

EOLE AD DC - T che #37578

Sc nario # 37568 (Nouveau): Maquette Sphinx 2.11 d montrant l'impl mentation du nouveau mod le strongSwan

prise en charge charon

10/08/2026 12:07 - Ludwig Seys

Statut:	R�solu	D�but:	01/10/2022
Priorit�:	Normal	Ech�ance:	
Assign� �:	Ludwig Seys	% r�alis�:	0%
Version cible:	Carnet Cadoles - MEN	Temps estim�:	0.00 heure
Description			

R visions associ es

R vision b2037994 - 10/08/2026 12:08 - Ludwig Seys

changement d pendance, ajout de charon

ref #37578

R vision 1b00527d - 10/08/2026 12:22 - Ludwig Seys

modification setpu.py pour build

ref #37578

R vision bf32a7b6 - 10/08/2026 12:31 - Ludwig Seys

add setuptools in debian

ref : #37578

Historique

#1 - 10/08/2026 12:07 - Ludwig Seys

- Statut chang  de Nouveau   En cours

#2 - 10/08/2026 13:57 - Ludwig Seys

Apr s modification des d pendances du paquet arv, l'installation de arv 2.11.0-3 entra ne bien l'installation du nouveau mod le strongSwan :

charon-systemd
strongswan-swanctl

Les anciens paquets sont supprim s :

strongswan-charon
strongswan-starter

Les paquets Sphinx restent install s :

eole-sphinx
eole-sphinx-all
eole-sphinx-module
eole-vpn
arv

  noter : le service systemd fourni par le paquet n'est pas expos  sous le nom charon-systemd.service, mais via strongswan.service, avec un alias strongswan-swanctl.service. La suite du portage devra donc tenir compte de ce nom de service pour les scripts EOLE, la haute disponibilit  et les contr les de diagnostic.

Note : la construction de paquet à du être modifié pour fonctionner, modification de rules et control en conséquence.

Côté code, la traduction propre deviendrais :

```
service strongswan-starter start/restart/stop
-> systemctl start/restart/stop strongswan
```

```
ipsec rereadall + ipsec update
-> systemctl reload strongswan
ou swanctl --load-all --noprompt
```

```
ipsec statusall
-> swanctl --list-sas
+ swanctl --list-conns
```

Selon la conf systemd:

```
ExecStart=/usr/sbin/charon-systemd
ExecStartPost=/usr/sbin/swanctl --load-all --noprompt
ExecReload=/usr/sbin/swanctl --reload
ExecReload=/usr/sbin/swanctl --load-all --noprompt
```

Ce qui est validé pour strongswan:

- strongswan.service est actif
 - le process lancé est /usr/sbin/charon-systemd
 - strongswan-swanctl.service est un alias
 - swanctl --load-all est exécuté au démarrage
 - swanctl --reload / --load-all est prévu au reload
 - le plugin vici est chargé
 - le plugin updown est chargé

validé à ce stade :

- corosync.service est actif ;
 - pacemaker.service est actif ;
 - corosync-quorumtool -s retourne un état quorum valide ;
 - le nœud local est Quorate: Yes ;
 - corosync-cfgtool -s retourne un lien local fonctionnel en transport knot ;
 - aucune erreur bloquante knot, crypto ou authkey n'est observée côté corosync.

Pas de soucis à prévoir à première vue pour corosync.

validé à ce stade :

- frr.service est actuellement masqué et inactif ;
 - vtysh ne peut donc pas se connecter aux daemons FRR ;
 - les logs montrent toutefois que FRR a bien démarré précédemment ;
 - watchfrr, mgmtd, zebra et staticd sont passés en état fonctionnel ;
 - le service a ensuite été arrêté proprement ;
 - aucune erreur bloquante de syntaxe de configuration FRR n'est observée au démarrage.

Conclusion provisoire : aucun blocage lié à frr 10.5.1 n'est identifié à ce stade. La validation runtime réelle devra être refaite avec frr.service non masqué, après génération complète de la configuration Sphynx et activation éventuelle du routage dynamique.

#3 - 10/08/2026 15:50 - Ludwig Seys

Validation instance Sphynx 2.11 après corrections Creole et ARV

Après mise à jour des paquets Creole en 2.11.0-7, et arv en 2.11.0-4, l'instance Sphynx 2.11 va jusqu'au bout.

Les étapes précédemment bloquantes passent désormais :

```
run-parts: executing /usr/share/eole/posttemplate/00-arv instance
Ajout du serveur sphynx...
* Certificat /var/lib/arv/CA/certs/sphynx.pem généré
```

Le script 00-rvp passe également sans erreur : run-parts: executing /usr/share/eole/posttemplate/00-rvp instance

La reconfiguration se termine correctement :

Reconfiguration OK

Corrections validées en situation réelle :

- correction du parsing du subject certificat dans creole.cert.get_subject()
- adaptation de arv.db.strongswandb à SQLAlchemy 2

La suite du travail peut reprendre sur le portage strongSwan/swanctl proprement dit :

1. vérification des fichiers générés,
2. des commandes appelées par ARV et du chargement effectif des configurations VPN avec strongswan.service / swanctl.

#4 - 11/08/2026 14:50 - Ludwig Seys

- Statut changé de *En cours* à *À valider*

#5 - 21/09/2026 15:29 - Ludwig Seys

- Statut changé de *À valider* à *Résolu*