EOLE AD DC - Tâche #37650

Scénario # 37406 (Nouveau): Porter Sphynx en 2.11

Validation technique strongSwan 6 / swanctl OK

21/09/2026 15:35 - Ludwig Seys

Statut:	À valider	**Début:**	21/09/2026
Priorité:	Normal	**Echéance:**	
Assigné à:	Ludwig Seys	**% réalisé:**	90%
Version cible:	Carnet Cadoles - MEN	**Temps estimé:**	0.00 heure

Description

reprise à 0, installation propre.

Problème à l'instance attendus =>

```
Le répertoire /etc/ipsec.d n'existe pas mais est obligatoire pour /etc/ipsec.d/ipsec_updown
Le répertoire /etc/ipsec.d n'existe pas mais est obligatoire pour /etc/ipsec.d/ipsec_updown
```

résolution manuel :

```
install -d -m 755 /etc/ipsec.d
install -d -m 755 /etc/ipsec.d/conf
install -d -m 755 /etc/ipsec.d/cacerts
install -d -m 755 /etc/ipsec.d/certs
install -d -m 755 /etc/ipsec.d/crls
install -d -m 700 /etc/ipsec.d/private
```

nécessite création d'un pretemplate
Ensuite, comme attendue, contretemps durant l'instance car le fichier de conf est vide. résolution manuel :

```
cat > /etc/ipsec.conf <<'EOF'
# configuration minimale legacy ARV, convertie ensuite vers swanctl

config setup
    uniqueids = yes
    cachecrls = yes
    strictcrlpolicy = no

conn %default
    keyingtries = 3
    keyexchange = ike
    authby = pubkey
    dpdaction = clear
    dpddelay = 120s
    ike = aes128-sha256-modp2048,aes192-sha384-modp3072
    esp = aes128gcm128,aes192gcm128,aes128-sha256
    forceencaps = no
    mobike = no

include /etc/ipsec.d/conf/*
EOF

install -m 600 /dev/null /etc/ipsec.secrets
```

a implémenter dans eole-vpn.

Révisions associées

Révision 0ed107b4 - 21/09/2026 15:50 - Ludwig Seys

création des fichier nécessaire à strongswan-swanctl

ref #37650

Révision 38d772df - 21/09/2026 15:52 - Ludwig Seys

ajout et prise en charge d'une conf minimale pour start le service

ref #37650

Historique

#1 - 21/09/2026 16:15 - Ludwig Seys

- Sujet changé de instance fonctionnelle à Validation technique strongSwan 6 / swanctl OK

test pour valider après maj et installation du nouveau paquet :

1. copie de la fausse clé

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

2. création test-conv + conversion + 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

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

3. retour attendu

```
agent plugin requires CAP_SETUID/CAP_SETGID capability
plugin 'agent': failed to load - agent_plugin_create returned NULL
loaded certificate from '/etc/swanctl/x509/CA-sphynx-RVP.pem'
loaded certificate from '/etc/swanctl/x509ca/CA-sphynx-RVP.pem'
no authorities found, 0 unloaded
no pools found, 0 unloaded
loaded connection 'test-conv'
successfully loaded 1 connections, 0 unloaded
rc=0
agent plugin requires CAP_SETUID/CAP_SETGID capability
plugin 'agent': failed to load - agent_plugin_create returned NULL
test-conv: IKEv1/2, no reauthentication, rekeying every 14400s, dpd delay 120s
  local:  192.168.0.11[500]
  remote: 192.168.0.24[500]
```

```
  local unspecified authentication:
    id: C=FR, O=Education Nationale, L=Dijon, OU=0002 110043015, CN=CA-sphynx-RVP
    certs: C=FR, O=Education Nationale, L=Dijon, OU=0002 110043015, CN=CA-sphynx-RVP
  remote unspecified authentication:
    id: %any
  test-conv: TUNNEL, rekeying every 3600s, dpd action is none
    local:  172.30.101.0/24
    remote: 172.30.102.0/24
```

4. après test, 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
```

5. retour 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-sphynx-RVP.pem'
no authorities found, 0 unloaded
no pools found, 0 unloaded
no connections found, 1 unloaded
rc=0
agent plugin requires CAP_SETUID/CAP_SETGID capability
plugin 'agent': failed to load - agent_plugin_create returned NULL
```

Ce qui in fine nous amène : conversion - chargement - déchargement => OK

```
ipsec.conf + /etc/ipsec.d/conf/test-conv.conf
        ↓
eole-ipsec-to-swanctl
        ↓
conversion ipsec2swanctl
        ↓
/etc/swanctl/conf.d/eole-arv.conf
        ↓
swanctl --load-all
        ↓
connexion visible avec swanctl --list-conns
        ↓
suppression du fichier legacy
        ↓
connexion déchargée proprement
```

Validation technique strongSwan 6 / swanctl OK.

Sur VM neuve avec paquets DEV :
- instance/reconfigure OK ;
- diagnose OK ;
- VPN => Aucun tunnel ;
- ARV => Ok ;
- wrapper eole-ipsec-to-swanctl OK ;
- ipsec_conf_apply OK ;
- conversion d'une connexion legacy factice OK ;
- chargement visible via swanctl --list-conns OK ;
- déchargement après suppression du fichier legacy OK.

Reste à valider le cycle fonctionnel complet ARV :
création/import des objets via interface ou imports EOLE/Zephir,

génération réelle des fichiers /etc/ipsec.d/conf/*,
conversion automatique, chargement swanctl, puis montage réel d'un tunnel.

#2 - 21/09/2026 16:16 - Ludwig Seys

- Statut changé de En cours à À valider

- % réalisé changé de 30 à 90

#3 - 21/09/2026 16:19 - Ludwig Seys

- Tâche parente changé de #37568 à #37406