Installer d'une sonde Svalinn virtualisée

Voir ici pour les prérequis : 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 bookworm main contrib non-free non-free-firmware" >> /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-svalinn-base -y
```

Ajouter le numéro de série

Il faut éditer le fichier /etc/gesa/sn

сору

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

Configurer SNMP

Ensuite, il faut aller éditer le fichier de configuration :

сору

nano /etc/snmp/snmpd.conf

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

сору

rocommunity public localhost

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

Redémarrer les services

сору

/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

```
сору
```

apt update apt **install** gnupg

сору

```
echo "deb http://stable.repository.esia-sa.com/esia bookworm
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://svalinn.repository.esia-sa.com/svalinn bookworm
contrib non-free" >> /etc/apt/sources.list
wget -0- "http://svalinn.repository.esia-sa.com/svalinn/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-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.

6	GESA						
	INFORMATIONS GÉNÉRALES						
\smile	Adresse IP publique /	Numéro de série	Serveur lié	/			
	Adresse IP locale	Туре	Port de connexion	/			
Ð	Masque de sous-réseau	Modèle					
	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						

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

F	GESA					
	мсмт 💽 1.					
\frown	CONFIGURATION DE L'INTERFACE					
	Label					
	Туре	MGMT	/			
	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					
		Ajoute				

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**".

vn	n-cluster-1	\sim	- I		0	
*	Matériel	^	Fon	ction	nalités avancées	
	Ajouter un matériel					
	BIOS		A	iress	e MAC	
	Démarrer à partir de CD) D	ynamique	
	V Sécurité) st	tatique	
	Lecteur de stockage de dé dés.			- -		
	Mémoire			0	10 - 15 - 50 - 00 - 19 - 01	
-	1024 Mo			Licur	nation d'adresse MAC permet aux ordinateurs virtuels de remplacer	
±	Processeur I processeur wirtuel		l k	adre	sse MAC source dans les paquets sortants par une adresse qui ne leur es	st
	Contrôlour IDE 0			as a	ttribuée.	
	Disgue dur				ctiver l'usurpation d'adresse MAC	
	vm-duster E4071529-382					
-	Contrôleur IDE 1		Dr	otec		
	Lecteur de DVD			apro	atection DHCP supprime les messages serveur DHCP des ordinateurs	
	Aucun			irtue	Is non autorisés se faisant passer pour des serveurs DHCP.	
-	Contrôleur SCSI		l r		ctiver la protection DHCP	
	+ Disque dur			^		
	second disque.vhdx					
Ξ	📮 Carte réseau		Pr Pr	otec	tion de routeur	
	LAN 1			a pro	otection de routeur supprime les messages de redirection et d'annonce de ur des ordinateurs virtuels non autorisés se faisant nasser pour des	e
	Accélération matérielle		r r	oute	urs.	
	Fonctionnalités avancées		Г		ctiver la protection de publication de routeur	
	🛱 СОМ 1					
	Aucun					
	COM 2		Re	èseau	u protégé	
	Aucun)épla lécor	cez cet ordinateur virtuel vers un autre nœud de cluster si une mexion réseau est détectée	
	Lecteur de disquettes				(
	Aucun				eseau protege	
~	Gestion	- 1				
	I Nom		Mi	se er	n miroir de ports	
			L	a mis	e en miroir de ports permet une surveillance du trafic réseau d'un	
	Ouelaues services offerts		0	rdina	ateur virtuel en copiant les paquets entrants et sortants, et en férant les copies vers un autre ordinateur virtuel configuré pour l'apalves	
	fooder of they dilet to	Ŧ		- un al	renences copies vers an addie orainateur virtuer configure pour ranalyse	

