Installer d'une sonde Svalinn virtualisée

Voir ici pour les prérequis : https://wiki.esia-sa.com/intro/prerequis#box_svalinn

Svalinn Scanner

copy

```
apt update
apt install gnupg
```

copy

```
echo "deb http://stable.repository.esia-sa.com/esia bookworm main
contrib non-free non-free-firmware" >> /etc/apt/sources.list
wget -O- "http://stable.repository.esia-sa.com/esia/gnupg.key" |
apt-key add -
```

copy

```
apt update
apt install snmpd -y
apt install gesa-base -y
apt install gesa-svalinn-base -y
```

Ajouter le numéro de série

Il faut éditer le fichier /etc/gesa/sn

copy

```
echo "<ton SN>" > /etc/gesa/sn
```

Configurer SNMP

Ensuite, il faut aller éditer le fichier de configuration :

copy

```
nano /etc/snmp/snmpd.conf
```

Il faut ensuite configurer la communauté SNMP en ajoutant la ligne suivante:

copy

```
rocommunity public localhost
```

Sauvegardez le fichier avec ctrl+o et ctrl+x pour quitter.

Redémarrer les services

copy

```
/etc/init.d/snmpd restart
/etc/init.d/ecatp-client restart
```

Votre Unity est maintenant active et doit remonter dans votre interface comme une Unity classique, vous pouvez vous rendre au tuto suivant.

Esia mercury avec Svalinn

copy

```
apt update
apt install gnupg
```

copy

```
echo "deb http://stable.repository.esia-sa.com/esia bookworm
contrib non-free" >> /etc/apt/sources.list
wget -O- "http://stable.repository.esia-sa.com/esia/gnupg.key" |
apt-key add -
```

copy

```
echo "deb http://svalinn.repository.esia-sa.com/svalinn bookworm
contrib non-free" >> /etc/apt/sources.list
wget -O- "http://svalinn.repository.esia-sa.com/svalinn/gnupg.key"
| apt-key add -
```

copy

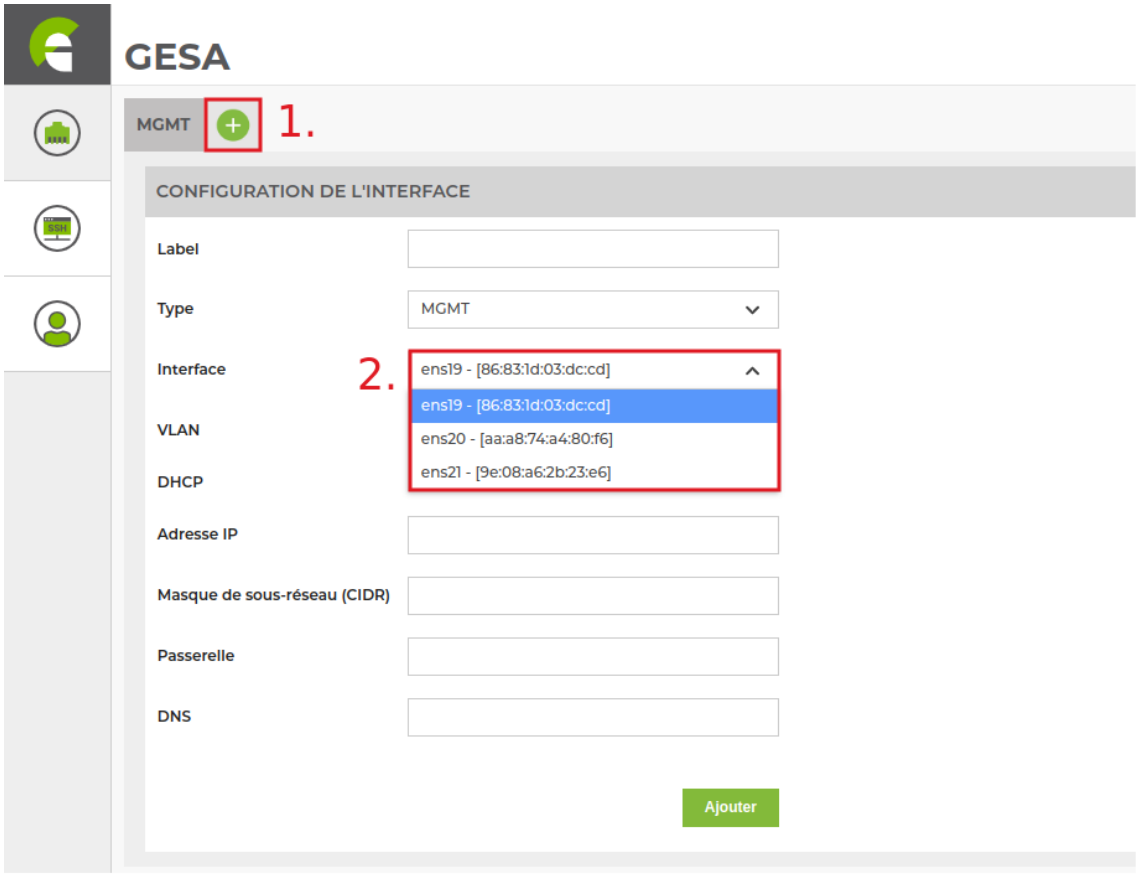
```
apt update
apt install esia-enterprise-base esia-db-plugins-gesa esia-ecatp-
```

```
server
apt install esia-webp-svascan esia-webp-inventory
apt install esia-svascan-cve
```

Configurer interfaces

Après avoir installé le scanner de vulnérabilité. Il faut ajouter les interfaces depuis l'interface graphique. Ensuite rendez-vous sur l'onglet interface.

Cliquez sur le +, remplissez le formulaire et choisissez l'interface.



VM Svalinn scanner sous VMWare

Si vous utilisez VMWare, il se peut que les scans Svalinn ne détectent pas de noeuds (y compris dans le même VLAN). Ceci est du à l'utilisation de containers et des drivers réseaux macvlan qui requiert que la VM utilise des adresses macs différentes de celle de l'interface réseau (VMWare).

Vous pouvez dans VMWare vérifier les options suivantes :

- Le mode Promiscuous est actif
- L'option Forged Transmits est configuré sur 'Accept'

VM Svalinn scanner sous HyperV

Si vous utilisez Hyper-V, il se peut que les scans Svalinn ne détectent pas de noeuds. Depuis l'interface graphique d'Hyper-V, vous pouvez activer cette option en accédant aux paramètres de la machine virtuelle. Cliquez sur le symbole “**+**” à côté de “**Carte réseau**”, puis sélectionnez “**Fonctionnalités avancées**”. Enfin, cochez l’option “**Activer l’usurpation d’adresse MAC**”.