

Configure a un servidor de Syslog para capturar los registros de las D98xx Series IRDs

Contenido

[Introducción](#)

[Antecedentes](#)

[Configure al servidor de Syslog](#)

[Configure el IRD \(D9854/D9858/D9859\) para enviar los registros al vigilante del Syslog](#)

[Exportando los mensajes salvados a archivo CSV](#)

[Borrar los viejos mensajes](#)

Introducción

Este documento describe cómo configurar a un servidor de Syslog para capturar los registros de los receptores/de los decodificadores integrados las D98xx Series (IRDs).

Antecedentes

Software Release 4.0 de D9854, D9858 y D9824, y cualquier versión de los **mensajes de Syslog** obedientes del RFC-3164 del soporte D9859. Los clientes pueden ahora capturar los mensajes con un servidor de Syslog para el almacenamiento y la extracción. Además, este procedimiento se puede también utilizar con el nuevo receptor del transporte de la red D9800.

El **vigilante del Syslog** es el **servidor de Syslog** libre soportado para las máquinas de Windows. Para las máquinas de Linux, el **servidor de Syslog** soportado es el Syslog-NG que es disponible desde HTTP: [/www.balabit.com/network-security/syslog-ng/opensource-logging-system](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system)

Este artículo se ocupa solamente de configurar en las máquinas de Windows.

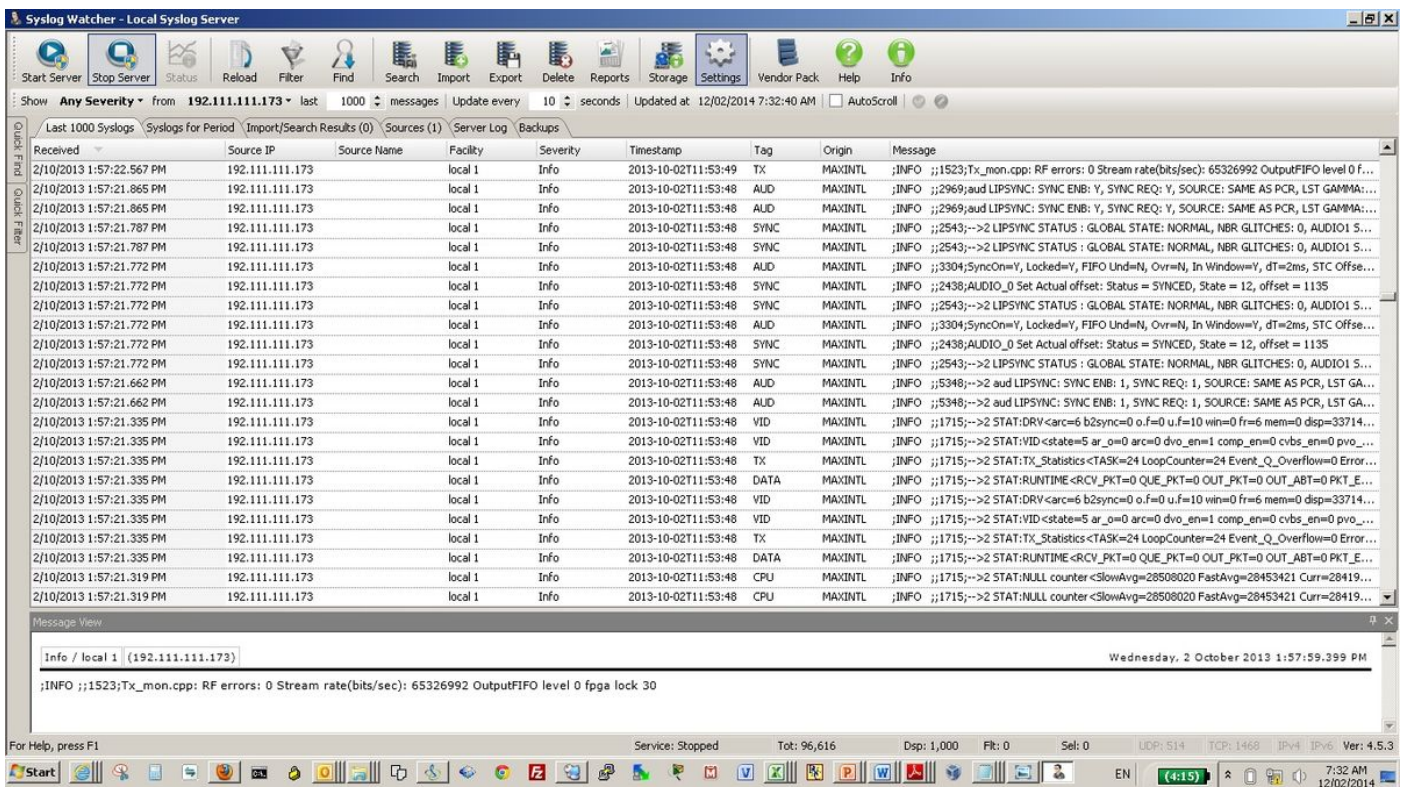
Configure al servidor de Syslog

Descargue al **vigilante del Syslog** de

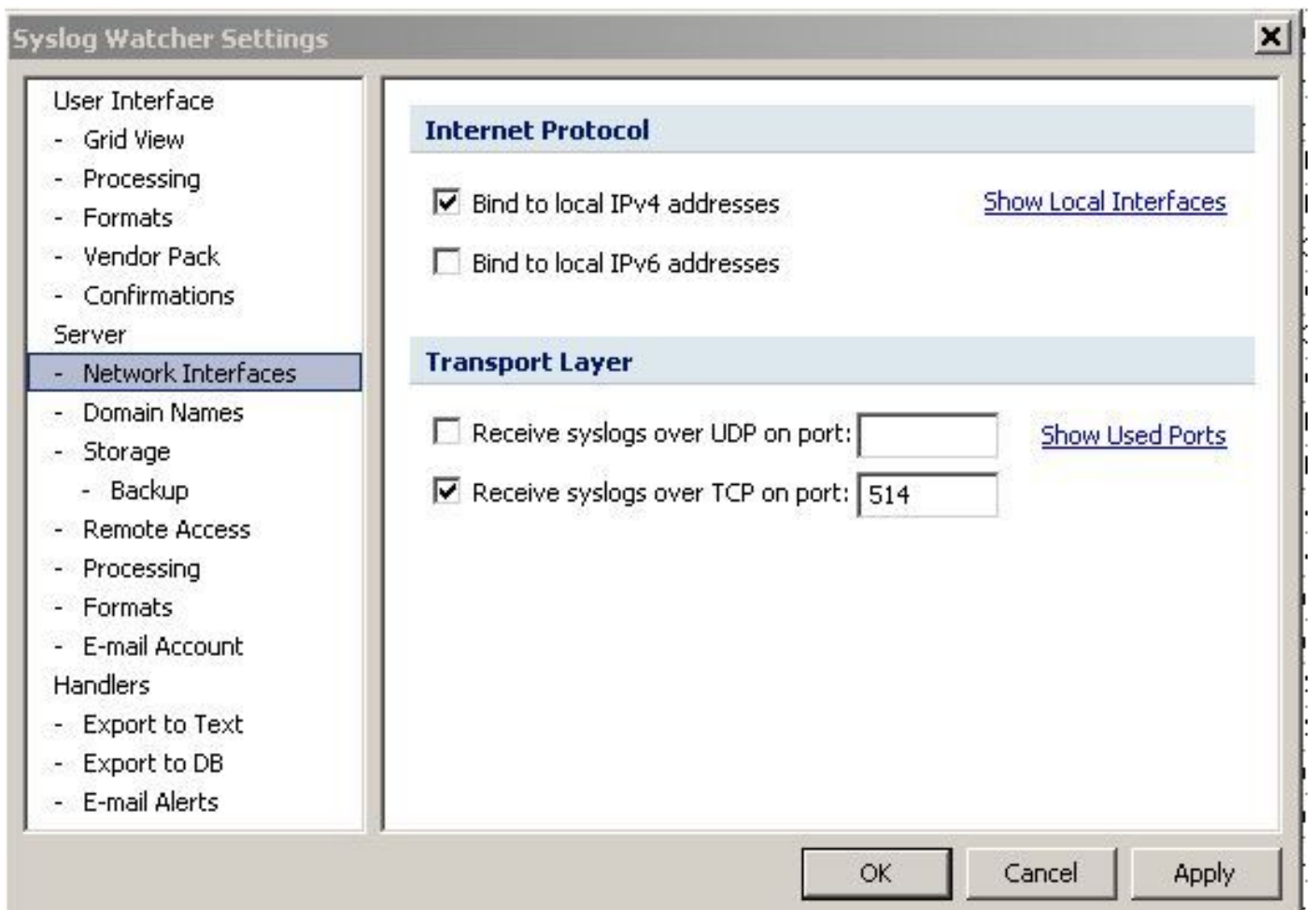
HTTP: [/www.snmpsoft.com/syslogwatcher/syslog-server.html](http://www.snmpsoft.com/syslogwatcher/syslog-server.html)

y instalelo en su computador con Windows.

Comience al vigilante del Syslog y seleccione al modo de operación para el GUI como **manejan servidor de Syslog local**, la imagen mostrada aparece:

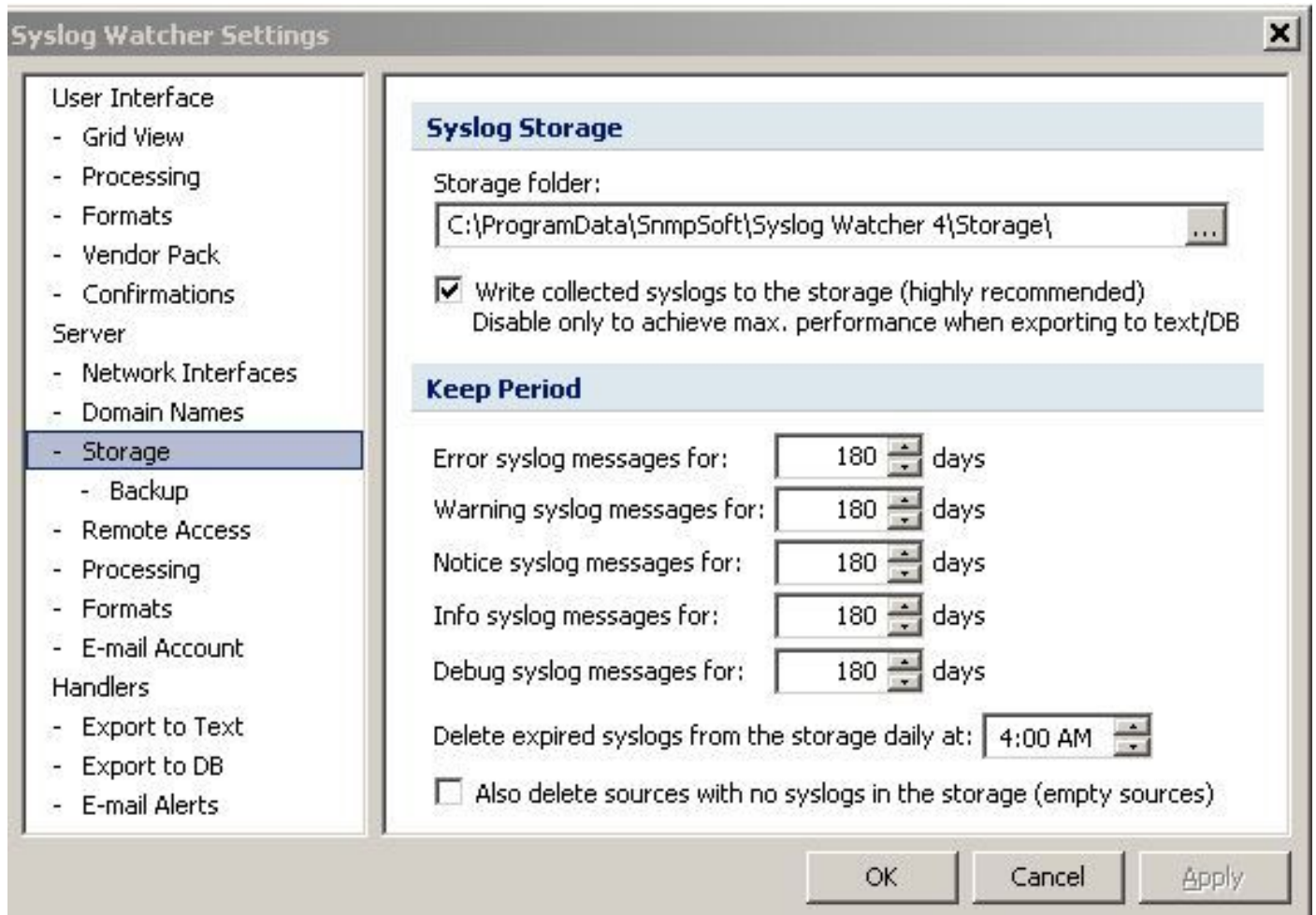


Haga clic en las **configuraciones** (resaltadas en la ilustración superior) en la barra de herramienta, la imagen mostrada aparece:



Seleccione las **interfaces de la red**. Marque el rectángulo **reciben los Syslog sobre el UDP en el puerto** e ingresa un número del puerto. El número del mismo puerto necesita ser configurado en los dispositivos de donde el vigilante del Syslog necesita recibir los registros.

Ahora seleccione el **almacenamiento** bajo **configuraciones del vigilante del Syslog**, tal y como se muestra en de la imagen:



Especifique una ubicación de la carpeta para salvar los mensajes, marque los Syslog **recogidos Write** del cuadro al **almacenamiento**.

Especifique el número de días para que cada tipo de mensaje sea mantenido el almacenamiento.

Configure el IRD (D9854/D9858/D9859) para enviar los registros al vigilante del Syslog

En el IRD GUI, seleccione las **configuraciones IP** de las **configuraciones del sistema** de la barra de herramienta. La imagen mostrada aparece:

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: Idle Timeout (seconds):

HTTP: 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

En la sección de control del protocolo de la página Configuración IP, configure éstos:

- **Syslog** seleccione el Syslog TCP o el Syslog UDP como sea necesario.
- El direccionamiento IP del servidor de Syslog ingresa el IP Address del ordenador donde el vigilante del Syslog está instalado.
- El puerto de servidor de Syslog ingresa un número del puerto. Esto debe corresponder con el número del puerto ingresado en las configuraciones del vigilante del Syslog.

Bajo el vigilante GUI del Syslog, comience el servicio seleccionando el servidor del comienzo, tal y como se muestra en de la imagen:

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

Exportando los mensajes salvados a archivo CSV

En el vigilante GUI del Syslog, tecleo en el botón de la exportación en la barra de herramienta,

que trae para arriba la pantalla, tal y como se muestra en de la imagen.

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

Usted puede seleccionar para exportar los mensajes durante un período específico de interés o para exportar solamente una selección determinada. En la pantalla antedicha, se selecciona para exportar los mensajes que ocurrieron durante un período.

Bajo el destino, seleccione el archivo de texto de encargo y haga clic **después**.

Export to Text File [X]

Destination Files

Export root folder: [...]

Subfolder: \ Filename: [Tag ▶] [Explore Folder](#)

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: [Tag ▶] Lines: 0

Message conversion template: [Tag ▶] Lines: 1

File footer: [Tag ▶] Lines: 0

Seleccione una carpeta de destino, agregue un Subfolder y dé un nombre del archivo con la extensión del .csv. Si no existe el Subfolder, se crea.

Tecleo en la **exportación**.

Borrar los viejos mensajes

En el vigilante GUI del Syslog, **cancelación del** teclado en la barra de herramienta, que trae para arriba la pantalla, tal y como se muestra en de la imagen:



Defina el período para el cual usted quisiera borrar los mensajes y hacer clic en la **cancelación**. Usted puede también, utilizar el botón de solidificación rápida para seleccionar rápidamente los períodos predefinidos como el último un día o una semana etc.