

# Installer un serveur Syslog

## Installer un serveur de stockage Syslog Esia

### Pré-requis

L'installation du serveur Syslog Esia se fait sur une VM/serveur indépendant de votre Esia Mercury.

Au MINIMUM (dépendants de la quantité de log à traité), un serveur ou une VM avec:

- 4 cœurs (64 bits)
- 4 Go de RAM
- 100 Go d'espace disque
  - 20 Go pour la racine '/'
  - 5 Go pour le '/tmp'
  - 5 Go de swap
  - 70 Go pour '/var' à adapter à votre besoin.
- **Debian 11 Bullseye 64 bits (amd64)** [Téléchargeable ici](#)

### Ajout du repot esia

Afin de pouvoir installer le Galaxy sur votre serveur, il faut ajouter notre repository à la liste des repositories de confiance de votre serveur. Il suffit pour cela de saisir les commandes suivantes.

copy

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

### Installer & configurer les paquets

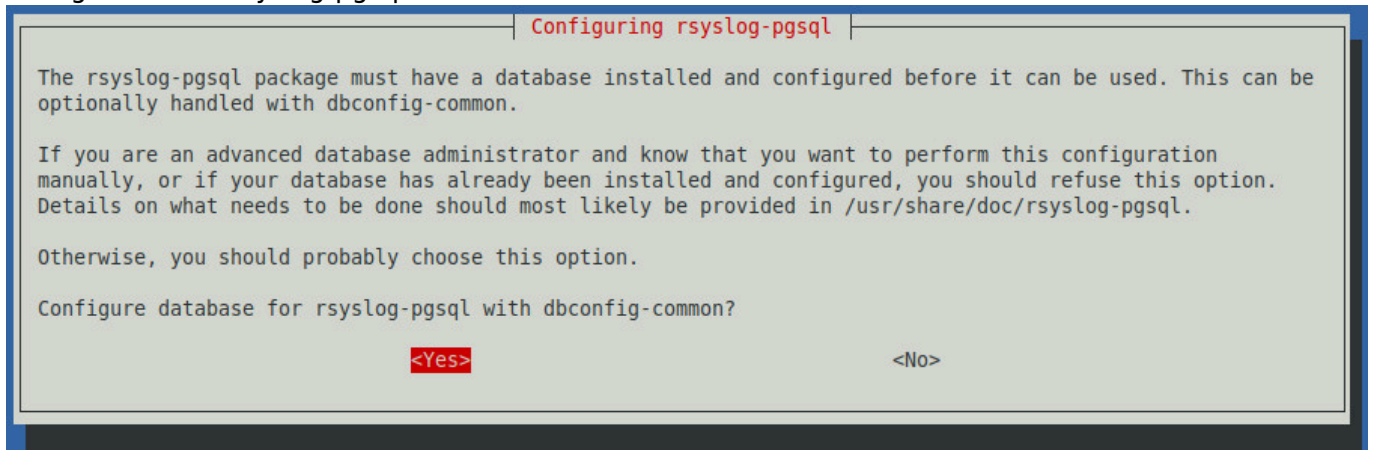
Saisissez les commandes suivantes :

copy

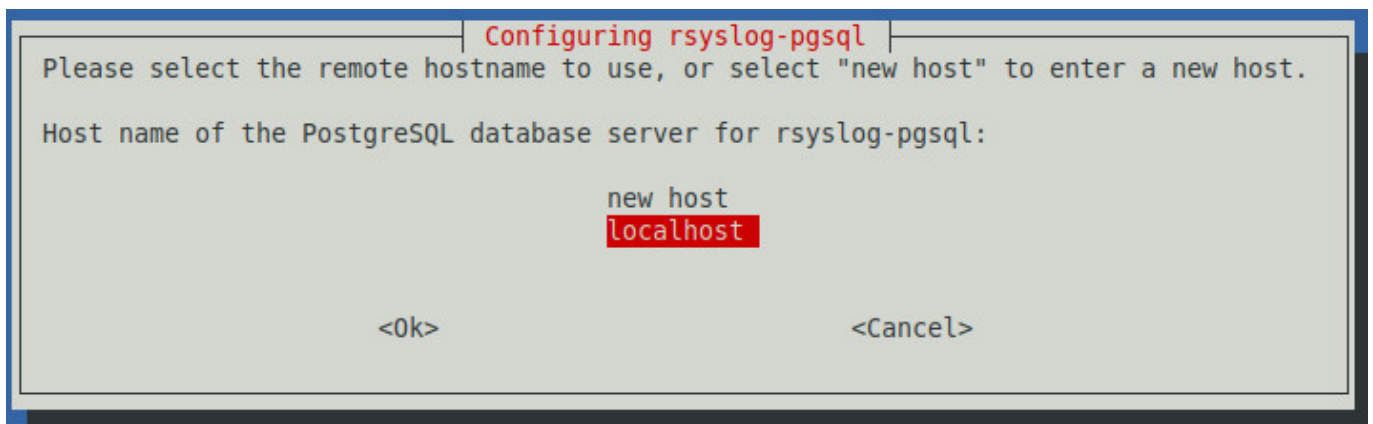
```
apt update
apt install -y postgresql
apt install -y esia-syslog-alarm
```

Une fois le téléchargement et le dépaquetage terminé, le système d'installation vous affichera la

### configuration de rsyslog-pgsql

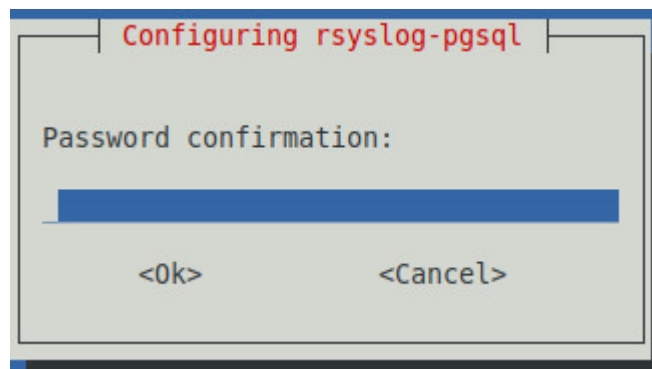
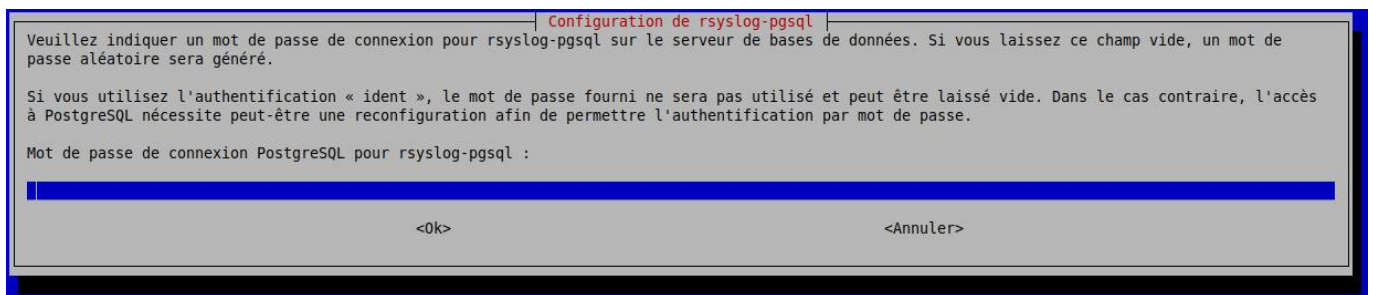


Sélectionnez "Yes", pour continuer la configuration.



Sélectionnez "localhost" pour indiquer que la base de données est local au serveur.

Entrez le mot de passe de la base de données



Confirmer avec le même mot de passe.

Le système va terminer de configurer les bases et logiciels autour.

Si vous souhaitez recevoir des alarmes asynchrones du serveur syslog. Il faut ajouter l'IP de votre Esia Mercury dans le fichier

copy

```
/etc/esia/syslog-alarm.conf
```

dans la partie "receiver". Il convient de vérifier que le port 2081 de votre serveur Esia est bien ouvert (iptables -L).

```
#####  
# Fichier de configuration d'ESIA      #  
# ESIA 3.0                             #  
# Biersart Nicolas                     #  
# support@esia-sa.com                  #  
#####  
[RECEIVER]  
    port=2081  
    key=2687b4e25ca52118ef03bfcdb31610a210b42202  
    #IP DE VOTRE SERVEUR ESIA  
    ip=10.12.0.145  
[CORE]  
    thread_number=10  
[DB]  
    #chaîne de connection postgresql  
    connection_number=4  
    PGSQL_host=localhost  
    PGSQL_port=5432  
    PGSQL_db=Syslog  
    PGSQL_username=rsyslog  
    PGSQL_pwd=syslog2022  
[LOG]  
    log_file=/var/log/esia/esiaSyslogAlarm.log
```

## Configurer Rsyslog

modifier le fichier de configuration de rsyslog pour autoriser les connexions entrantes:

copy

```
nano /etc/rsyslog.conf
```

Dé commenter les lignes suivantes

```
# provides UDP syslog reception  
module(load="imudp")  
input(type="imudp" port="514")
```

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

En dessous de cette configuration, ajouter les lignes suivantes, afin de sécuriser un minimum le serveur de log.

copy

```
$AllowedSender TCP, 127.0.0.1, <ip du réseau>/8
$AllowedSender UDP, 127.0.0.1, <ip du réseau>/8
```

redémarrer le service rsyslog

copy

```
/etc/init.d/rsyslog restart
```

## Configurer SNMP

SNMP est installé par défaut, il faut maintenant le configurer. Il faut aller éditer le fichier de configuration :

copy

```
nano /etc/snmp/snmpd.conf
```

Changez la ligne suivante (ou la mettre en commentaire) :

```
agentAddress udp:127.0.0.1:161
```

Et la remplacer par :

copy

```
agentAddress udp:0.0.0.0:161
```

Il faut ensuite configurer la communauté SNMP :

copy

```
rocommunity read_community default
```

ou rocommunity « nom de la communauté » « range ip (ip unique ) /masque de sous-réseaux »

copy

```
rocommunity read_community 10.7.0.14/32
```

**ATTENTION, ne pas laisser de rocommunity avec la vue par défaut systemonly (commentez, effacez ou modifiez la ligne suivante) :**

copy

```
# rocommunity public default -V systemonly
```

Ensuite il faut redémarrer le service SNMP en tapant :

copy

```
/etc/init.d/snmpd restart
```

Afin d'**éviter** que le l'agent n'ajoute une ligne toutes les X minutes dans votre fichier de log (à chaque interrogation par le serveur Esia), n'oubliez pas de rendre SNMP moins verbeux. Saisissez la commande suivante :

copy

```
systemctl edit snmpd
```

Cela va (entre autres) créer le fichier « /etc/systemd/system/snmpd.service.d/override.conf ». Ajoutez ce code dans le fichier :

copy

```
[Service]
ExecStart=
ExecStart=/usr/sbin/snmpd -LS4d -Lf /dev/null -u Debian-snmp -g
Debian-snmp -I -smux,mteTrigger,mteTriggerConf -f
```

Ensuite il faut redémarrer le service SNMP en tapant :

copy

```
service snmpd restart
```

Sur Debian Buster si la commande service n'existe pas vous pouvez redémarrer avec cette commande:

copy

```
systemctl restart snmpd
```

## Conclusion

Votre système est maintenant prêt à recevoir les log/journaux des autres nœuds réseau. Nous allons maintenant le lier au serveur Esia.

## Installer le système de liaison sur le Mercury

### Installer les paquets

Sur votre serveur Esia Mercury, installez les paquets suivants:

copy

```
apt install -y esia-receiver esia-webp-syslog
```

### Autoriser les connexions entrantes

Afin que le serveur Syslog puissent envoyer les alertes vers votre serveur Esia, il faut autoriser les connexions sur le port 2801. En tapant les lignes de commande suivantes:

copy

```
iptables -A INPUT -p tcp -m tcp --dport 2801 -s <ip serveur  
syslog>/32 -j ACCEPT  
iptables-save > /etc/iptables.rules
```

## Ajout dans l'interface web

Pour ajouter le serveur syslog dans votre Esia, allez dans l'administration d'Esia et ensuite sur « **Ajouter Nœud** ». Remplissez les champs en spécifiant bien le type de nœud comme « **Syslog Server** ». N'oubliez pas la communauté SNMP.

AJOUTER UN NOEUD

INFORMATIONS GÉNÉRALES

Nom du noeud: syslog-server

Type de noeud: Syslog Server

Groupe: syslog

Adresse IP: 10.12.0.16

Connecté derrière la Unity: none

Description:

INFORMATIONS SNMP

Version SNMP: SNMP v2c

Timeout SNMP (en ms): 1000

Communauté snmp vl-v2c: public

Ajouter

Cliquez sur « **Ajouter** » et ensuite le système de configuration vous demandera l'URL HTTP/HTTPS vers le syslog, par défaut il prend l'IP de votre nœud.

AJOUTER UN NOEUD

LIAISON AVEC LE SERVEUR

URL de connexion du serveur syslog: http://10.12.0.16

Retour Sauver

Cliquez sur « **Sauvez** », ESIA vous affichera le message suivant en principe.

AJOUTER UN NOEUD

Mise à jour reussie

LIAISON AVEC LE SERVEUR

URL de connexion du serveur syslog: http://10.12.0.16

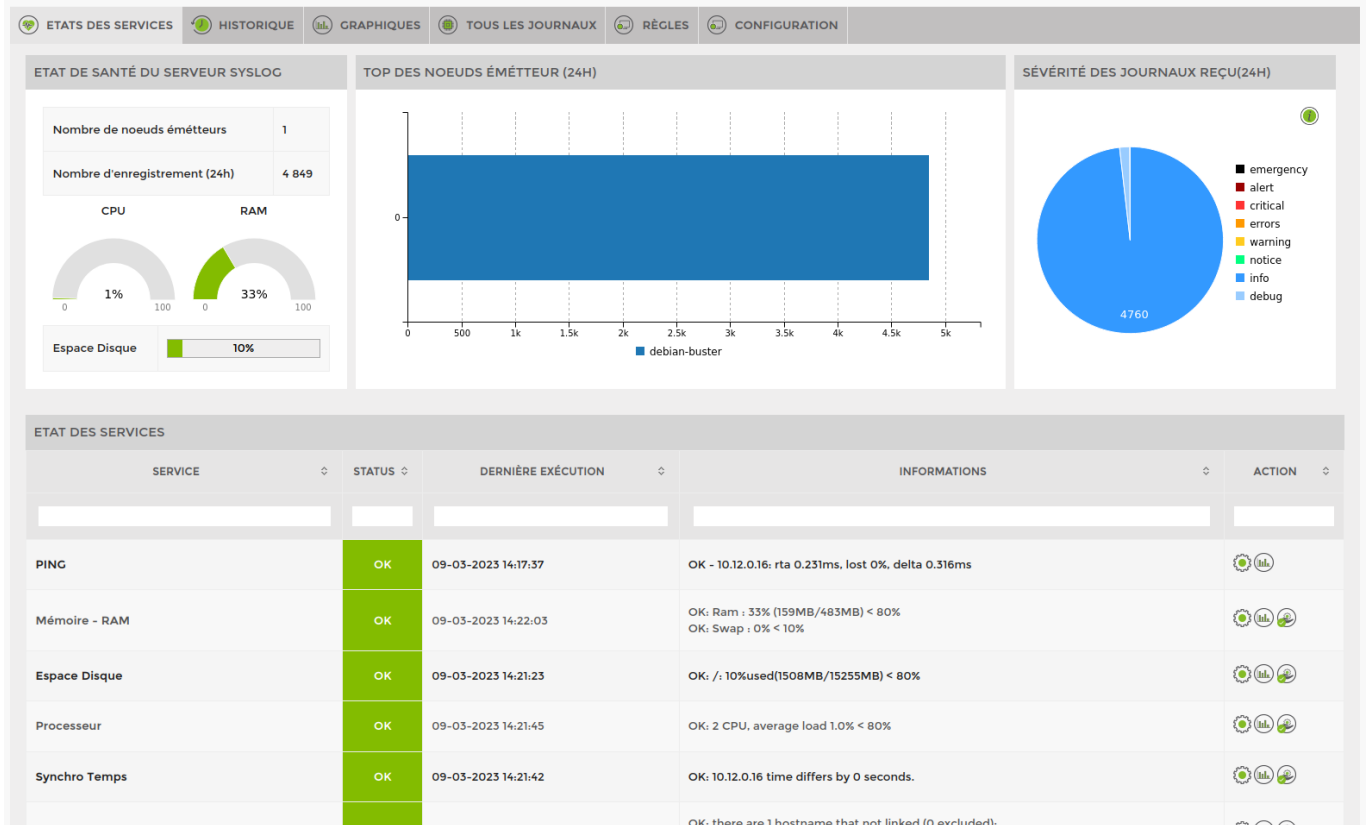
Retour Sauver

Le pattern par défaut « **default\_snmp\_linux\_server** » est appliqué ainsi que 2 services :

- CHECK\_SYSLOG\_AUTO\_LINK
- MAN\_SYSLOG\_AUTO\_LINK

Le premier vérifie que les nom d'hôtes (hostname) reçu par le serveur syslog correspondent au nœud dans ESIA. Le plugin 'MAN' lie les deux ensemble automatiquement.

Votre serveur est maintenant ajouté dans ESIA et vous pouvez aller sur la page de contrôle des nœuds afin de voir votre serveur de journaux (logs).



From: <https://wiki.esia-sa.com/> - **Esia Wiki**

Permanent link: [https://wiki.esia-sa.com/interface/module\\_syslog](https://wiki.esia-sa.com/interface/module_syslog)

Last update: **2023/12/13 15:24**

