Procédure installation et configuration d’une Sonde Snort

Auteur : Arthur GUILET
Reference : Assurmer
Date : 07/04/2023

DIFFUSION et VISAS

Diffusion				
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**	**Pour info**
Assumer	Service IT	Procédure	Réseau	

Visas			
Société/Entité	**Nom**	**Fonction**	

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.0	07/04/2023	Arthur GUILET	Installation et configuration d'une Sonde Snort	6

COORDONNEES

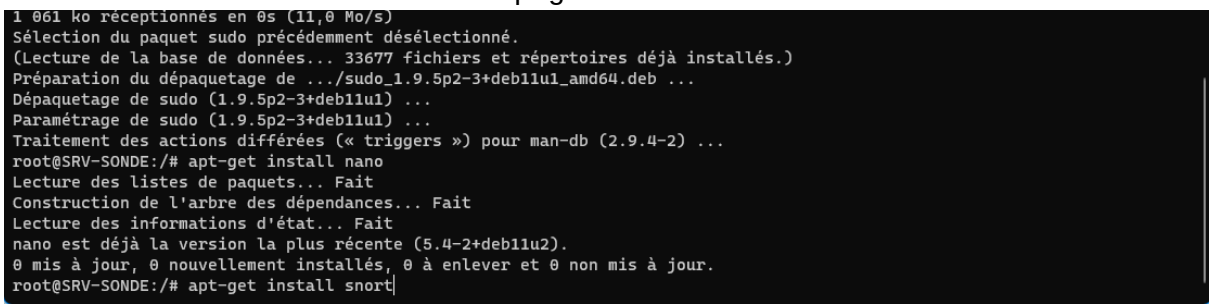
Contacts		
Nom	**E-mail**	**Téléphone**
Arthur GUILET	arthur.guilet@assurmer.fr	01.54.23.79.02

SOMMAIRE

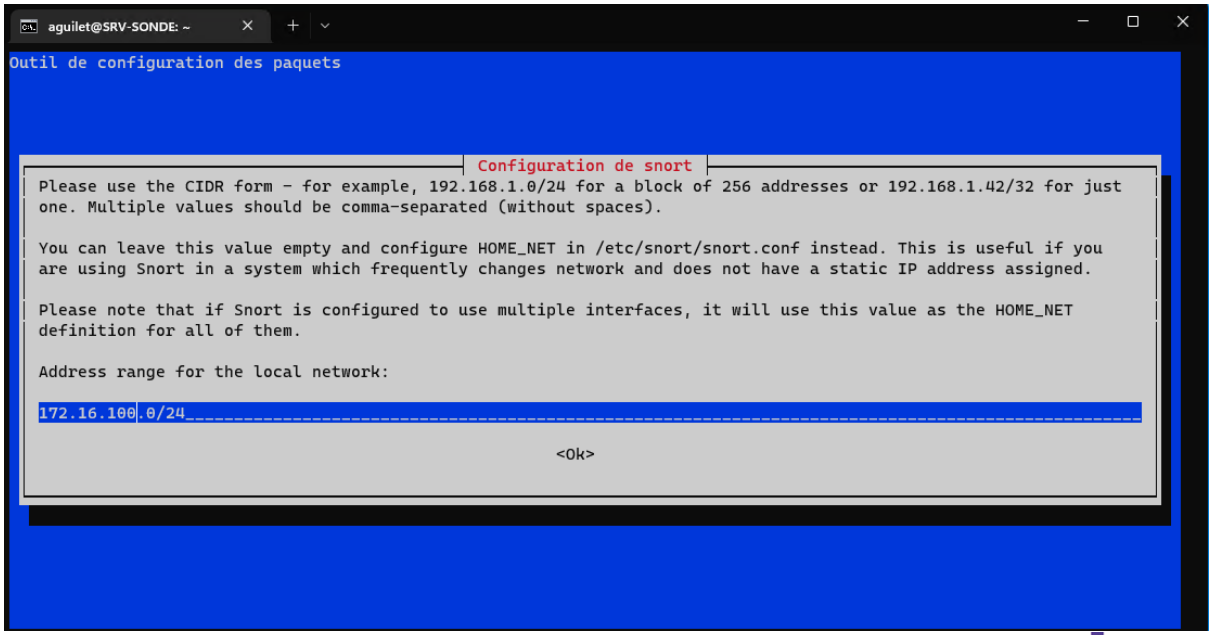
Installation de Snort

1.Commencer par mettre à jour votre machine avec un : apt-get update & upgrade

2. Installer Snort avec la commande : apt-get install snort

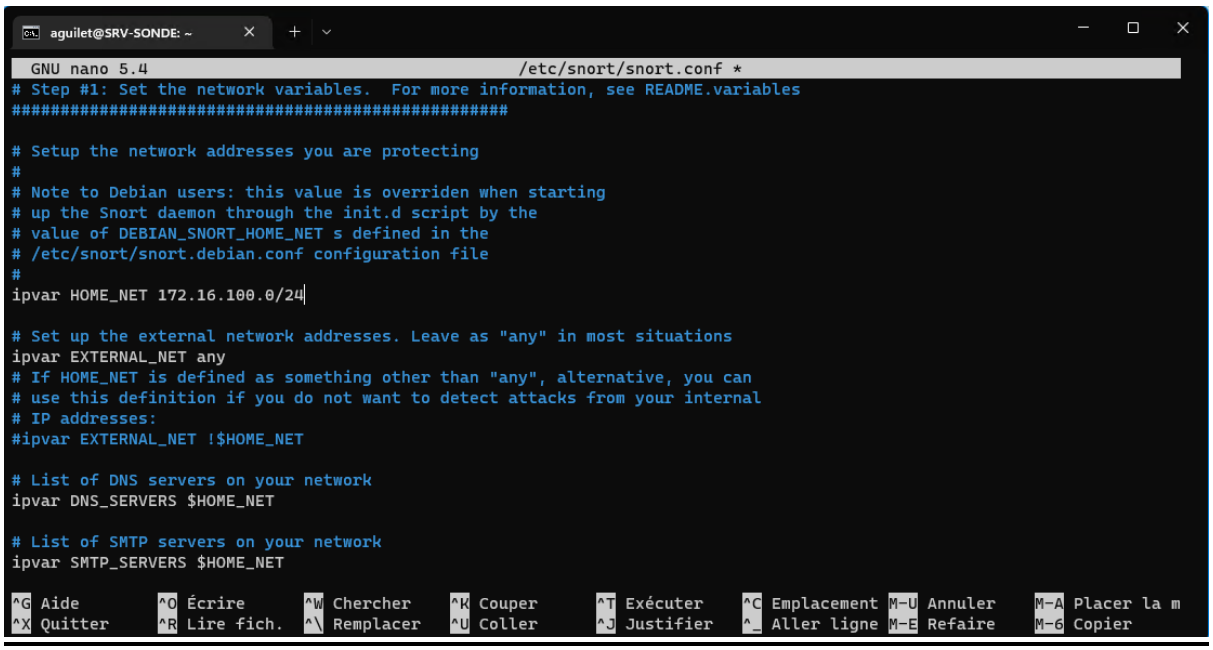


3. Indiquer le réseau que vous souhaitez écouter avec snort dans notre cas le réseau serveur : 172.16.100.0/24

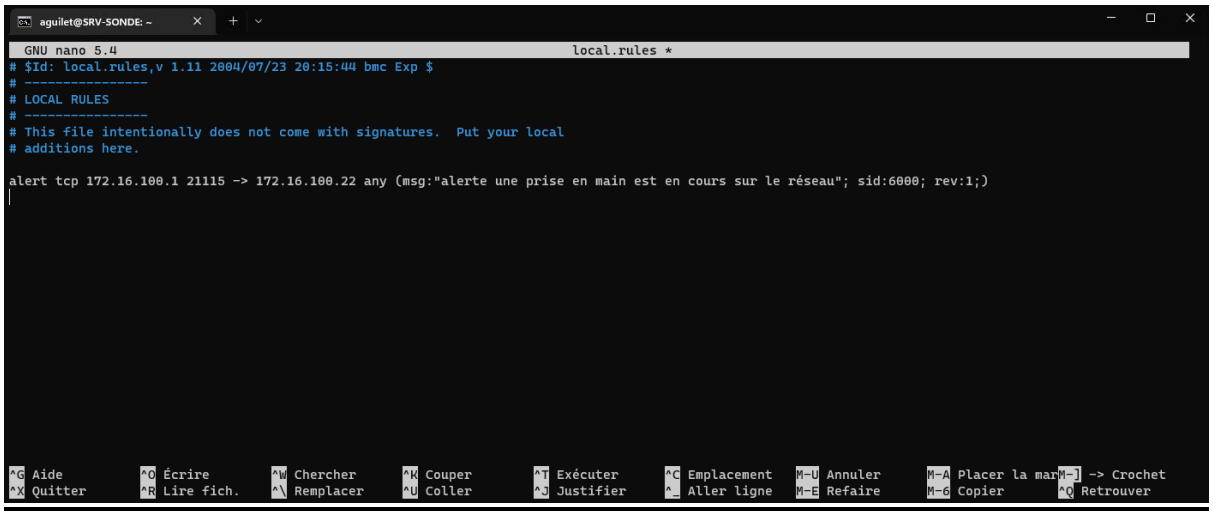


Configuration de Snort

4.Aller dans le fichier de conf de snort pour indiquer correctement le réseau. Le chemin : cd /etc/snort/snort.conf. En modifier avec l'adresse de votre réseau ipvar HOME_NET any



5.Aller dans le fichier de rules de snort pour indiquer vos premières règles. Le chemin : cd /etc/snort/rules et ensuite faite nano local.rules. Exemple pour écouter rustdesk : alert tcp 172.16.100.1 21115 -> 172.16.100.22 any (msg:"alerte une prise en main est en cours sur le réseau"; sid:6000; rev:1;)



6.Ensuite tester la votre nouvelle configuration si elle est bien valide avec la commande : snort -T -c /etc/snort/snort.conf

```
bash: cd: /etc/snort/snort.conf: N'est pas un dossier
root@SRV-SONDE:/# nano /etc/snort/snort.conf
root@SRV-SONDE:/# cd /etc/snort/rules/
root@SRV-SONDE:/etc/snort/rules# nano local.rules
root@SRV-SONDE:/etc/snort/rules# cd /
root@SRV-SONDE:/# snort -T -c /etc/snort/snort.conf
```

7. Après test

```
Total snort Fixed Memory Cost - MaxRss:106232
Snort successfully validated the configuration!
Snort exiting
root@SRV-SONDE:~# _
```

8. Enfin pour lancer l'analyse de votre réseau avec snort lancer la commande : snort -A console -c /etc/snort/snort.conf

```
Total snort Fixed Memory Cost - MaxRss:106232
Snort successfully validated the configuration!
Snort exiting
root@SRV-SONDE:~# snort -A console -c /etc/snort/snort.conf _
```

9. Et enfin complet il vous reste seulement à ajouter les règles que vous souhaitez