

Installez un serveur de Syslog pour saisir des logs de la gamme D98xx IRDs

Contenu

[Introduction](#)

[Informations générales](#)

[Configurez le serveur de Syslog](#)

[Configurez l'IRD \(D9854/D9858/D9859\) pour envoyer des logs au watcher de Syslog](#)

[Exporter les messages enregistrés à un fichier CSV](#)

[Supprimer de vieux messages](#)

Introduction

Ce document décrit comment installer un serveur de Syslog pour saisir des logs des récepteurs/des décodeurs intégrés par gamme D98xx (IRDs).

Informations générales

Version de logiciel 4.0 de D9854, D9858 et D9824, et toute version D9859 des messages conformes de **Syslog** du support RFC-3164. Les clients peuvent maintenant capturer les messages avec un serveur de Syslog pour la mémoire et la récupération. En outre, cette procédure peut également être utilisée avec le nouveau récepteur de transport du réseau D9800.

Le **watcher de Syslog** est le **serveur** libre pris en charge de **Syslog** pour des ordinateurs Windows. Pour des machines Linux, le **serveur** pris en charge de **Syslog** est le Syslog-NG qui est fourni par le HTTP : [/www.balabit.com/network-security/syslog-ng/opensource-logging-system](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system)

Cet article traite seulement l'établissement sur des ordinateurs Windows.

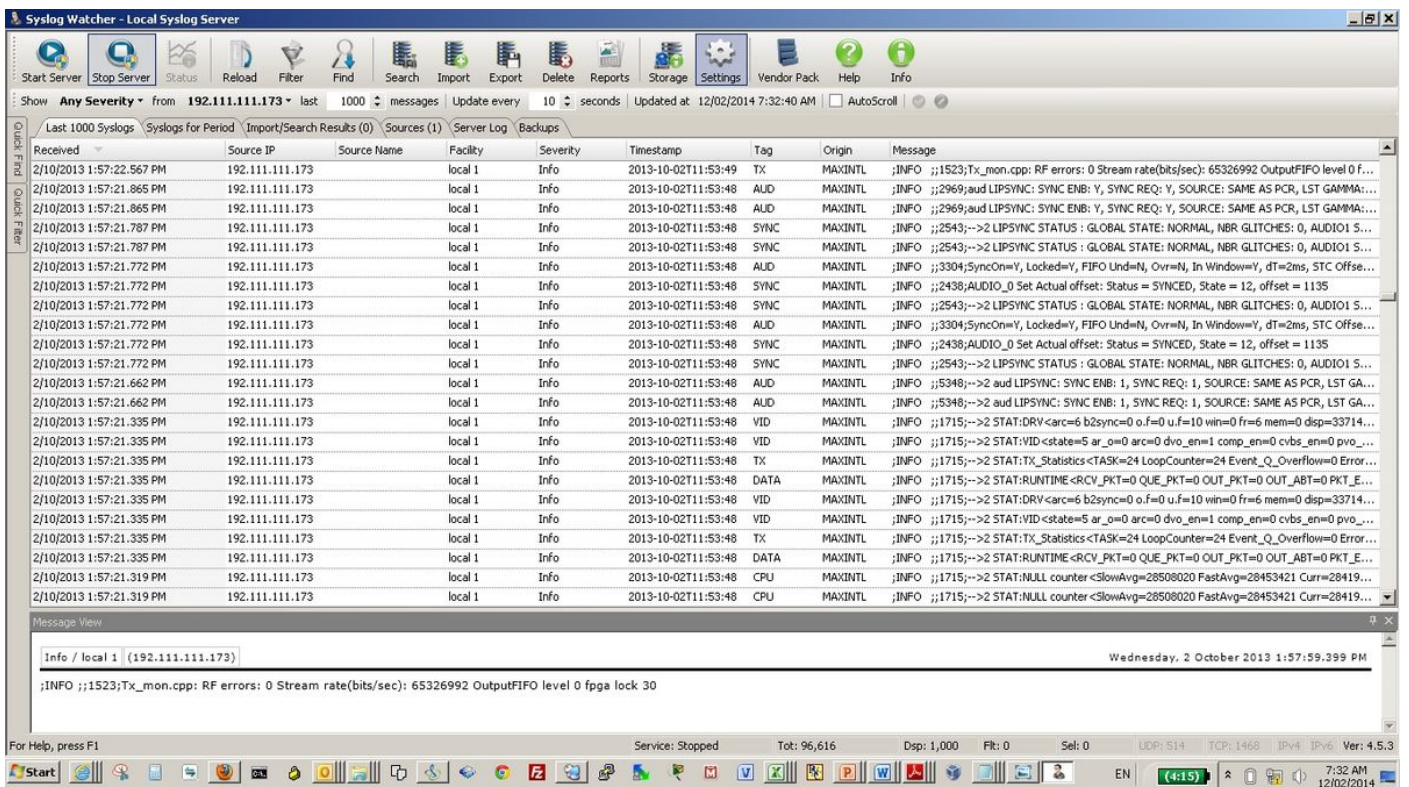
Configurez le serveur de Syslog

Téléchargez le **watcher de Syslog** de

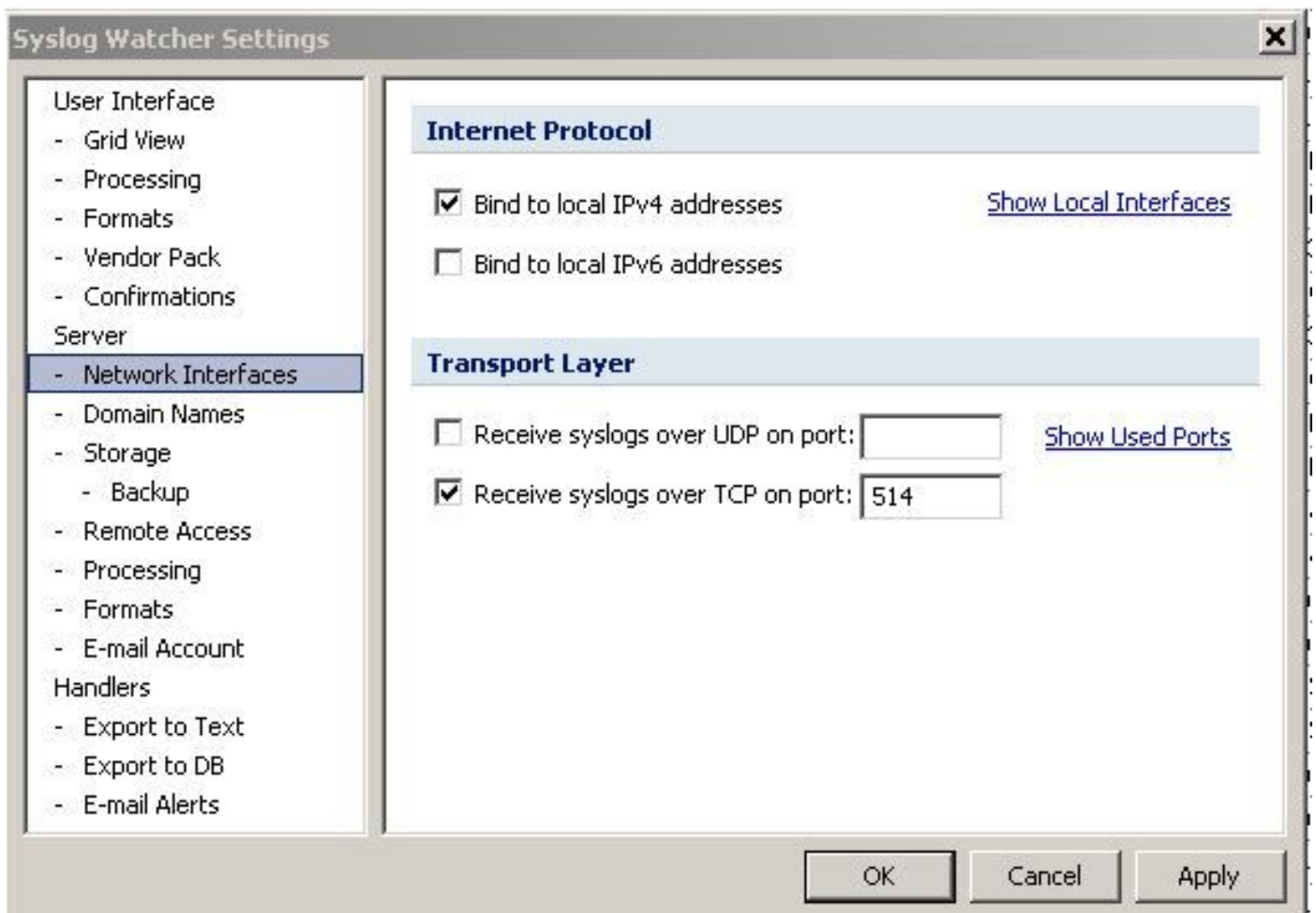
HTTP : [/www.snmpsoft.com/syslogwatcher/syslog-server.html](http://www.snmpsoft.com/syslogwatcher/syslog-server.html)

et installez-le dans votre ordinateur de fenêtres.

Commencez le watcher de Syslog et sélectionnez le mode de fonctionnement pour le GUI comme **gèrent serveur local de Syslog**, l'image affichée apparaît :

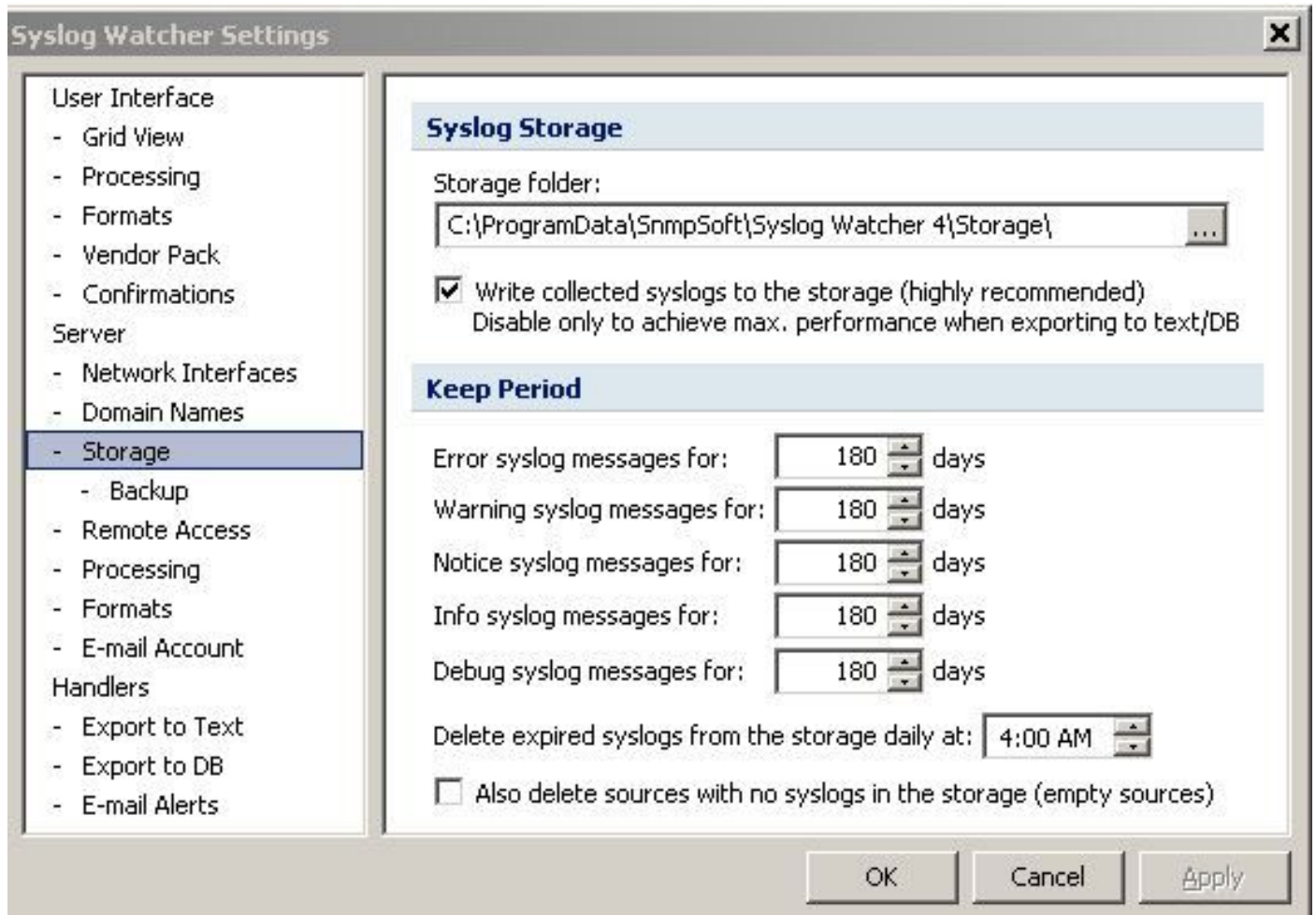


Cliquez sur dans les configurations (mises en valeur dans l'image ci-dessus) dans la barre d'outil, l'image affichée apparaît :



Interfaces réseau choisies. Cochez la case reçoivent des Syslog au-dessus d'UDP sur le port et introduisent un numéro de port. Le même numéro de port doit être configuré sur les périphériques d'où le watcher de Syslog doit recevoir des logs.

Mémoire maintenant choisie sous des **configurations de watcher de Syslog**, suivant les indications de l'image :



Spécifiez un emplacement de répertoire pour enregistrer les messages, cochez les Syslog collectés **Write de case** à la mémoire.

Spécifiez le nombre de jours pour chaque type de message à maintenir dans la mémoire.

Configurez l'IRD (D9854/D9858/D9859) pour envoyer des logs au watcher de Syslog

Sur le GUI IRD, sélectionnez les **paramètres IP de configurations de système de la barre d'outil**. L'image affichée apparaît :

D9854 - Advanced Program Receiver Admin(admin) | About | Log Out

Summary | Input | Audio & Video | Transport Stream | **System Settings** | Support

System

- Features/Licenses
- IP Settings**
 - IP Unicast Routing
 - MPE
 - SNMP
- Alarms
- Versions
- Settings File
- Security/Accounts

IP Settings

| Port ID | Destination IP Address | Mask | Gateway Address | PHY Mode |
|---------|------------------------|------|-----------------|----------|
| control | 192.111.111.172 | 24 | 192.111.111.1 | Auto |
| data | 192.131.244.7 | 24 | 192.131.244.254 | Auto |

Protocol Control

Telnet: SNMP:

SSH:

HTTP: Idle Timeout (seconds):

Syslog: Syslog Server IP Address: Syslog Server Port:

Redundancy Control

Mode: Direction: Delay Forward (ms): Delay Back (seconds):

Redundancy Status

| Ports In Use | Change Reason | Change Date & Time |
|--------------|---------------|---------------------|
| None | Setup+Link | 2007/02/09 10:00:01 |

Dans l'unité de commande de **Protocole des paramètres IP** paginez, configurez ces derniers :

- **Sgf** sélectionnez le TCP de Syslog ou l'UDP de Syslog au besoin.
- **L'adresse IP de serveur de Syslog** écrit l'adresse IP de l'ordinateur où le watcher de Syslog est installé.
- **Le port de serveur de Syslog** introduit un numéro de port. Ceci devrait apparier le numéro de port introduit dans les **configurations de watcher de Syslog**.

Sous le GUI de watcher de Syslog, commencez le service par sélectionner le **serveur de début**, suivant les indications de l'image :

Syslog Watcher - Local Syslog Server

Start Server | Stop Server | Status | Reload | Filter | Find | Search | Import | Export | Delete | Reports | Storage | Settings | Vendor Pack | Help | Info

Show: Any Severity from All Sources last 1000 messages Update every 10 seconds Updated at 2/12/2014 5:57:35 AM AutoScroll

| Received | Source IP | Source Name | Facility | Severity | Timestamp | Tag | Origin | Message |
|--------------------------|-----------------|-------------|----------|----------|----------------------|------|-------------|---|
| 2/12/2014 5:57:35.794 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | SETM | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.744 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | AUD | SETM | ;INFO ;:2969;aud LIPSYNC: SYNC ENB: Y, SYNC REQ: Y, SOURCE: SAME AS PCR, LST GA... |
| 2/12/2014 5:57:35.724 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | AUD | MAXINT | ;INFO ;:2969;aud LIPSYNC: SYNC ENB: Y, SYNC REQ: Y, SOURCE: SAME AS PCR, LST GA... |
| 2/12/2014 5:57:35.704 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | SETM | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.664 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | SYNC | SETM | ;INFO ;:2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD... |
| 2/12/2014 5:57:35.649 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | AUD | SETM | ;INFO ;:3304;SyncOn=Y, Locked=Y, FIFO Und=N, Ovr=N, In Window=Y, dT=2ms, STC ... |
| 2/12/2014 5:57:35.649 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | SYNC | MAXINT | ;INFO ;:2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD... |
| 2/12/2014 5:57:35.649 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | SYNC | SETM | ;INFO ;:2438;AUDIO_0 Set Actual offset: Status = SYNCED, State = 12, offset = -647 |
| 2/12/2014 5:57:35.624 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | AUD | MAXINT | ;INFO ;:3304;SyncOn=Y, Locked=Y, FIFO Und=N, Ovr=N, In Window=Y, dT=0ms, STC ... |
| 2/12/2014 5:57:35.624 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | SYNC | MAXINT | ;INFO ;:2438;AUDIO_0 Set Actual offset: Status = SYNCED, State = 12, offset = 580 |
| 2/12/2014 5:57:35.584 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | SETM | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.584 AM | 192.111.111.172 | local1 | local1 | Info | 2014-02-12T05:53:14Z | SYNC | SETM | ;INFO ;:2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD... |
| 2/12/2014 5:57:35.544 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:4230;-->2 PES Buffer Size: 425 bytes |
| 2/12/2014 5:57:35.539 AM | 192.111.111.171 | local1 | local1 | Info | 2014-02-12T19:23:13Z | SYNC | User-cfg... | ;INFO ;:2543;-->2 LIPSYNC STATUS: GLOBAL STATE: NORMAL, NBR GLITCHES: 0, AUD... |
| 2/12/2014 5:57:35.534 AM | 192.111.111.171 | local1 | local1 | Info | 2014-02-12T19:23:13Z | AUD | User-cfg... | ;INFO ;:5940;-->2 aud_st_task: Stream Mode has changed from 0 to 1 |
| 2/12/2014 5:57:35.504 AM | 192.111.111.171 | local1 | local1 | Info | 2014-02-12T19:23:13Z | AUD | User-cfg... | ;INFO ;:5397;-->2 aud LIPSYNC: SYNC ENB: 1, SYNC REQ: 1, SOURCE: SAME AS PCR, LS... |
| 2/12/2014 5:57:35.489 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.469 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.434 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.354 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.214 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |
| 2/12/2014 5:57:35.199 AM | 192.111.111.173 | local1 | local1 | Info | 2014-02-12T05:53:14Z | VID | MAXINT | ;INFO ;:0 ;-->2 STAPE: Cisco: NeedForUpdateReferenceList == TRUE |

Message View

Exporter les messages enregistrés à un fichier CSV

Sur le GUI de watcher de Syslog, clic dans le bouton d'exportation sur la barre d'outil, qui apporte

l'écran, suivant les indications de l'image.

Export Syslogs

Source

Selected syslog messages

Displayed syslog messages

Syslog messages from the storage:

Period from: 7/02/2014 2:00 PM QuickSet ▶

to: 12/02/2014 2:00 PM Criteria...

Destination

Syslog file (recommended to exchange between Syslog Watchers)

Custom text file

SQL database (ODBC)

Next > Cancel

Vous pouvez sélectionner pour exporter des messages au cours d'une période spécifique d'intérêt ou pour exporter seulement une sélection particulière. Dans l'écran ci-dessus, il est sélectionné pour exporter les messages qui se sont produits au cours d'une période.

Sous la destination, sélectionnez le fichier texte fait sur commande et cliquez sur Next.

Export to Text File [X]

Destination Files

Export root folder: [Explore Folder](#)

Subfolder: \ Filename:

Create next file when the size is more than: KBytes

Processing Options

Trim large syslog messages to: characters

Preprocess message for:

Line ending: Encoding:

File Format

File header: Lines: 0

Message conversion template: Lines: 1

File footer: Lines: 0

Sélectionnez un répertoire de destination, ajoutez un sous-dossier et donnez un nom du fichier avec l'extension .csv. Si le sous-dossier n'existe pas, il est créé.

Clic dans l'exportation.

Supprimer de vieux messages

Sur le GUI de watcher de Syslog, cliquez sur Delete sur la barre d'outil, qui apporte l'écran, suivant les indications de l'image :



Définissez la période l'où vous voudriez supprimer les messages et cliquer sur dans l'**effacement**. Vous pouvez également, utiliser le bouton à congélation rapide pour sélectionner rapidement des périodes de prédéfinis comme l'un jour passé ou une semaine etc.