



Procédure installation et configuration d'une Sonde Snort

Auteur : Arthur GUILLET

Reference : Assumer

Date : 07/04/2023



	Titre	Reference	Page	
	Installation et configuration d'une Sonde Snort	Assumer	2 / 6	

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 GUILLET	Installation et configuration d'une Sonde Snort	6



COORDONNEES

Contacts		
Nom	E-mail	Téléphone
Arthur GUILLET	arthur.guilet@assumer.fr	01.54.23.79.02

	Titre	Reference	Page	
	Installation et configuration d'une Sonde Snort	Assumer	3 / 6	

SOMMAIRE

-Installation de Windows Serveur 2019	page 5
-Configuration de Windows serveur 2019	page 7
-Installation de l'active directory	page 10
-Vérification de la réplication du serveur	page 14

	Titre	Reference	Page	
	Installation et configuration d'une Sonde Snort	Assumer	4 / 6	

Installation de Snort

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

```

aguilet@SRV-SONDE: ~
Microsoft Windows [version 10.0.22621.1485]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\unknown>ssh aguilet@172.16.100.4
The authenticity of host '172.16.100.4 (172.16.100.4)' can't be established.
ED25519 key fingerprint is SHA256:nfFGtRmYVx5cbI1VdtkRjodDVkXh1AE2chAu/ppwe0c.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.100.4' (ED25519) to the list of known hosts.
aguilet@172.16.100.4's password:
Linux SRV-SONDE 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
aguilet@SRV-SONDE:~$ su
Mot de passe :
root@SRV-SONDE:/home/aguilet# cd /
root@SRV-SONDE:/# apt-get update & upgrade

```

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

```

1 061 ko réceptionnés en 0s (11,0 Mo/s)
Sélection du paquet sudo précédemment désélectionné.
(Lecture de la base de données... 33677 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../sudo_1.9.5p2-3+deb11u1_amd64.deb ...
Dépaquetage de sudo (1.9.5p2-3+deb11u1) ...
Paramétrage de sudo (1.9.5p2-3+deb11u1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@SRV-SONDE:/# apt-get install nano
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
nano est déjà la version la plus récente (5.4-2+deb11u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@SRV-SONDE:/# 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

```

aguilet@SRV-SONDE: ~
Outil de configuration des paquets



Configuration de snort
Please use the CIDR form - for example, 192.168.1.0/24 for a block of 256 addresses or 192.168.1.42/32 for just one. Multiple values should be comma-separated (without spaces).

You can leave this value empty and configure HOME_NET in /etc/snort/snort.conf instead. This is useful if you are using Snort in a system which frequently changes network and does not have a static IP address assigned.

Please note that if Snort is configured to use multiple interfaces, it will use this value as the HOME_NET definition for all of them.

Address range for the local network:
172.16.100.0/24
<Ok>

```

	Titre	Reference	Page	
	Installation et configuration d'une Sonde Snort	Assumer	5 / 6	

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

```

GNU nano 5.4 /etc/snort/snort.conf *
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 172.16.100.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler   M-A Placer la m
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire   M-6 Copier

```

5. Aller dans le fichier de règles de snort pour indiquer vos premières règles. Le chemin : `cd /etc/snort/rules` et ensuite faire `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;)`



```

GNU nano 5.4 local.rules *
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# -----
# LOCAL RULES
# -----
# This file intentionally does not come with signatures. Put your local
# additions here.

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;)
|

^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler   M-A Placer la mar
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire   M-6 Copier   M-> Crochet

```

	Titre	Reference	Page	
	Installation et configuration d'une Sonde Snort	Assumer	6 / 6	

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

```
root@SRV-SONDE:~# cd /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