TPLOG Compte rendu Noa Fontaine

Compétences :

Déployer les moyens appropriés de preuve électronique (suite)Identifier les obligations légales qui s'imposent en matière d'archivage et deprotection des données de l'organisationOrganiser la collecte et la conservation des preuves numériques

Contexte :

ChezNexylan, nous accompagnons nos clients au quotidien et proposons des solutions qui lesdélestent totalement de la gestion technique. Nos clients se concentrent sur leur réel métier, ils nousfont confiance pour la gestion technique de leur infrastructure.Notre volonté est d'apporter une expertise et un accompagnement qui dépassent les standardshabituels. Nous avons les capacités techniques et les compétences pour accompagner les projets denos clients depuis les couches les plus basses (serveurs, hardware, réseau) jusqu'aux couches les plusélevées d'une application Web (sécurité applicative, performances, vitesse de chargement) enmettant en oeuvre des couches intermédiaires de haute qualité (redondance, haute-disponibilité,sauvegarde).Vous faites partie de l'équipe SOC de l'entrepriseNexylanet pour donner suite à un incident desécurité sur la plateforme d'un client, il est demandé de mettre en place une solution permettant des'assurer du suivi des actions sur les différents serveurs Windows et Linux.Pour cela, vous traiterez les différentes missions ci-dessous mais également vous repondérez auxdifférents tickets du client, encore sous pression pour donner suite à l'attaque subit.

Mission 1

On vous demande de mettre en place l'outil permettant la centralisation des logs « Rsyslog » sur unserveur Rocky Linux ayant la configuration ci-dessous :

- 2 VCPU

- 2 Go de RAM

- 30 Go de disque

Vous pouvez utiliser l'annexe 1 à votre disposition pour vous aider dans la mise en place du serveur

Hostname :

```
[root@RSYSLOG-1 ~]# hostname
SRV-RSYSLOG
```

Installation package RSYSLOG sur le SRVRSYSLOG :

```
Rocky Linux 9.1 (Blue Onyx)
Kernel 5.14.0-162.6.1.el9_1.x86_64 on an x86_64

RSYSLOG-1 login: root
Password:
Last failed login: Wed Mar 29 16:15:11 CEST 2023 from 192.168.213.1 on ssh:notty
There were 13 failed login attempts since the last successful login.
Last login: Wed Mar 29 16:08:21 on tty1
[root@RSYSLOG-1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:7d:a9:57 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.213.154/24 brd 192.168.213.255 scope global dynamic noprefixroute ens160
       valid_lft 1745sec preferred_lft 1745sec
    inet6 fe80::20c:29ff:fe7d:a957/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@RSYSLOG-1 ~]# dnf install rsyslog nano -y
```

```
[root@RSYSLOG-1 ~]# dnf install rsyslog nano -y
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
Package rsyslog-8.2102.0-105.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                Architecture            Version                  Rep
================================================================================
Installing:
 nano                   x86_64                  5.6.1-5.el9              bas

Transaction Summary
================================================================================
Install  1 Package

Total download size: 694 k
Installed size: 2.7 M
Downloading Packages:
nano-5.6.1-5.el9.x86_64.rpm
--------------------------------------------------------------------------------
Total
Rocky Linux 9 - BaseOS
Importing GPG key 0x350D275D:
 Userid     : "Rocky Enterprise Software Foundation - Release key 2022 <releng@rockylinux.org>"
 Fingerprint: 21CB 256A E16F C54C 6E65 2949 702D 426D 350D 275D
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-Rocky-9
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : nano-5.6.1-5.el9.x86_64
  Running scriptlet: nano-5.6.1-5.el9.x86_64
  Verifying        : nano-5.6.1-5.el9.x86_64

Installed:
  nano-5.6.1-5.el9.x86_64

Complete!
[root@RSYSLOG-1 ~]#
```

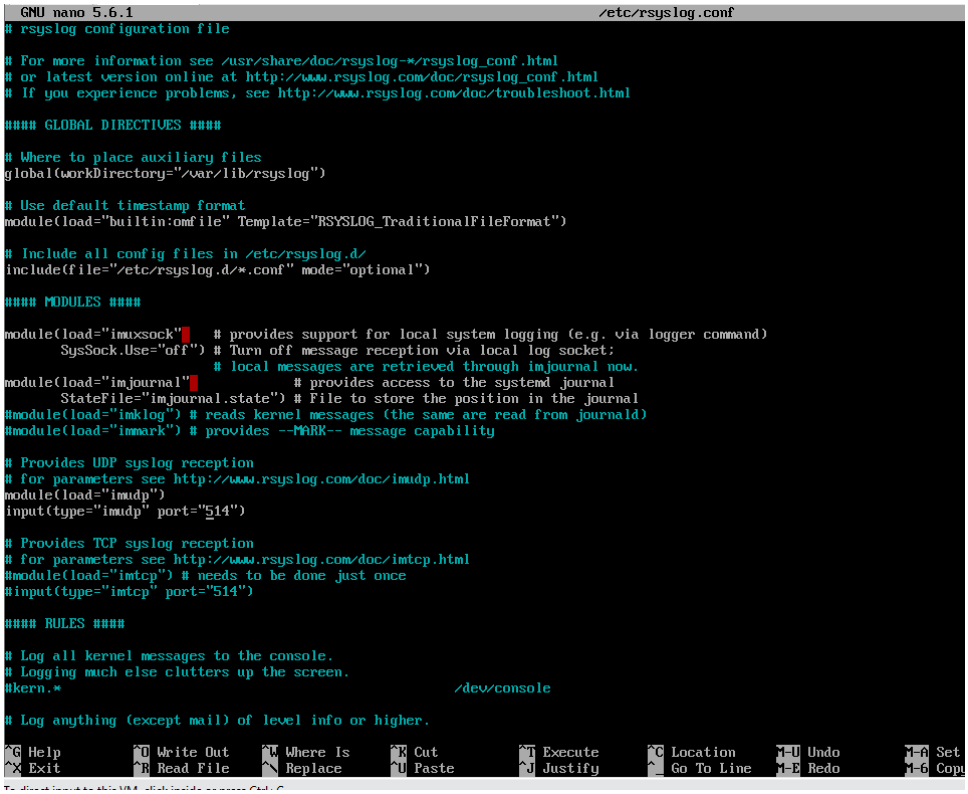
Ouverture port 514 dans firewall avec protocole UDP

```
[root@RSYSLOG-1 ~]# firewall-cmd  --add-port=514/udp --permanent
success
[root@RSYSLOG-1 ~]#
```

```
[root@RSYSLOG-1 ~]# firewall-cmd --reload
success
[root@RSYSLOG-1 ~]#
```

Edition fichier rsyslog.conf dans /etc/ grâce à la commande : nano /etc/rsyslog.conf

Il faut décommenter les lignes module et input pour activer le SRVRSYSLOG qui écoute sur le port 514 en UDP



Désactivation SELINUX

```
[root@RSYSLOG-1 ~]# setenforce 0
[root@RSYSLOG-1 ~]#
```

NB : c'est à faire après chaque redémarrage.

Démarrer le service rsyslog et activer au démarrage

```
[root@RSYSLOG-1 ~]# systemctl start rsyslog
[root@RSYSLOG-1 ~]# systemctl enable rsyslog
[ 1031.987329] systemd-rc-local-generator[10821]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@RSYSLOG-1 ~]#
```

Indentification version rsyslog

```
[root@RSYSLOG-1 ~]# rsyslogd -v
rsyslogd  8.2102.0-105.el9 (aka 2021.02) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@RSYSLOG-1 ~]#
```

Vérification du service rsyslog (on vérifie si il écoute bien sur le port 514 en UDP)

```
[root@RSYSLOG-1 ~]# ss -4tunlp | grep 514
[root@RSYSLOG-1 ~]#
```

Mission 2

Suite à la mise en place du serveur Rsyslog, vous allez maintenant sur un deuxième serveur RockyLinux configurer Rsyslog en tant que client pour permettre d'envoyer les évènements sur le serveur

Vous pouvez utiliser les annexes 2 et 3 à votre disposition pour vous aider dans la mise en place du serveur

Installation package rsyslog sur deuxième serveur

```
[root@SRV-CLIENT ~]# dnf install rsyslog nano -y
Rocky Linux 9 - BaseOS                                          371 kB/s | 1.8 MB     00:04
Rocky Linux 9 - AppStream                                       2.8 MB/s | 6.6 MB     00:02
Rocky Linux 9 - Extras                                          9.5 kB/s | 8.5 kB     00:00
Package rsyslog-8.2102.0-105.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================================================
 Package               Architecture            Version                       Repository                Size
================================================================================================================
Installing:
 nano                  x86_64                  5.6.1-5.el9                   baseos                   694 k

Transaction Summary
================================================================================================================
Install  1 Package

Total download size: 694 k
Installed size: 2.7 M
Downloading Packages:
nano-5.6.1-5.el9.x86_64.rpm                                     3.9 MB/s | 694 kB     00:00
----------------------------------------------------------------------------------------------------------------
Total                                                           1.8 MB/s | 694 kB     00:00
Rocky Linux 9 - BaseOS                                          1.7 MB/s | 1.7 kB     00:00
Importing GPG key 0x350D275D:
 Userid     : "Rocky Enterprise Software Foundation - Release key 2022 <releng@rockylinux.org>"
 Fingerprint: 21CB 256A E16F C54C 6E65 2949 702D 426D 350D 275D
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-Rocky-9
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                              1/1
  Installing       : nano-5.6.1-5.el9.x86_64                                                      1/1
  Running scriptlet: nano-5.6.1-5.el9.x86_64                                                      1/1
  Verifying        : nano-5.6.1-5.el9.x86_64                                                      1/1

Installed:
  nano-5.6.1-5.el9.x86_64

Complete!
[root@SRV-CLIENT ~]#
```

Désactivation Selinux

NB : c'est à faire après chaque redémarrage.

```
[root@SRV-CLIENT ~]# setenforce 0
[root@SRV-CLIENT ~]#
```

Edition fichier rsyslog.conf présent dans /etc/ et il faut indiquer l'adresse ip, le port et le protocole de fonctionnement du serveur

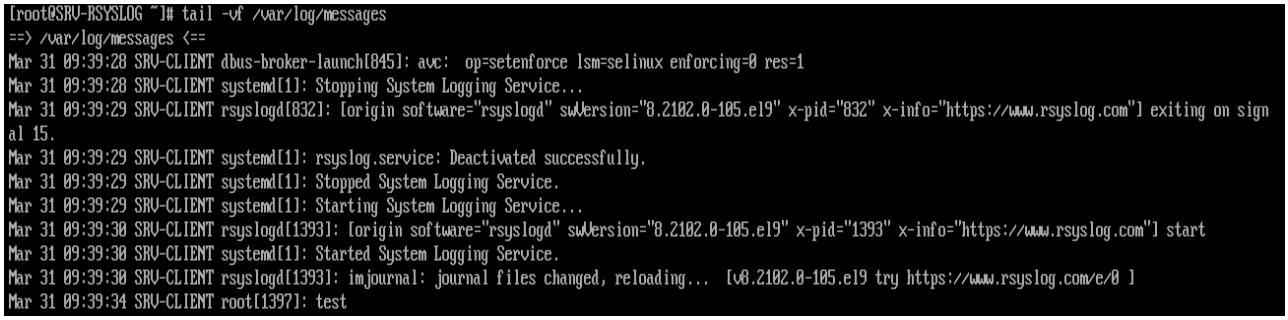
```
# # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
*.* @192.168.213.156:514
```

Démarrage service rsyslog et activation au démarrage

```
[root@SRV-CLIENT ~]# systemctl start rsyslog
[root@SRV-CLIENT ~]# systemctl enable rsyslog
[root@SRV-CLIENT ~]#
```

Nous allons faire le teste de communication :

```
[root@SRV-CLIENT ~]# logger "test"
[root@SRV-CLIENT ~]#
```



On peut voir que tout fonctionne et communique !

Mission 3

Ticket : 45768

De : S.houllier@syn.fr

A : Support@nexylan.fr

Objet : Problème configuration

Bonjour le support,

Suite à la mise en place des logs, je comprends rien, l'ensemble des logs de mes serveurs sont dans le même fichier, cela est inexploitable , merci de m'expliquer le problème et de corriger rapidement

S. HoullierDirecteur de la sécurité SYN

Vous pouvez utiliser l'annexe 4 à votre disposition pour vous aider dans la mise en place du serveur

Tout d'abord nous allons faire le test.

Taper dans le serveur rsyslog la commande suivant :

Nano /etc/rsyslog.conf

Puis rajouter ceci :

Remote Logs Template

$template Incoming-logs,"/var/log/remote-logs/%HOSTNAME%/%HOSTNAME%.log"

. ?Incoming-logs

Enregistrez et ensuite fait un logger sur la machine cliente avec le message que vous voulez et pour finir taper la commande ls et le serveur client apparaîtra séparément du serveur rsyslog.

Mission 4 :

De : S.houllier@syn.fr

A : Support@nexylan.fr

Objet : Et MES SERVEURS WINDOWS ?

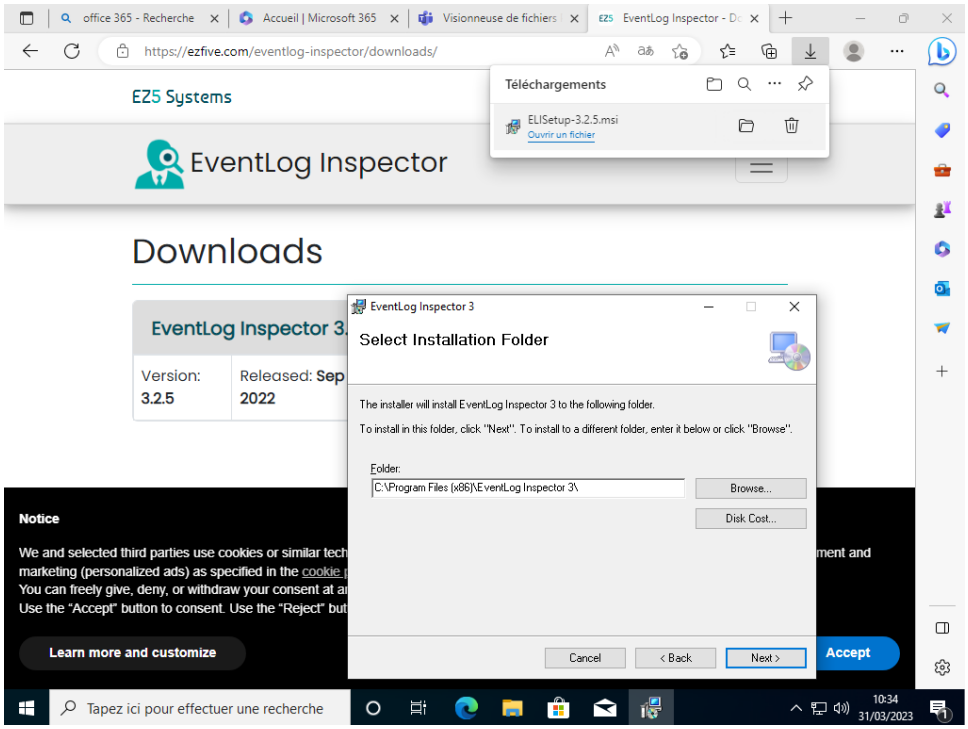
Bonjour le support Nexylan,

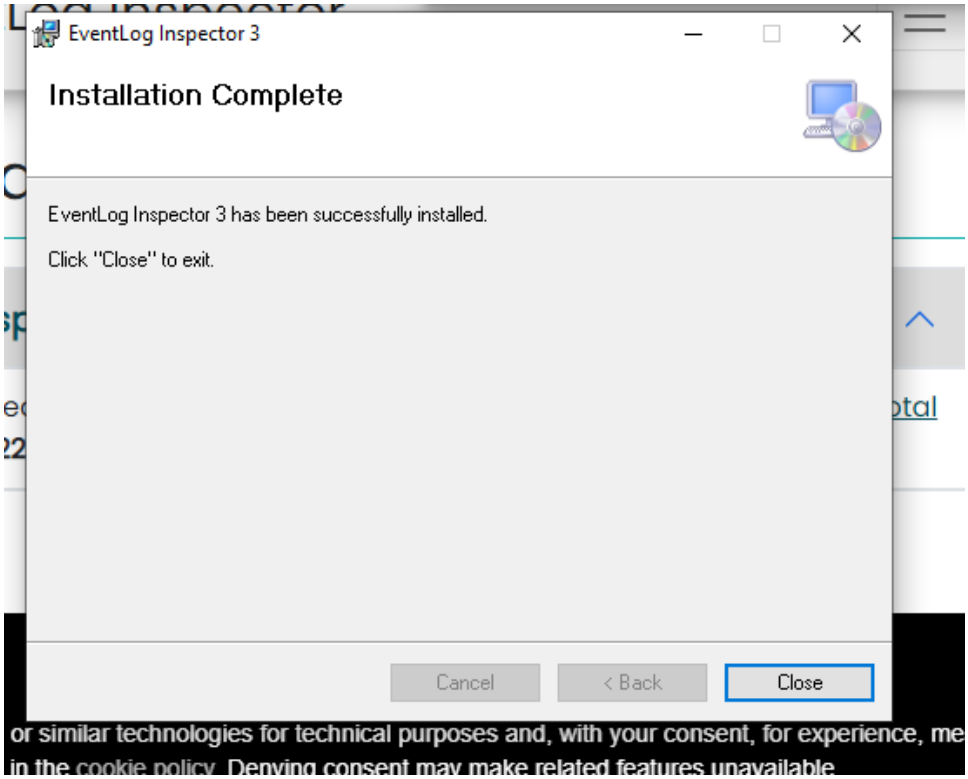
C'est bien beau d'avoir configuré le rsyslog sur mes serveurs Linux, mais cela est-il compatible sous Windows ? Car je vous rappelle que nous avons des machines sous Windows et il est nécessaire decentraliser également les logs.S. HoullierDirecteur de la sécurité SYN

Vous pouvez utiliser l'annexe 5 à votre disposition pour vous aider dans la mise en place du serveur

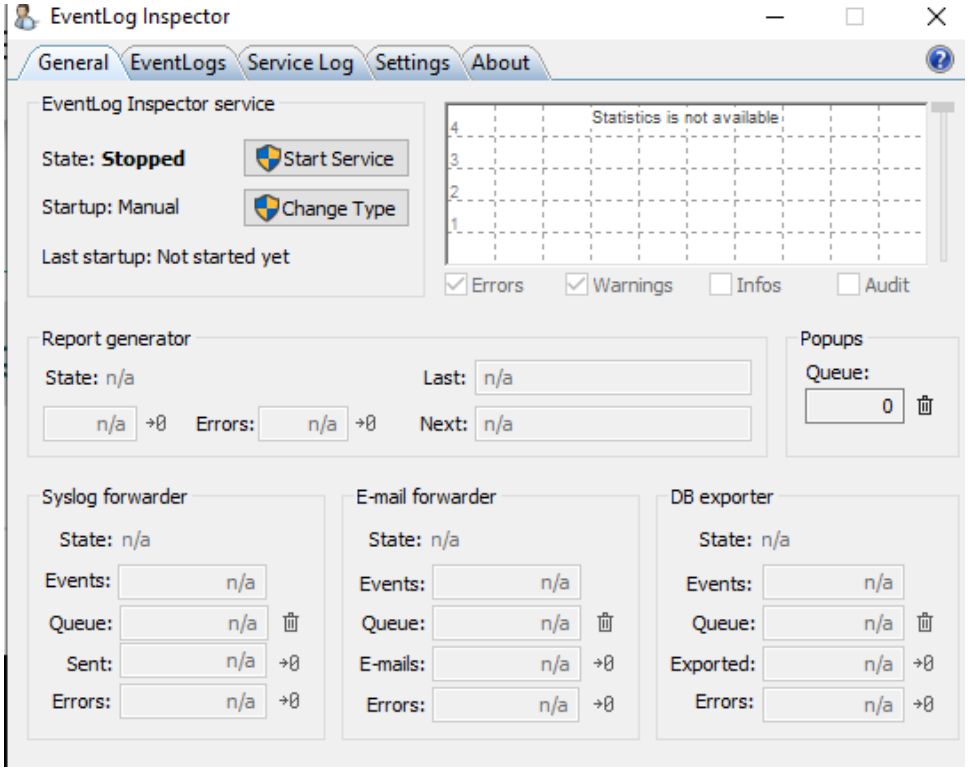
J'ai créé une machine Windows 10 de base pour pouvoir faire une installation et une configuration rsyslog client sous windows

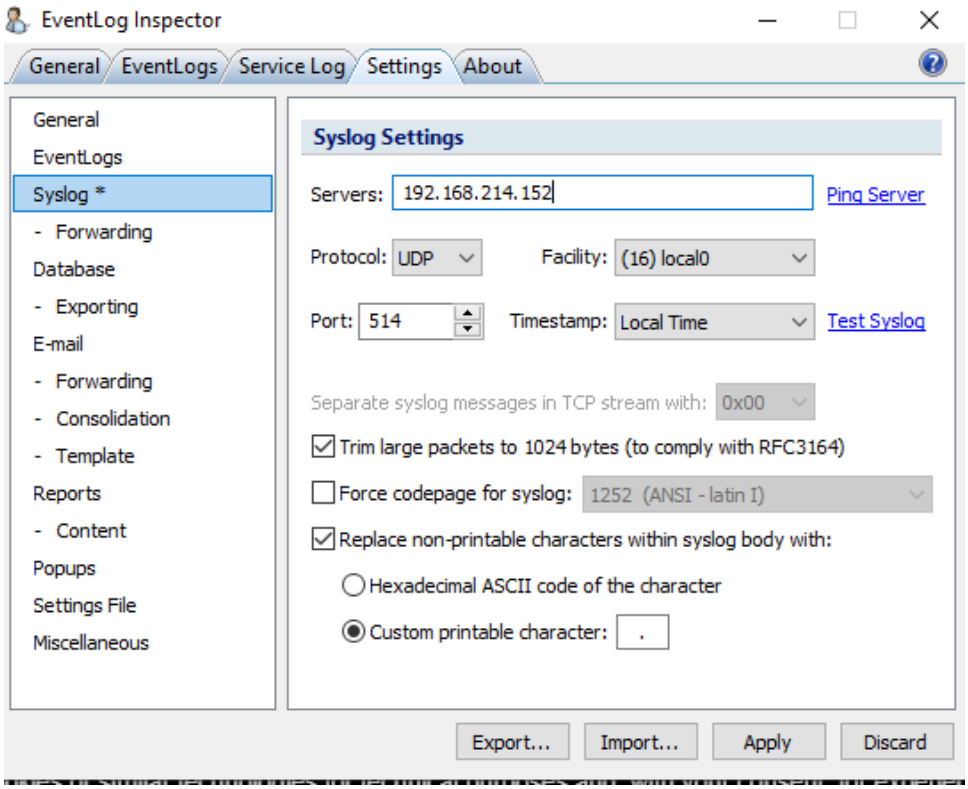
J'ai installé le client rsyslog via le lien suivant : https://ezfive.com/eventlog-inspector/downloads/



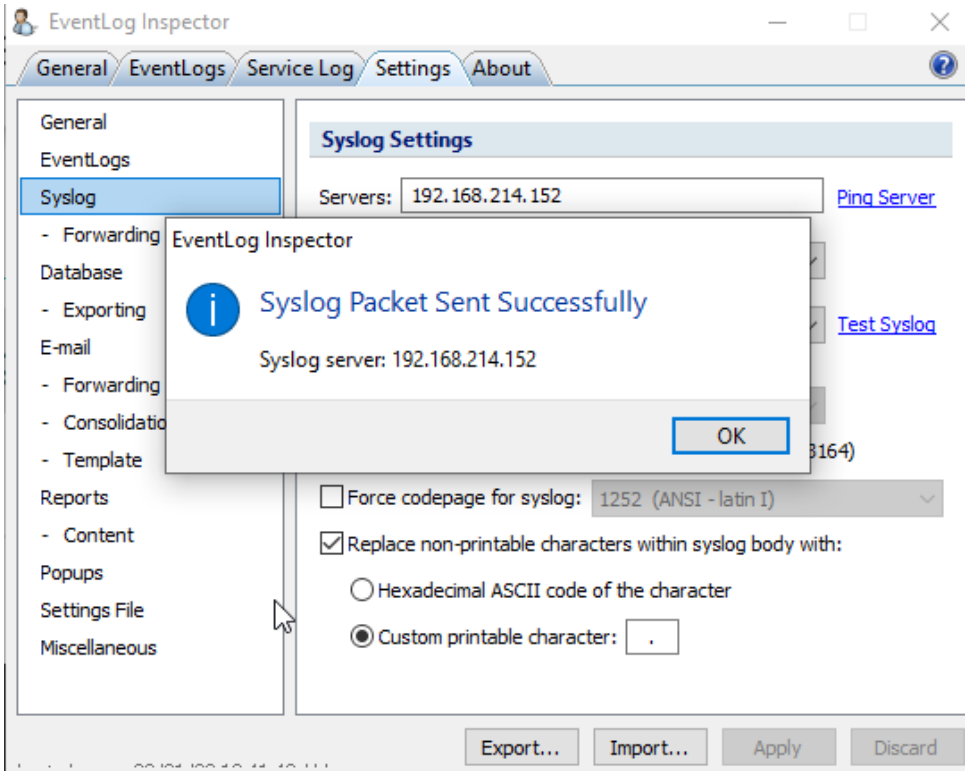


Après l'installation nous devons configurer le client pour envoyer les logs sur le serveur RSYSLOG



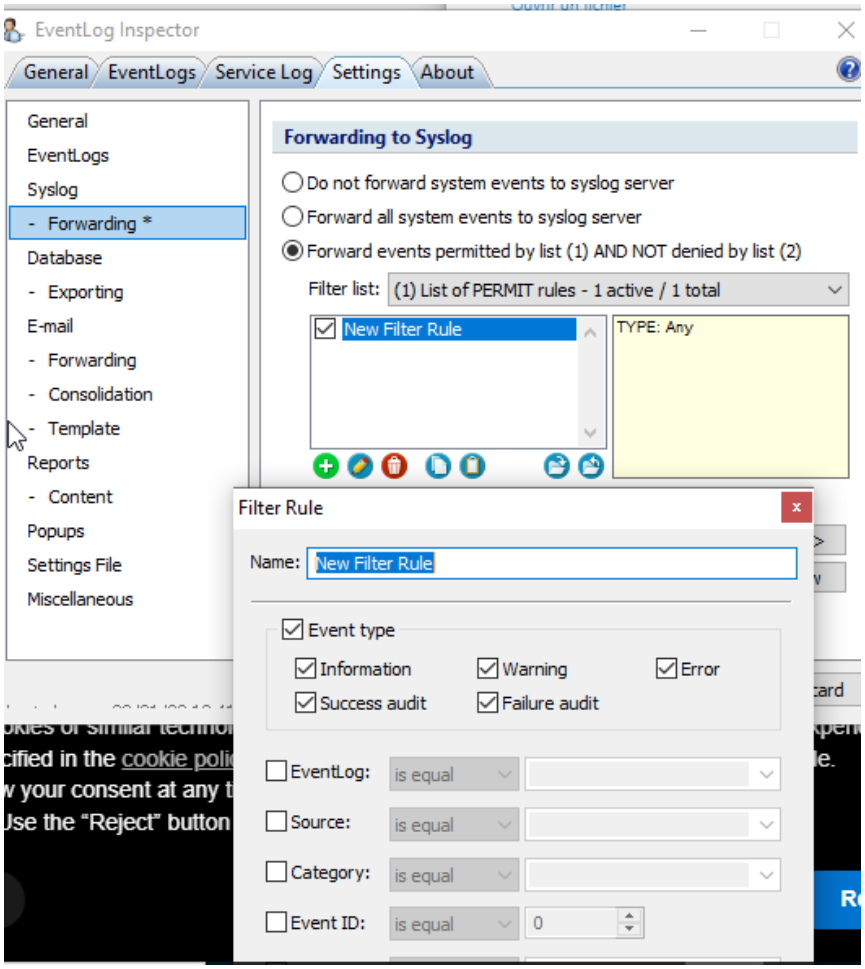


J'ai fait le teste pour voir si ça fonctionne.



Et ça communique !

Là je configure une redirection.



Maintenant la mise en place du serveur rsyslog sous windows est terminé.

Mission 5 :

De : S.houllier@syn.fr

A : Support@nexylan.fr

Objet : ALERT ESPACE DISQUE 95 %

Bonjour le support Nexylan,

Après avoir configuré la centralisation des logs, cela consomme un espace très important noussommes proche de la saturation du serveur et donc de l'arrêt du serveur....Merci de mettre en place un système automatique permettant de purger les logs régulièrement maiségalement de les compresser...

S. HoullierDirecteur de la sécurité SYN

Vous pouvez utiliser l’annexe 6 à votre disposition pour vous aider dans la mise en place du serveur

Nous allons faire une rotation des logs.

Pour cela,