```
Installing Svalinn
```

See here for prerequisites: https://wiki.esia-sa.com/intro/prerequis#box\_svalinn

# **Svalinn Scanner**

### сору

apt update apt **install** gnupg

### сору

```
echo "deb http://stable.repository.esia-sa.com/esia bullseye
contrib non-free" >> /etc/apt/sources.list
wget -0- "http://stable.repository.esia-sa.com/esia/gnupg.key" |
apt-key add -
```

#### сору

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

## Add the serial number

You need to edit the /etc/gesa/sn file

### сору

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

## **Configure SNMP**

Next, edit the :

## сору

nano /etc/snmp/snmpd.conf

You then need to configure the SNMP community by adding the following line:

#### сору

rocommunity public localhost

Save the file with ctrl+o and ctrl+x to exit.

### **Restart services**

сору

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

Your Unity is now active and should appear in your interface like a regular Unity. You can go to the following tutorial following tutorial.

## Esia mercury with Svalinn

```
сору
```

apt update apt **install** gnupg

#### сору

```
echo "deb http://stable.repository.esia-sa.com/esia bullseye
contrib non-free" >> /etc/apt/sources.list
wget -0- "http://stable.repository.esia-sa.com/esia/gnupg.key" |
apt-key add -
```

#### сору

```
echo "deb http://svalin.repository.esia-sa.com/svalin bullseye
contrib non-free" >> /etc/apt/sources.list
wget -0- "http://svalin.repository.esia-sa.com/svalin/gnupg.key"
apt-key add -
```

#### сору

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-svalin-cve-all
```

# **Configure interfaces**

Once you have installed the vulnerability scanner. You need to add the interfaces from the graphical interface. Then go to the interface tab.

E	GESA					
	INFORMATIONS GÉNÉRALES					
	Adresse IP publique /	Numéro de série	Serveur lié	/		
	Adresse IP locale	Туре	Port de connexion	/		
	Masque de sous-réseau	Modèle				
2	Passerelle	Version de l'OS Debian 11.7				
	DNS					
	MISES À JOUR				Mettre à jour	
	Dernière mise à jour - Début Heure	e de mise à jour journalière Pas conf	igurées			
	Dernière mise à jour - Fin					

Click on the +, fill in the form and choose the interface.

F	GESA						
	мсмт 🕒 1.						
	CONFIGURATION DE L'INTERFACE						
	Label		]				
	Туре	MGMT V					
-	Interface 2.	ens19 - [86:83:1d:03:dc:cd]					
	VLAN	ens19 - [86:83:1d:03:dc:cd] ens20 - [aa:a8:74:a4:80:f6]					
	DHCP	ens21 - [9e:08:a6:2b:23:e6]					
	Adresse IP		]				
	Masque de sous-réseau (CIDR)		]				
	Passerelle		]				
	DNS						
		Ajouter					

## VM Svalinn scanner under VMWare

If you are using VMWare, Svalinn scans may not detect nodes (even in the same VLAN). This is due to the use of containers and macvlan network drivers which require the VM to use different mac addresses to the network interface (VMWare).

You can check the following options in VMWare:

- Le Promiscuous mode is active
- L'option Forged Transmits is set to 'Accept'.

# VM Svalinn scanner under HyperV

From the Hyper-V graphical interface, you can activate this option by accessing the virtual machine settings. Click on the "+"symbol next to**Network card**"and then select**Advanced features**". Finally, tick the option "**Enable MAC address spoofing**".

/m-cluster-1	$\sim$		<u>ی</u>		
Matériel	^	Fonctio	onnalités avancées		
Ajouter un matériel					
BIOS		Adres	sse MAC		
Démarrer à partir de CD			Dynamique		
Sécurité		0:	Statique		
Lecteur de stockage de de des					
Memoire 1024 Mo			00 - 13 - 30 - 00 - 19 - 01		
		L'usu	urpation d'adresse MAC permet aux ordinateurs virtuels d	e remplacer	
1 processeur virtuel		l'adre	esse MAC source dans les paquets sortants par une adre	sse qui ne le	ur est
Contrôleur IDE 0		pas	attribuée.		
+ Disque dur			Activer l'usurpation d'adresse MAC		
vm-cluster_E4071529-382.					
🗉 🔳 Contrôleur IDE 1		Prote	ection DHCP		
Lecteur de DVD		Lap	rotection DHCP supprime les messages serveur DHCP des	ordinateurs	
Aucun		virtu	iels non autorisés se faisant passer pour des serveurs DH	CP.	
🗉 🗐 Contrôleur SCSI			Activer la protection DHCP		
🗉 🚃 Disque dur					
second disque.vhdx	<u> </u>	Prote	ection de routeur		
Carte réseau		Lap	rotection de routeur supprime les messages de redirection	et d'annon	ce de
		rout	eur des ordinateurs virtuels non autorisés se faisant pass	er pour des	
Acceleration materielle		rout	eurs.		
Fonctionnalites avancees		🗌 /	Activer la protection de publication de routeur		
		Résea	au protégé		
Aucun		Dépl	lacez cet ordinateur virtuel vers un autre nœud de cluster	si une	
Lecteur de disquettes		déco	onnexion réseau est détectée.		
Aucun			Réseau protégé		
Cestion					
I Nom		Mise	en miroir de ports		
vm-cluster-1		lam	nise en miroir de ports permet une surveillance du trafic ré	seau d'un	
Services d'intégration		ordir	nateur virtuel en copiant les paquets entrants et sortants,	eten	
Quelques services offerts	$\sim$	trans	sférant les copies vers un autre ordinateur virtuel configu	ré pour l'ana	alyse.

