

# Estabelecer um servidor de SYSLOG para capturar logs do D98xx Series IRDs

## Índice

[Introdução](#)

[Informações de Apoio](#)

[Configurar o servidor de SYSLOG](#)

[Configurar o IRD \(D9854/D9858/D9859\) para enviar logs ao observador do Syslog](#)

[Exportando mensagens armazenadas para um arquivo CSV](#)

[Suprimindo de mensagens velhas](#)

## Introdução

Este documento descreve como estabelecer um servidor de SYSLOG para capturar logs dos receptores/decodificadores integrados D98xx Series (IRDs).

## Informações de Apoio

Software Release 4.0 de D9854, D9858 & D9824, e alguma liberação de **mensagens do syslog** complacentes do RFC-3164 do apoio D9859. Os clientes podem agora capturar as mensagens com um servidor de SYSLOG para o armazenamento e a recuperação. Além, este procedimento pode igualmente ser usado com o receptor novo do transporte da rede D9800.

O **observador do Syslog** é o **servidor de SYSLOG** livre apoiado para máquinas de Windows. Para máquinas de Linux, o **servidor de SYSLOG** apoiado é o Syslog-NG que está disponível do [HTTP: /www.balabit.com/network-security/syslog-ng/opensource-logging-system](http://www.balabit.com/network-security/syslog-ng/opensource-logging-system)

Este artigo trata somente a fundação em máquinas de Windows.

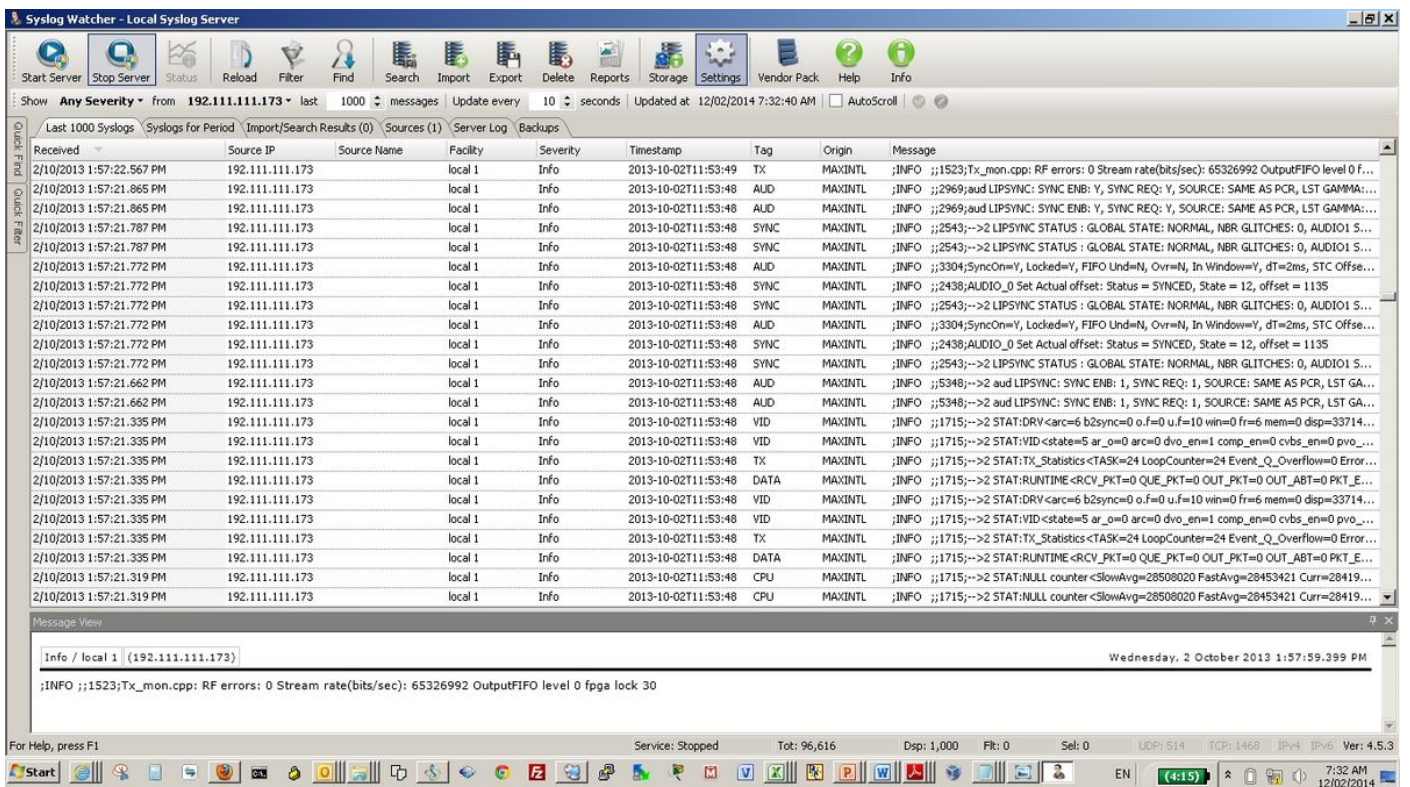
## Configurar o servidor de SYSLOG

Transfira o **observador do Syslog** de

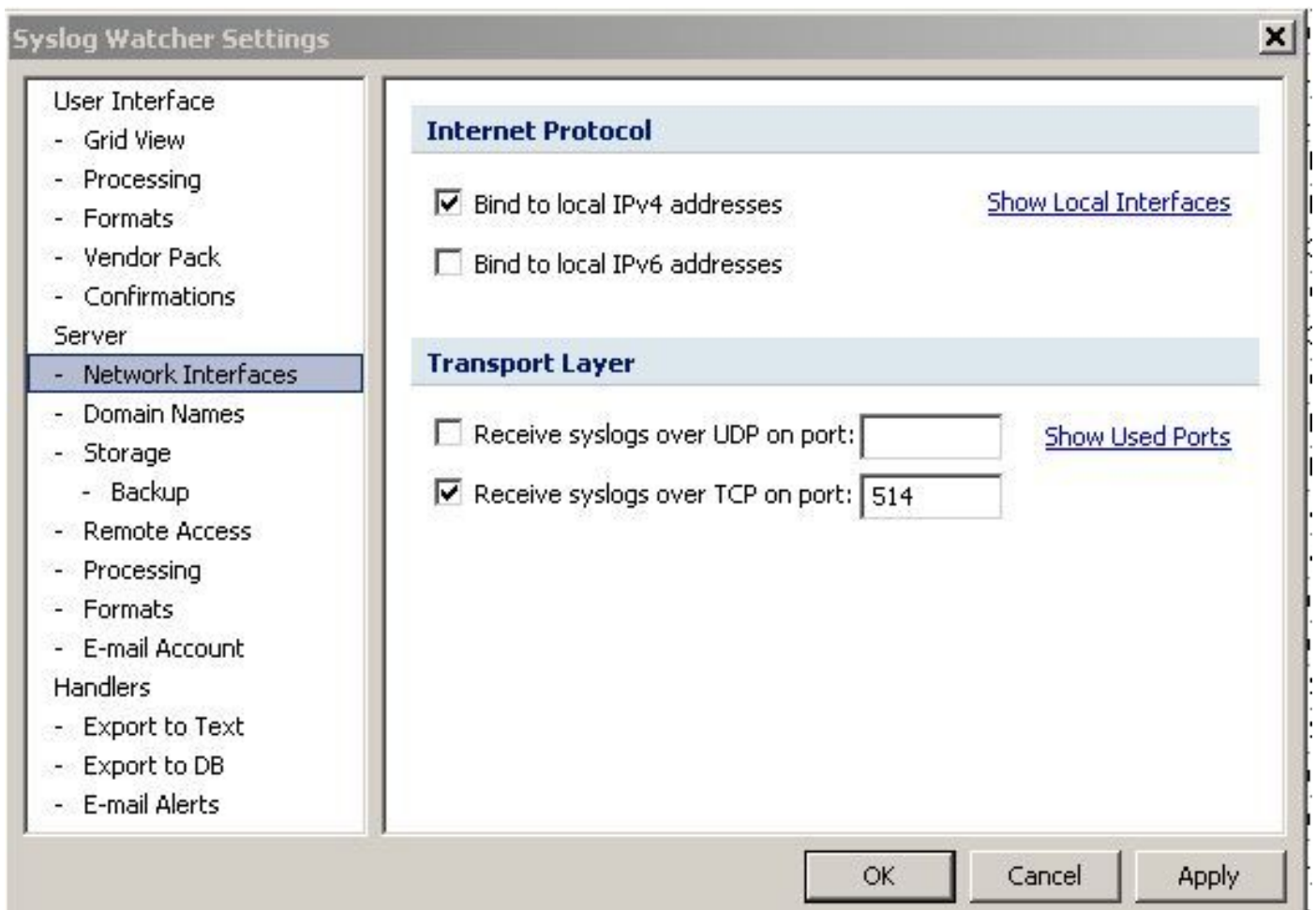
[HTTP: /www.snmpsoft.com/syslogwatcher/syslog-server.html](http://www.snmpsoft.com/syslogwatcher/syslog-server.html)

e instale-o em seu computador Windows.

Comece o observador do Syslog e selecione o modo operacional para o GUI como **controlam servidor de SYSLOG local**, a imagem mostrada aparece:

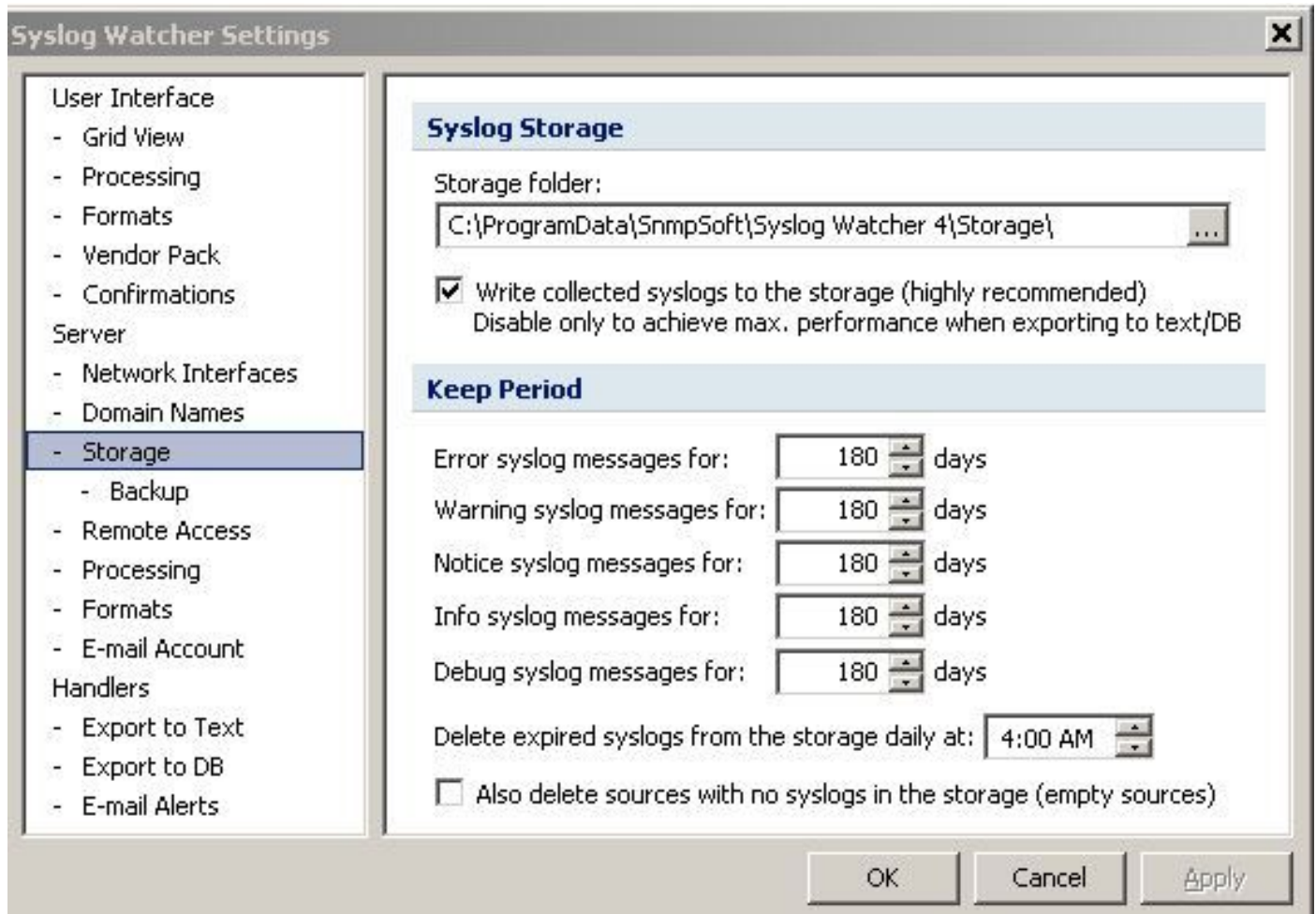


Clique nos **ajustes** (destacados na imagem acima) na barra de ferramentas, a imagem mostrada aparece:



Selecione **interfaces de rede**. Verifique a caixa **recebem Syslog sobre o UDP** na porta e entram em um número de porta. O número de mesma porta precisa de ser configurado nos dispositivos de onde o observador do Syslog precisa de receber logs.

Selecione agora o **armazenamento** sob **ajustes do observador do Syslog**, segundo as indicações da imagem:



Especifique um local da pasta armazenando as mensagens, verifique os Syslog **recolhidos Write** da caixa ao **armazenamento**.

Especifique o número de dias para que cada tipo de mensagem seja mantido no armazenamento.

## Configurar o IRD (D9854/D9858/D9859) para enviar logs ao observador do Syslog

No IRD GUI, selecione os **ajustes IP** dos **ajustes do sistema** da barra de ferramentas. A imagem 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

Na seção de controle de protocolo do IP os ajustes paginam, configuram estes:

- O Syslog seleciona o Syslog TCP ou o Syslog UDP como necessário.
- O endereço IP do servidor de SYSLOG incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT do computador onde o observador do Syslog é instalado.
- A porta de servidor de SYSLOG entra em um número de porta. Isto deve combinar o número de porta inscrito nos ajustes do observador do Syslog.

Sob o observador GUI do Syslog, comece o serviço selecionando o server do começo, segundo as indicações da imagem:

Syslog Watcher - Local Syslog Server

Start Service | 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 mensagens armazenadas para um arquivo CSV

No observador GUI do Syslog, clique no botão da exportação na barra de ferramentas, que traz

acima a tela, segundo as indicações da imagem.

**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

Você pode selecionar para exportar mensagens durante um período específico de interesse ou para exportar somente uma seleção particular. Na tela acima, é selecionada para exportar as mensagens que ocorreram durante um período.

Sob o destino, selecione o arquivo de texto feito sob encomenda e clique-o **em seguida**.

**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

Selecione uma pasta de destino, adicionar uma subpasta e dê um nome de arquivo com extensão .csv. Se a subpasta não existe, está criada.

Clique na **exportação**.

## Suprimindo de mensagens velhas

No observador GUI do Syslog, **supressão do** clique na barra de ferramentas, que traz acima a tela, segundo as indicações da imagem:



Defina o período para que você gostaria de suprimir das mensagens e das clicar na **supressão**. Você pode igualmente, para usar o botão do QuickSet para selecionar rapidamente períodos predefinidos como o último um dia ou a uma semana etc.