"/>	

Certificats Let's Encrypt

onglet *Certificats SSL* : certificats supplémentaires

Certificats supplémentaires à demander

 **Nom de domaines supplémentaires**

Pas de valeur



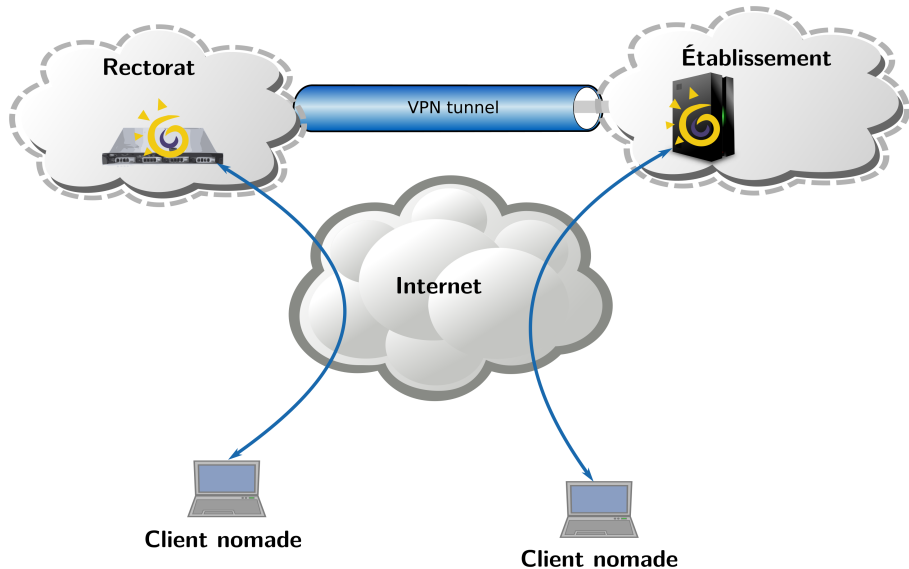
scribe.lycee-de-test.ac-dijon.fr



Ne pas oublier les enregistrements DNS publics

Clients IPsec nomades

les guerriers de la route sont là



Clients IPSec nomades

tout est dans ARV

Tunnels | **Serveurs RVP** | Modèles | Certificats

UAI	Nom	Type de serveur	État
0000000A	sphinx	sphinx	
0000000A	Roadwarrior-académique	roadwarrior	Pb de tunnels ou non configuré

Ajouter un nouveau serveur RVP

UAI :

Nom :

Sélectionner un modèle de serveur RVP: ▼

- Roadwarrior
- Sphinx
- Etablissement
- Roadwarrior

« Précédent Suivant »

➕ Ajouter | ➦ Modifier | 🗑️ Supprimer | 📜 Certificat | 🌐 IP externe | 📧 Renvoyer sur Zéphi | 📄 Zéphi infos serveur


Prêt Appliquer

Clients IPsec nomades

pas de lieu fixe, pas d'IP

Tunnels	Serveurs RVP	Modèles	Certificats				
UAI	Nom	Identifiant Zéphir	Version Eole	Type de serveur	État		
0000000A	aca.sphinx-default-2.6.1	246	2.6.1	sphinx			
00000001	etb1.amon-default-2.6.1	318	2.6.1	etablissement	Pb de tunnels ou non configuré		
0000000A	Roadwarrior-académique			roadwarrior	Pb de tunnels ou non configuré		
00000001	Roadwarrior-étab			roadwarrior	Pb de tunnels ou non configuré		

Information

 Un roadwarrior n'a pas besoin d'adresse IP externe

Ajouter | Modifier | Supprimer | Certificat | IP externe | Renvoyer sur Zéphir | Zéphir infos serveur

Prêt

Appliquer

Clients IPsec nomades

rien de neuf sous le modèle

Tunnels | Serveurs RVP | **Modèles** | Certificats

Modèle de lien sécurisé		
Nom	Envoi certifi...	Fragmentation IKE
amon-sphinx	always	no
rw-aca	always	no
rw-etab	always	no

Autorité de Certification		
CA-sphinx-RVP		
Modèle de serveur RVP 1		Modèle de serveur RVP 2
Sphinx		Roadwarrior
Modèle de tunnel		
Nom	Modèle de réseau local 1	Modèle de réseau local 2
ader-rw	reseau_ader	RW_SourceIP
agriates	reseau_eth1	RW_SourceIP

Modèle de réseau		
Nom	Type	Modèle de serveur RVP
RW_SourceIP	ip	Roadwarrior
reseau_eth1	network	Sphinx
reseau_10	network	Sphinx
reseau_192	network	Sphinx
reseau_172	network	Sphinx
reseau_ader	network	Sphinx
admin	network	Etablissement
pedago	network	Etablissement
dmz	network	Etablissement

Prêt Appliquer

Clients IPSec nomades

le DNS est obligatoire

The screenshot shows a VPN configuration interface with three main sections: 'Serveur RVP 1', 'Serveur RVP 2', and 'Tunnel'. A modal dialog titled 'Ajouter un lien sécurisé vers' is open, displaying configuration for two servers. The 'DNS du VPN' field for the second server is empty, which has triggered a red warning icon. The dialog includes fields for 'Certificat', 'IP', 'Envoi certificat', and 'Fragmentation IKE', each with a corresponding 'Ajouter' button. Navigation buttons '« Précédent Suivant »', 'Annuler', and 'Créer' are also present.

Serveur RVP 1		Serveur RVP 2		Tunnel	
UAI	Nom	UAI	Nom	Nom	IP / Réseau
0000000A	aca.sphyxix-default-2...				
00000001	etb1.amon-default-2.6.1				
0000000A	Roadwarrior-académi...				
00000001	Roadwarrior-étab				

Ajouter un lien sécurisé vers

etb1.amon-default-2.6.1

Certificat: etb1.amon-2.6.1.ac-test.fr


IP: 192.168.0.31

Roadwarrior-étab

Certificat: nw-etb1.ac-test.fr

Envoi certificat: TOUJOURS via le protocole ipsec

Fragmentation IKE: non

DNS du VPN: 

« Précédent Suivant »

Clients IPsec nomades

on ne voit pas l'IP du client

Tunnels Serveurs RVP Modèles Certificats

Serveur RVP 1		Serveur RVP 2		Tunnel		
UAI	Nom	UAI	Nom	Nom	IP / Réseau	IP / Réseau
0000000A	aca.sphinx-default-2...	00000001	Roadwarrior-étab	rw-etab - 192.168.0.31 - any	certificate send : ALWAYS via ipsec protocol / IKE fragmentation : no	
00000001	etb1.amon-default-2.6.1			pedago-rw	pedago : 10.1.2.0 / 255.255.255.0	RW_SourceIP
0000000A	Roadwarrior-académi...			dmz-rw	dmz : 10.1.3.0 / 255.255.255.0	RW_SourceIP
00000001	Roadwarrior-étab					

Ajouter Modifier

Prêt Appliquer

Questions ?

Remerciements

Je remercie la communauté du logiciel libre pour tous ces merveilleux logiciels sans lesquels si peu de choses existeraient.

Cette présentation a été réalisée grâce aux logiciels libres suivants :

- Le système de composition \LaTeX [TeX Live](#)
- L'éditeur de texte [GNU/Emacs](#)
- L'environnement graphique [Awesome](#)
- Le système d'exploitation [Debian GNU/Linux](#)



Licence

Cette présentation est mise à disposition sous licence
Creative Commons BY-SA 4.0

- Attribution
- Partage dans les mêmes conditions

Vous pouvez obtenir une copie de la licence

par Internet

<http://creativecommons.org/licenses/by-sa/4.0>

par courrier postal

*Creative Commons
444 Castro Street, Suite 900 Mountain View,
California, 94041, USA.*