

Rsyslog et Winsyslog

Rsyslog et Winsyslog sont deux agents quasiment identiques(GUI similaire). Ils sont commercialisés par la même entreprise. Il y a quelques différences selon la licence. Vous pouvez voir la comparaison [ici](#) et [ici](#).

Rsyslog et Winsyslog se configurent de la même façon.

note : Rsyslog et Winsyslog sont propriétaires et sous licence.

Installation

Fichier **.exe** à exécuter que vous pouvez télécharger [ici](#) (rsyslog) et/ou [ici](#) (winsyslog).

Créer une règle

Dans un premier temps il faut créer une règle. Une règle par défaut est déjà présente. Vous pouvez la supprimer.

Pour ajouter une règle cliquez droit sur **RuleSets > Add RuleSet**

Nommez votre règle et cochez uniquement « **Add a single Rule including these Actions.** » et « **Syslog Forwarding** »

Add RuleSet

Adding a new RuleSet ...

Enter the Name of the new RuleSet

ForwardSyslog

For example MyRuleSet or RuleSet 1

After the RuleSet has been added...

☐ Do not add a Rule yet.

☒ Add a single Rule including these Actions.

☐ Add a Rule for each of these Actions.

1

Storing Actions

Forwarding Actions

☐ Send RELP

☒ Syslog Forwarding

2

Internal Actions

☐ Call RuleSet

☐ Compute Status Variable

☐ Discard

☐ Normalize Event

☐ Set Property

☐ Set Status

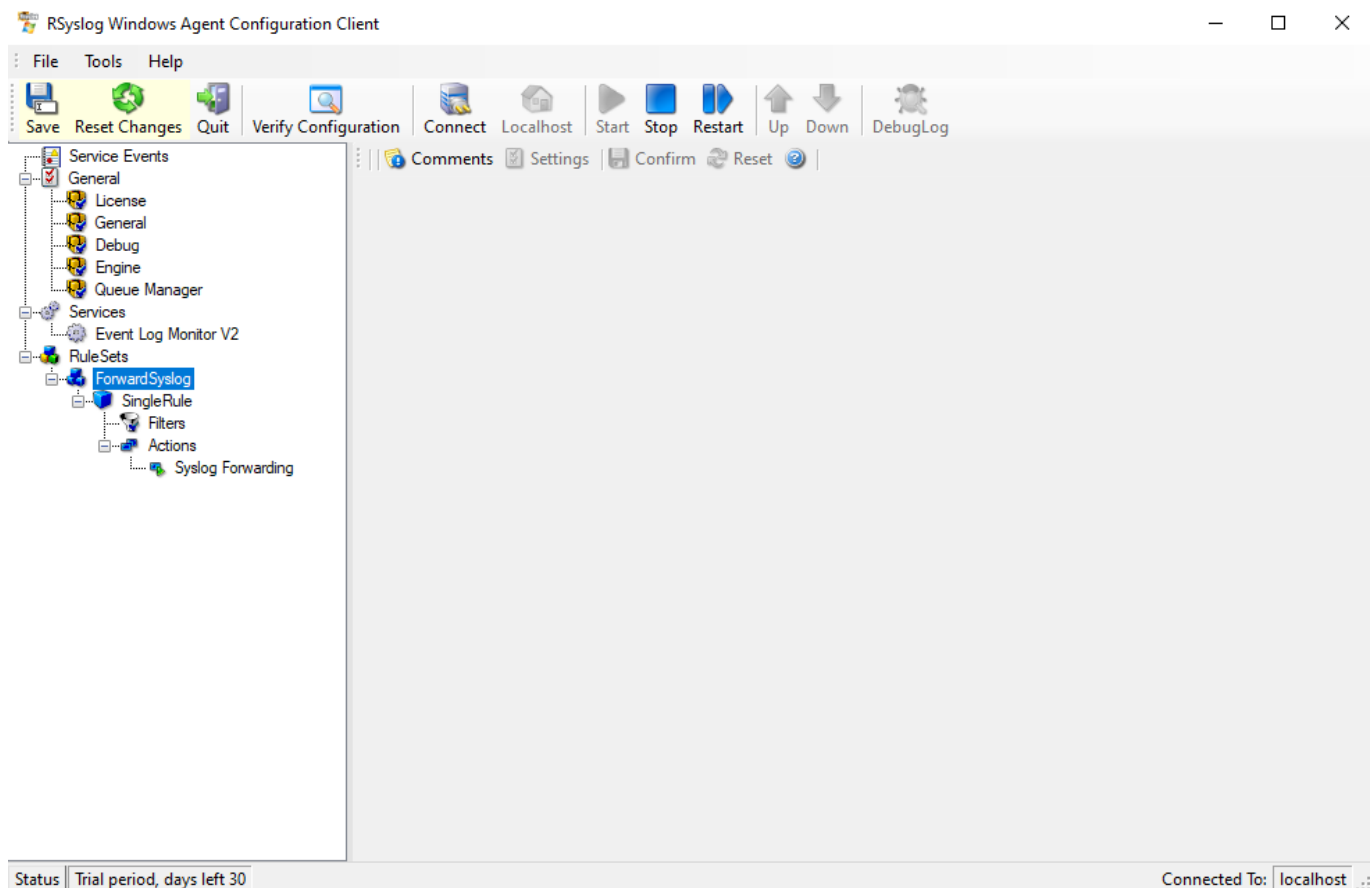
Other Actions

OK

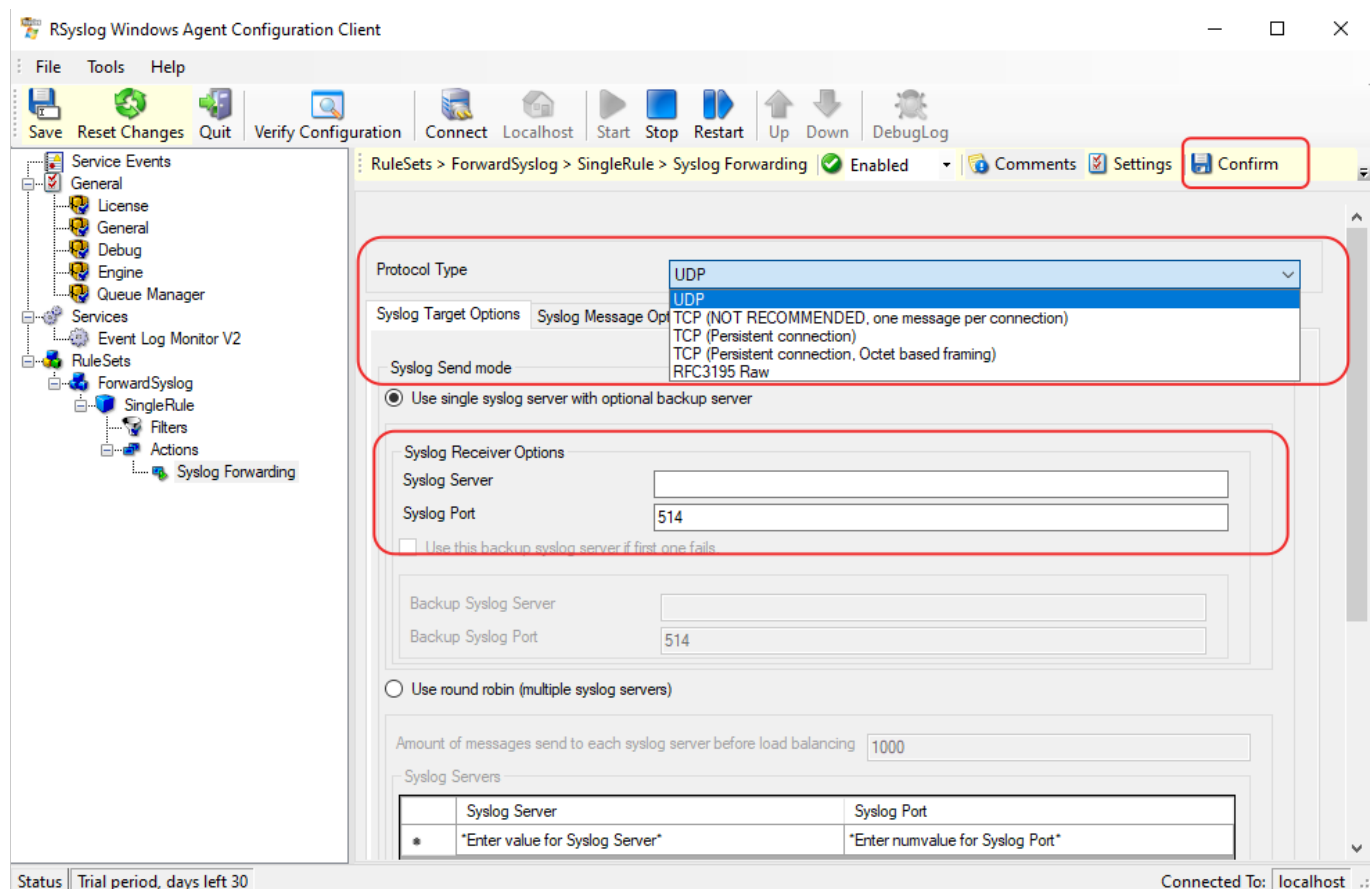
Cancel

note: cette règle forward simplement les logs sans filtre particulier

La règle apparaît dans le menu latéral gauche.



Développez l'arborescence jusqu'à l'action de la règle et cliquez sur celle-ci.

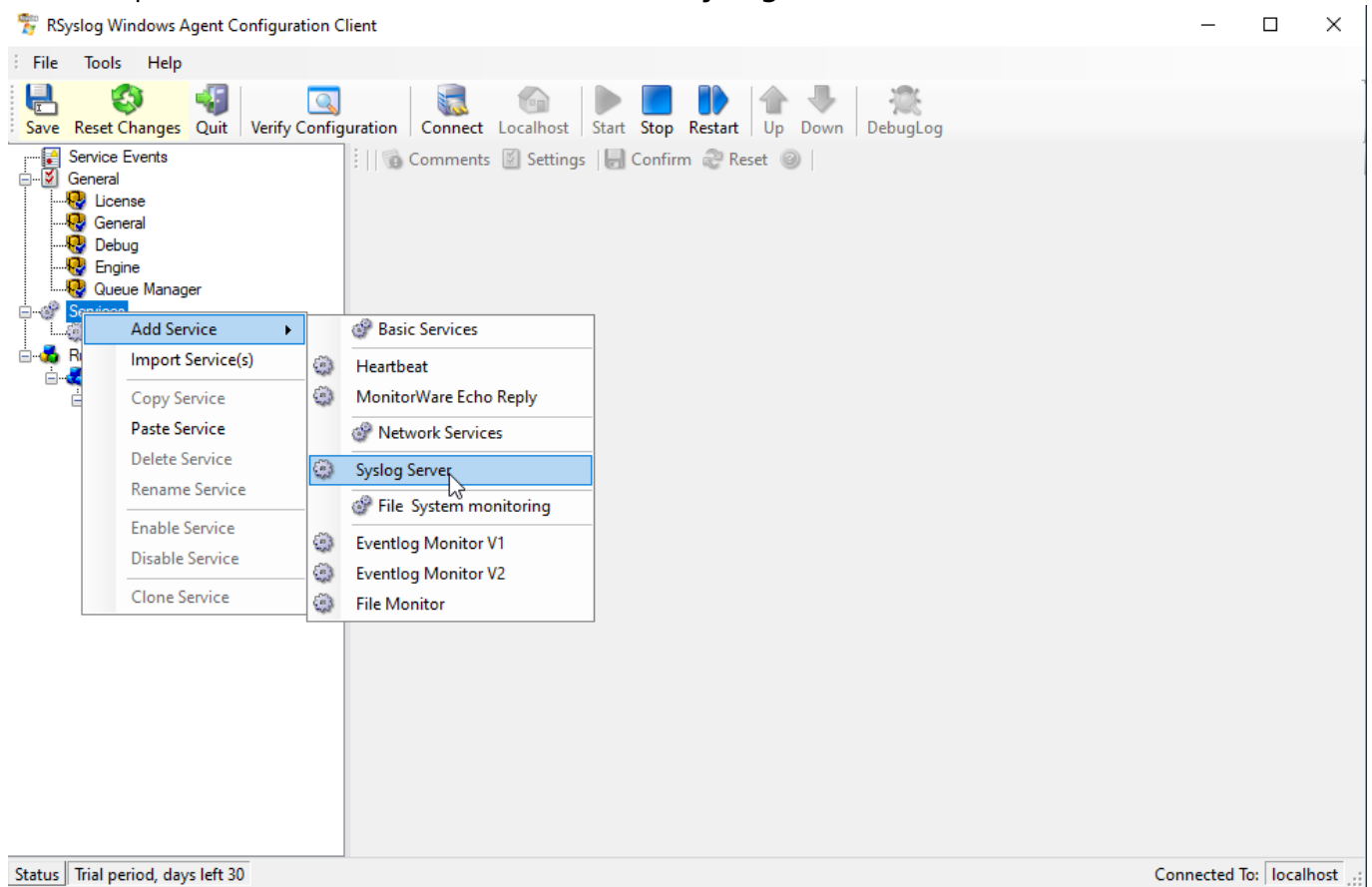


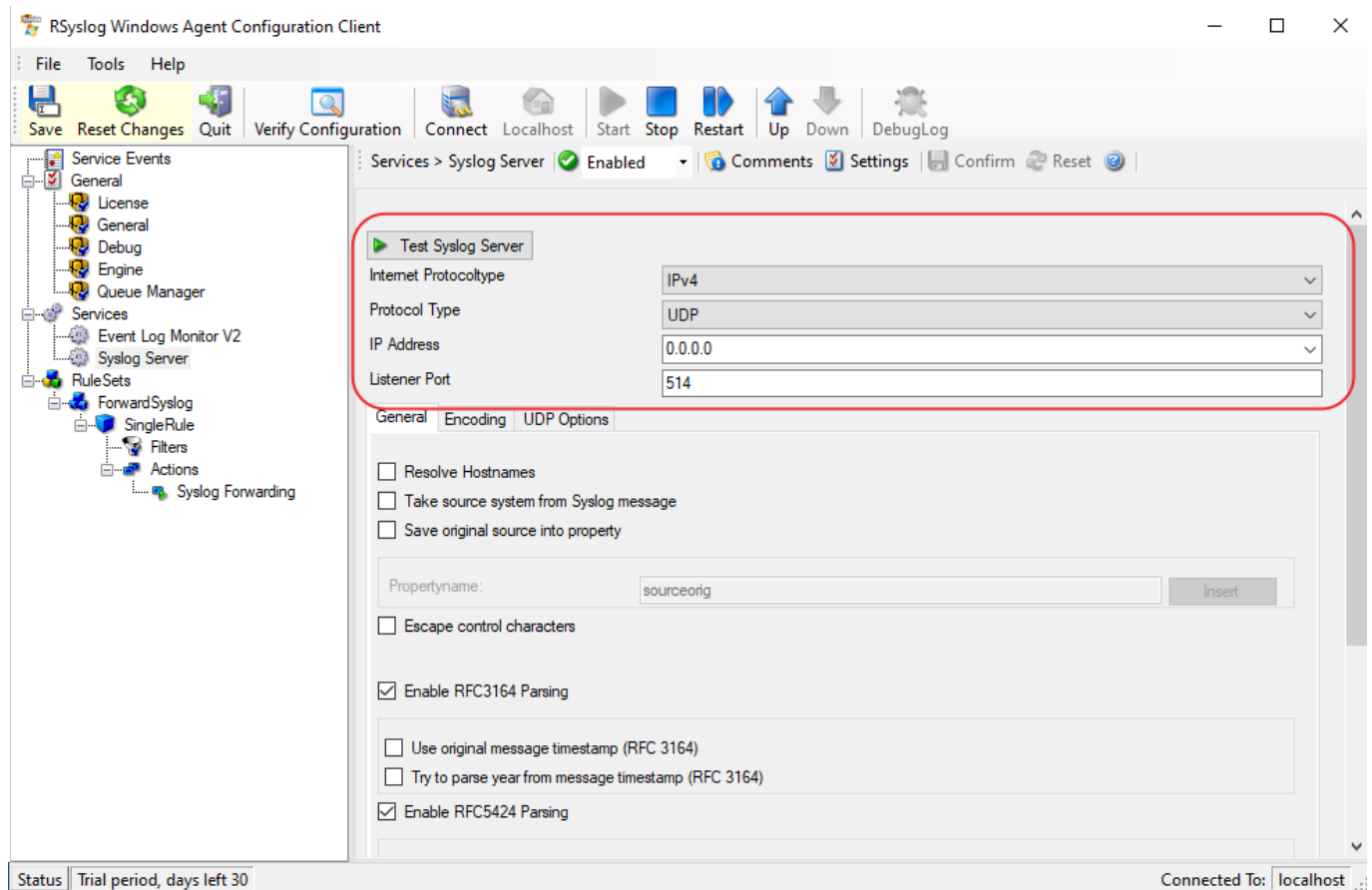
Choisissez **UDP** Ou **TCP** selon votre préférence, entrez l'**adresse IP** du serveur Syslog et le port.

Pour terminer cliquez sur « **Confirm** » dans le coin supérieur droite.

Définir un serveur Syslog

Faites clique droit sur **Services** > **Add Service** > **Syslog Server**

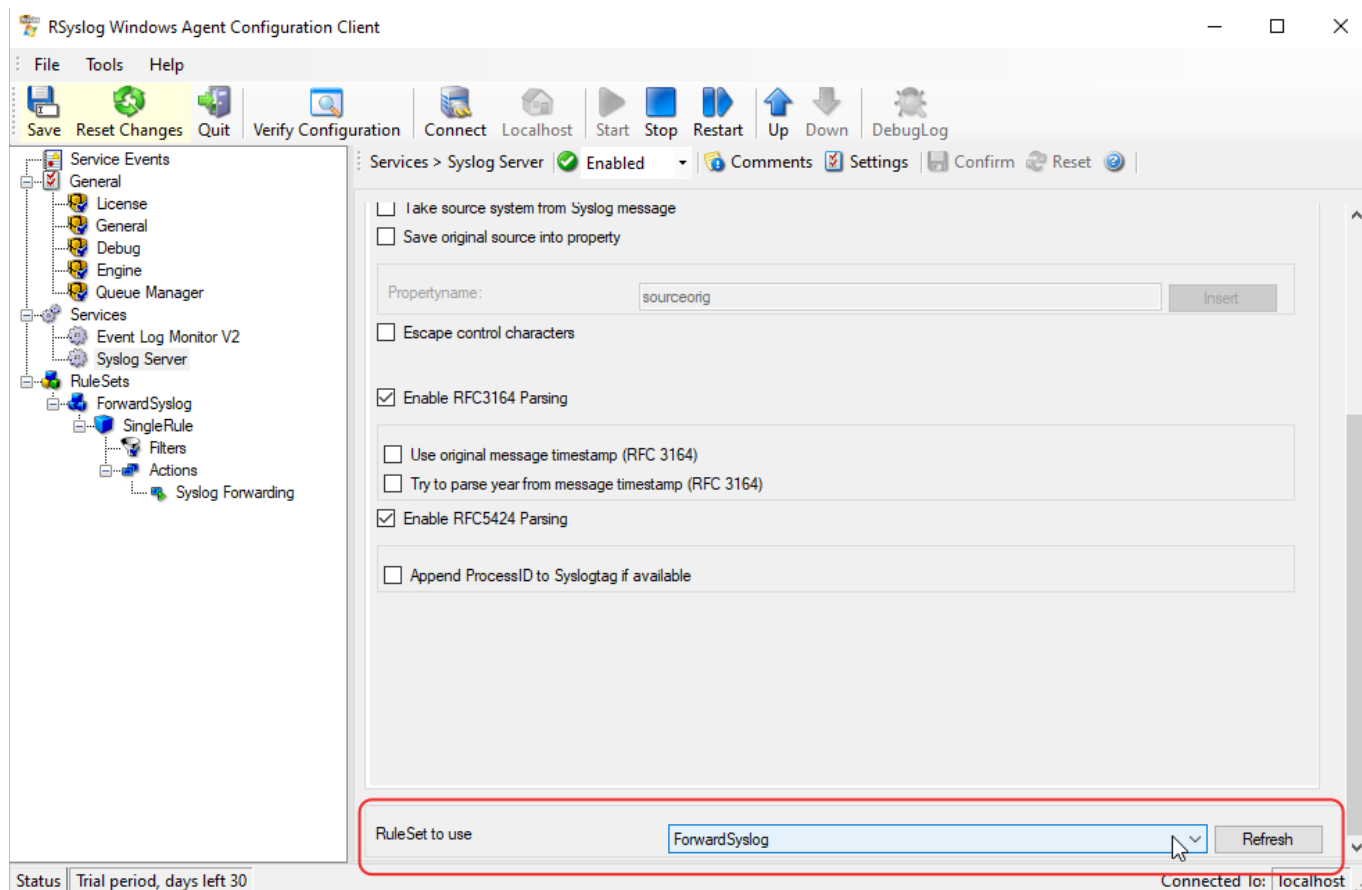




Configurez le serveur à joindre en entrant :

- IPv4 ou IPv6
- Protocole
- Adresse IP
- Porte d'écoute

Ensuite tout en bas sélectionnez la règle qui vous avez créé au préalable.



Configurer l'agent Syslog

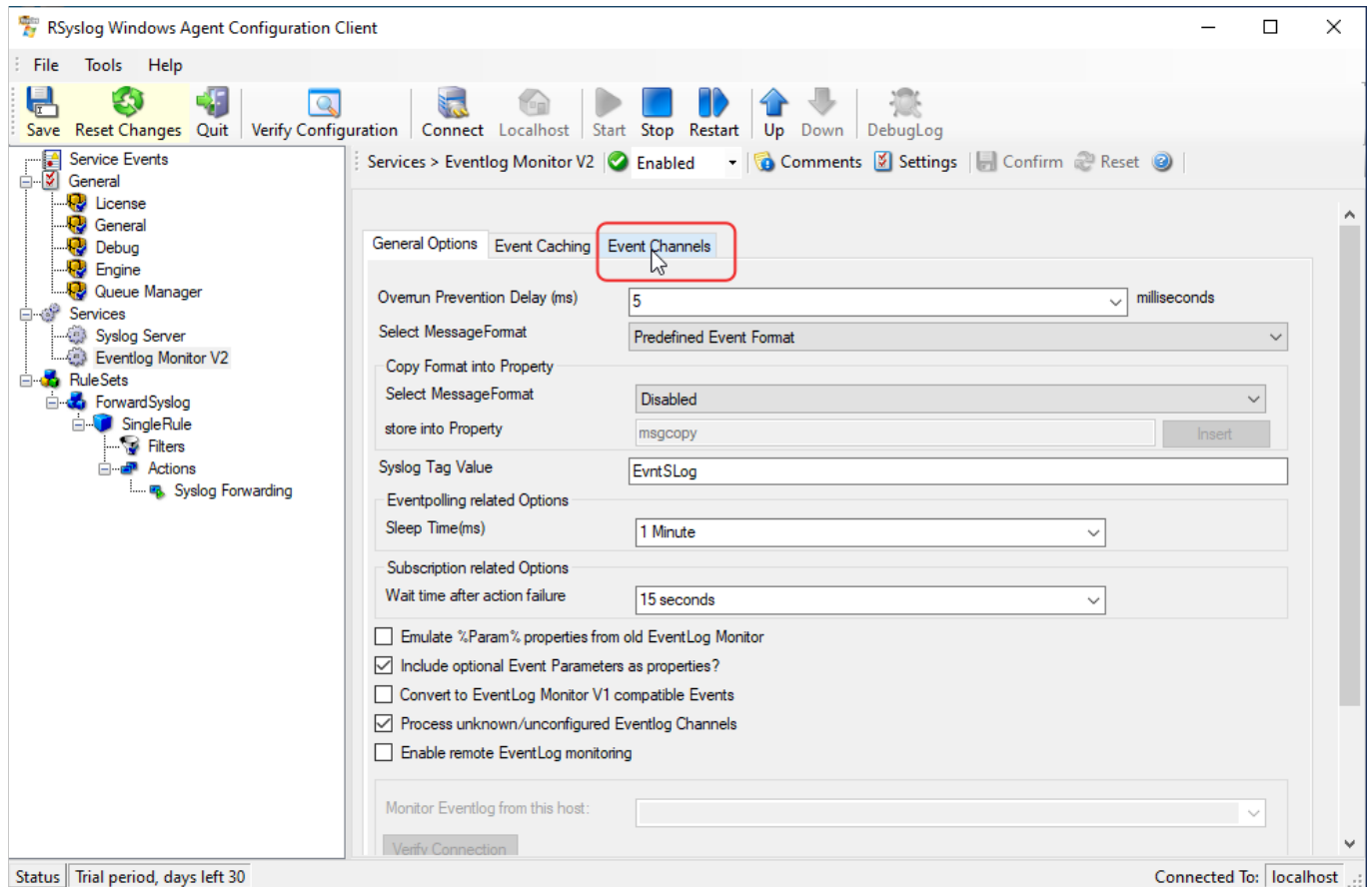
Faites cliquer droit sur **Services > Add Service > Moniteur EventLog V1 ou V2**

Selon la version de l'OS :

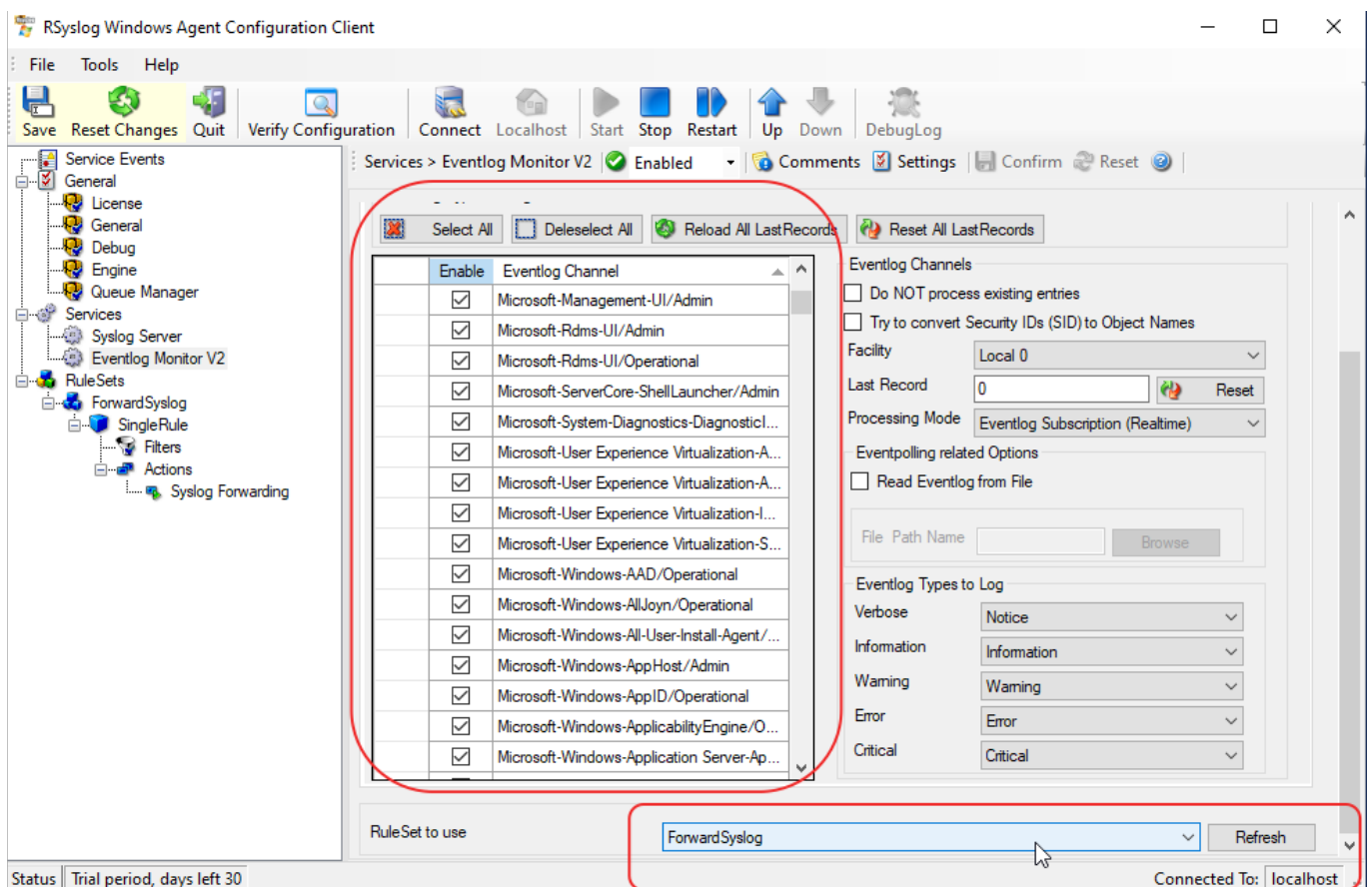
- Moniteur EventLog V1 : 2000, XP, 2003
- Moniteur EventLog V2 : Vista, 2008, 7, 10

note : pour les versions serveurs se référer au noyau (ex : microsoft server 2019 = windows 10)
Services > Add Service > Eventlog Monitor V1/2

Cliquez sur l'onglet « **Event Channels** »

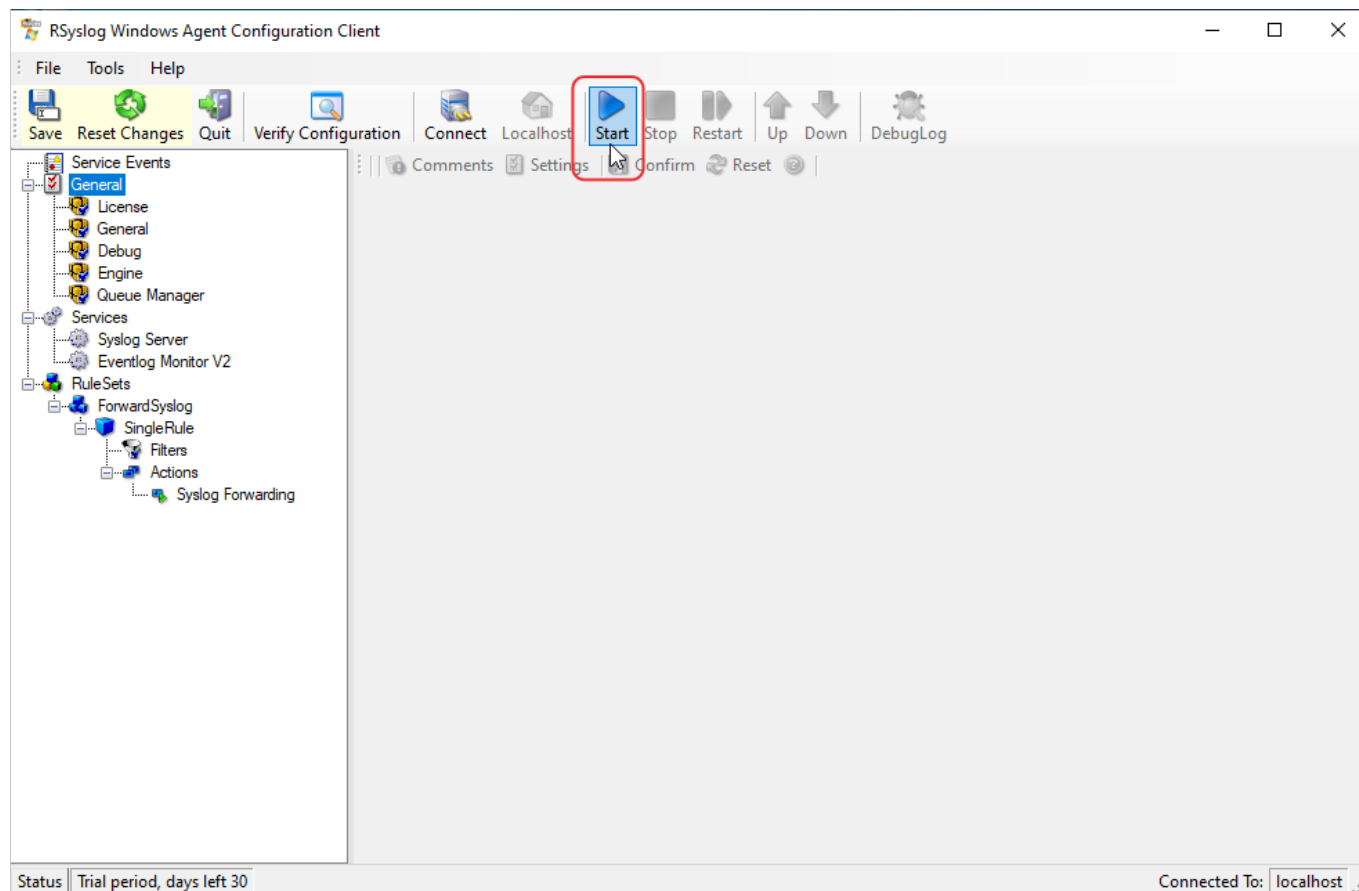


À partir de là vous pouvez sélectionner les eventslog à forward. N'oubliez pas de sélectionner la bonne règle au bas de la fenêtre. (si il y en a plusieurs) et d'enregistrer avant de quitter.



Démarrer le service

Cliquer sur start pour démarrer le service. Après la configuration et le démarrage du service vous pouvez fermer le programme.



From:

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

Permanent link:

https://wiki.esia-sa.com/syslog/syslog_rsyslog_winsyslog

Last update: **2023/03/09 14:50**

