

EOLE AD DC - T che #37586

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

test  tat en cours

11/08/2026 14:37 - Ludwig Seys

Statut:	R�solu	D�but:	01/10/2022
Priorit�:	Normal	Ech�ance:	
Assign� �:	Ludwig Seys	% r�alis�:	100%
Version cible:	Carnet Cadoles - MEN	Temps estim�:	0.00 heure
Description			

Historique

#1 - 11/08/2026 14:47 - Ludwig Seys

Test de validation Sphinx 2.11 / strongSwan 6 / swanctl

D marrer une VM `aca-sphinx-2.11-auto` d j  instanci e ou lancer l'instance normalement.

Remarque : si `arv` reste en `2.10`, forcer l'installation de la version `2.11.0-6`. Le paquet `arv` 2.10 d pend encore de `strongswan-starter`, alors que le paquet `arv` 2.11 d pend de `strongswan-swanctl` et `charon-systemd`.

Installer explicitement la version DEV d'ARV :

```
apt install arv=2.11.0-6
```

1. V rifier les paquets

```
dpkg -l | grep -E 'arv|python-arv|eole-vpn|strongswan|charon-systemd|swanctl'
```

Attendu :

```
ii  arv                2.11.0-6
ii  python-arv         2.11.0-6
ii  eole-vpn           2.11.0-2
ii  strongswan-swanctl 6.0.4...
ii  charon-systemd     6.0.4...
```

`strongswan-starter` et `strongswan-charon` peuvent rester en `rc`, mais ne doivent plus  tre en `ii`.

V rifier aussi que les fichiers ajout s sont pr sents :

```
dpkg -L arv python-arv eole-vpn | grep -E 'eole-ipsec-to-swanctl|ipsec2swanctl|sw_config_apply.py|util.py|active_rvp|152-rvp'
```

Attendu :

```
/usr/share/eole/sbin/eole-ipsec-to-swanctl
/usr/lib/python3/dist-packages/arv/lib/ipsec2swanctl.py
/usr/lib/python3/dist-packages/arv/lib/sw_config_apply.py
/usr/lib/python3/dist-packages/arv/lib/util.py
/usr/share/eole/diagnose/152-rvp
/usr/share/eole/sbin/active_rvp
```

2. Relancer la configuration EOLE

Après changement du paquet ARV et remplacement de `strongswan-starter` par `charon-systemd/swanctl`, relancer :

```
reconfigure
```

Attendu : Reconfiguration OK

3. Vérifier strongSwan / swanctl

```
systemctl status strongswan --no-pager  
swanctl --version
```

Attendu : les deux commandes fonctionnent.

Le service utilisé doit être `strongswan.service`, avec `charon-systemd`.

4. Lancer le wrapper

```
/usr/share/eole/sbin/eole-ipsec-to-swanctl  
echo "rc=$?"
```

Attendu : rc=0

Les warnings suivants ne sont pas bloquants :

```
agent plugin requires CAP_SETUID/CAP_SETGID capability  
plugin 'agent': failed to load - agent_plugin_create returned NULL
```

5. Test ARV direct

```
python3 - <<'PY'  
from arv.lib.sw_config_apply import ipsec_conf_apply  
  
ipsec_conf_apply(zephir=None)  
print("ipsec_conf_apply OK")  
PY
```

Attendu :

```
agent plugin requires CAP_SETUID/CAP_SETGID capability  
plugin 'agent': failed to load - agent_plugin_create returned NULL  
loaded certificate from '/etc/swanctl/x509ca/CA-sphinx-RVP.pem'  
no authorities found, 0 unloaded  
no pools found, 0 unloaded  
no connections found, 0 unloaded  
ipsec_conf_apply OK
```

Le point important : il ne doit plus y avoir :

```
ipsec: commande introuvable  
/usr/share/eole/sbin/eole-ipsec-to-swanctl: Aucun fichier ou dossier
```

6. Diagnostic

diagnose

Attendu :

```
*** Réseau virtuel privé
.                VPN => Aucun tunnel
.                ARV => Ok
```

ou équivalent sans traceback ni erreur VPN.

7. Test de conversion avec tunnel factice

Créer une connexion factice :

Comme ce tunnel est factice et utilise la CA comme certificat local, copier temporairement la CA dans le magasin des certificats machine swanctl :

```
mkdir -p /etc/swanctl/x509
cp -f /etc/ipsec.d/cacerts/CA-sphynx-RVP.pem /etc/swanctl/x509/
```

créer la connexion de test

```
cat > /etc/ipsec.d/conf/test-conv.conf <<'EOF'
conn test-conv
    left=192.168.0.11
    leftsubnet=172.30.101.0/24
    leftcert=CA-sphynx-RVP.pem
    leftid="C=FR, O=Education Nationale, L=Dijon, OU=0002 110043015, CN=CA-sphynx-RVP"
    right=192.168.0.24
    rightsubnet=172.30.102.0/24
    rightid=%any
    auto=add
EOF
```

Puis lancer :

```
/usr/share/eole/sbin/eole-ipsec-to-swanctl
echo "rc=$?"
swanctl --list-conns
```

Attendu :

```
loaded certificate from '/etc/swanctl/x509/CA-sphynx-RVP.pem'
loaded certificate from '/etc/swanctl/x509ca/CA-sphynx-RVP.pem'
loaded connection 'test-conv'
successfully loaded 1 connections
rc=0
```

Et dans `swanctl --list-conns`, on doit voir :

```
test-conv: IKEv1/2
local: 192.168.0.11[500]
remote: 192.168.0.24[500]
local: 172.30.101.0/24
remote: 172.30.102.0/24
```

8. Nettoyage

```
rm -f /etc/ipsec.d/conf/test-conv.conf
rm -f /etc/swanctl/x509/CA-sphynx-RVP.pem

/usr/share/eole/sbin/eole-ipsec-to-swanctl
echo "rc=$?"
swanctl --list-conns
```

Attendu :

```
rc=0
no connections found
```

ou :

```
no connections found, 1 unloaded
```

#2 - 11/08/2026 14:52 - Ludwig Seys

si passant =>

La migration technique strongSwan 6 / swanctl est validée.

ARV ne charge plus la configuration via strongswan-starter/ipsec, mais via un wrapper de conversion ipsec.conf -> swanctl.conf puis swanctl --load-all.

Les tests manuels confirment que la conversion, le chargement et le déchargement d'une connexion fonctionnent.

Il reste à valider le cycle fonctionnel complet ARV : création/import des objets via l'interface ou les imports EOLE, génération d'une vraie configuration VPN, puis chargement swanctl de cette configuration générée.

Ce qui restera à tester / valider

La partie fonctionnelle ARV complète, c'est-à-dire la génération réelle d'une configuration VPN depuis les données ARV, et non plus depuis un fichier de test manuel.

À tester :

1. Création d'une topologie via l'interface ARV
2. Ajout des nœuds / extrémités / connexions
3. Import ou génération des certificats attendus
4. Génération de la configuration ARV réelle
5. Présence de vrais blocs conn dans /etc/ipsec.d/conf/*
6. Conversion automatique vers /etc/swanctl/conf.d/eole-arv.conf
7. Chargement via swanctl --load-all
8. Vérification avec swanctl --list-conns
9. Vérification avec swanctl --list-sas si un tunnel réel peut être monté
10. Vérification diagnose

Le point restant sensible est l'interface ARV et ses imports EOLE/Zephir : la dernière fois, l'interface avait créé des données partielles en base, mais pas une topologie complète exploitable. Donc il faut encore confirmer que l'UI ou les imports EOLE génèrent bien les objets attendus jusqu'à produire de vrais fichiers de configuration qui seront convertis par le script.

#3 - 17/08/2026 10:28 - Ludwig Seys

- Assigné à Ludwig Seys supprimé

#4 - 21/09/2026 16:18 - Ludwig Seys

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

valide :

[#37578](#)

[#37579](#)

[#37580](#)

[#37583](#)

[#37584](#)

[#37585](#)

#5 - 21/09/2026 16:18 - Ludwig Seys

- Assigné à mis à Ludwig Seys