

# Implementação de servidor syslog.

[cfresqui@br.ibm.com](mailto:cfresqui@br.ibm.com)

[v1](#)



## Introdução

Com o requisito de estar de acordo com as políticas de retenção de logs dos ambientes, bem como a necessidade de análise dos logs para determinação de problemas e pensando nas modificações do sistema de arquivos a partir da versão *i* dos ESX, temos a necessidade de implementação de um serviço de syslog no ambiente.

Este documento mostra de forma simples como implementar um serviço de syslog para retenção/armazenamento de logs do ambiente VMware em uma máquina Windows. Lembrando que o syslog é um protocolo de rede (<http://tools.ietf.org/html/rfc5424>) e esse serviço pode ser utilizado para coletar/armazenar qualquer tipo de dispositivo compatível com este protocolo.

## Requisitos

**Windows server** (qualquer versão exceto NT4 e CE, 32 ou 64 bits)

Cygwin (software licenciado sob a GNU/GPL – opensource) para elaboração deste documento é utilizado a versão [1.7.16-1](http://www.cygwin.com/) - <http://www.cygwin.com/>

**Syslog-ng** Serviço propriamente de coleta/tratamento e armazenagem dos logs. Também opensource, instalado a partir do cygwin. Para elaboração deste documento foi utilizada a versão 3.2.5-1.

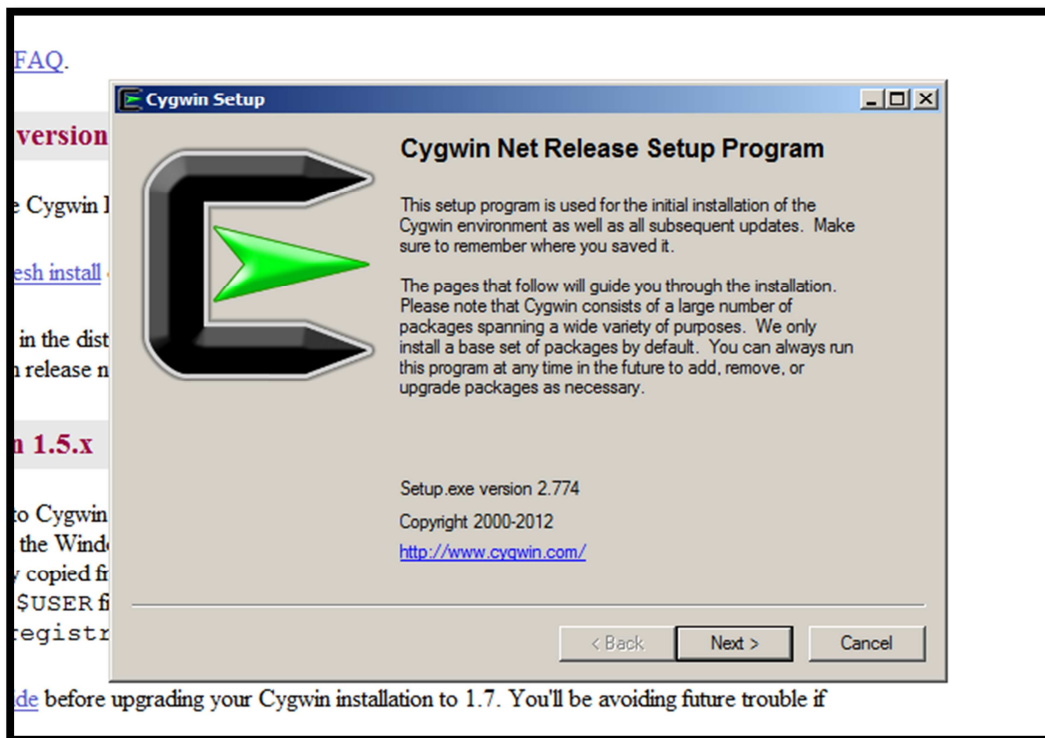
O cygwin faz o download dos pacotes necessário para funcionamento seu direto da internet. É possível fazer uma instalação offline, mas isto não é escopo deste documento.

## Instalação

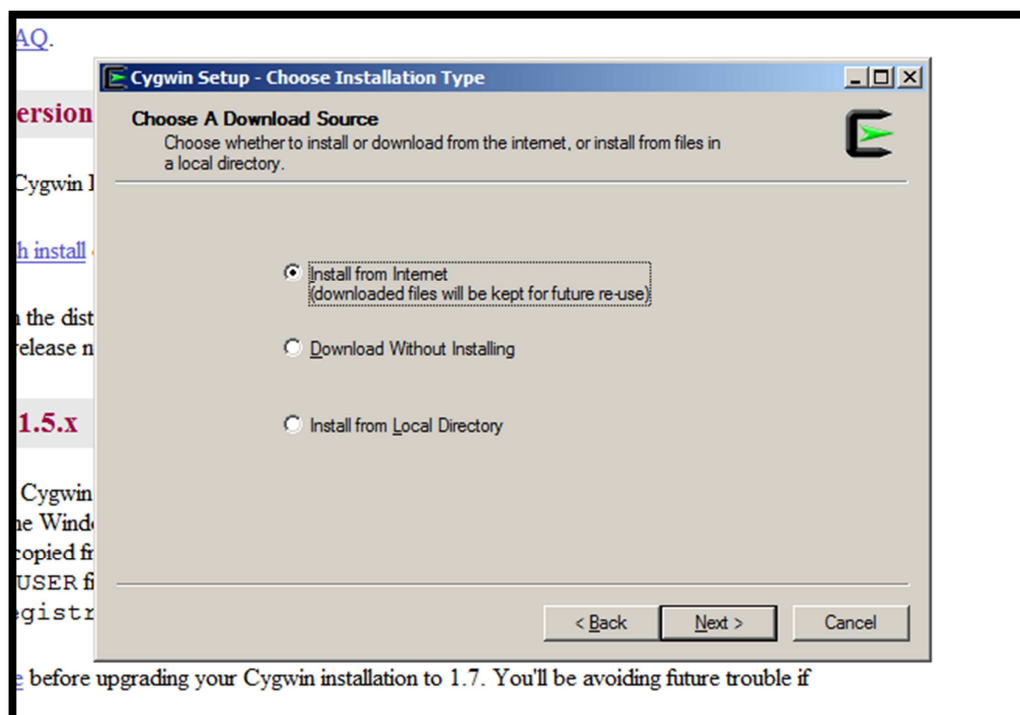
Baixar o arquivo setup.exe no site do cygwin - <http://www.cygwin.com/>



Execute o 'setup.exe'

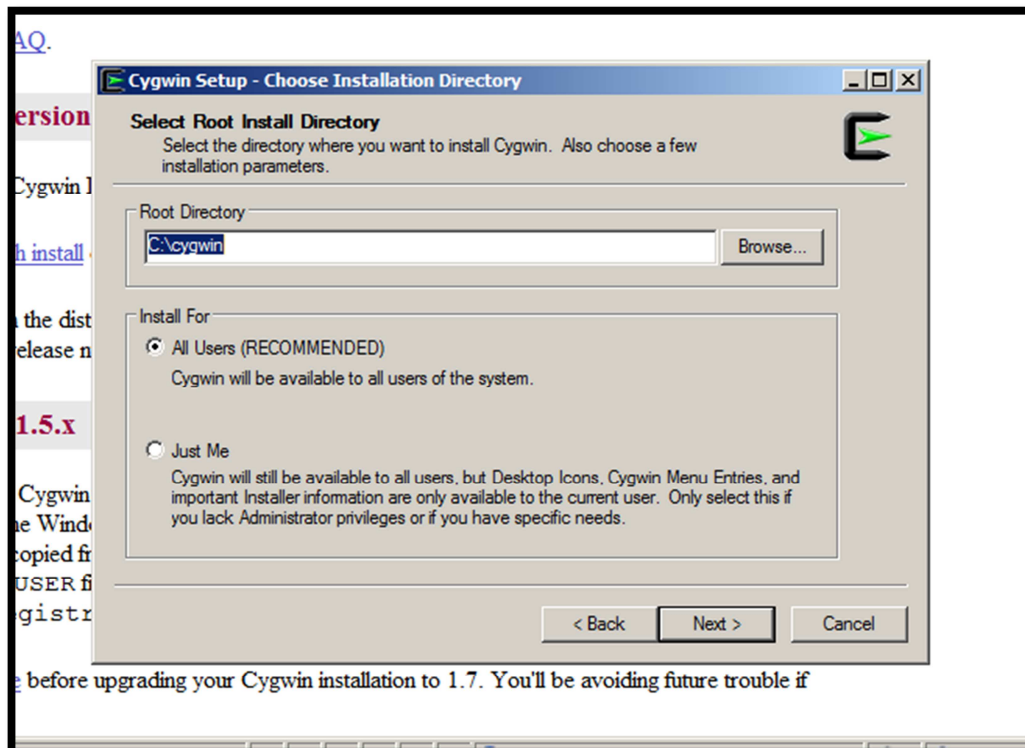


Next

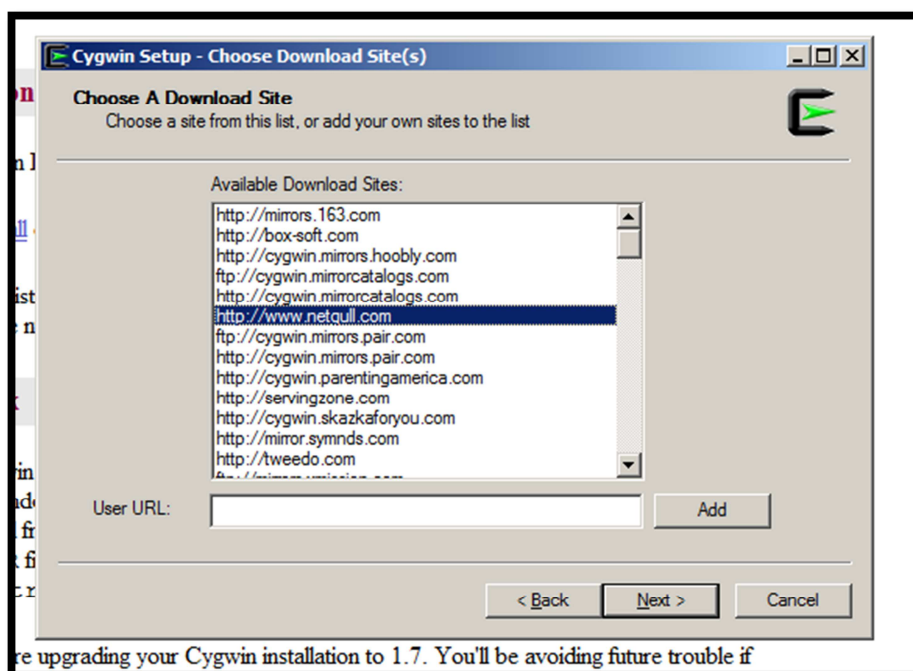


Next

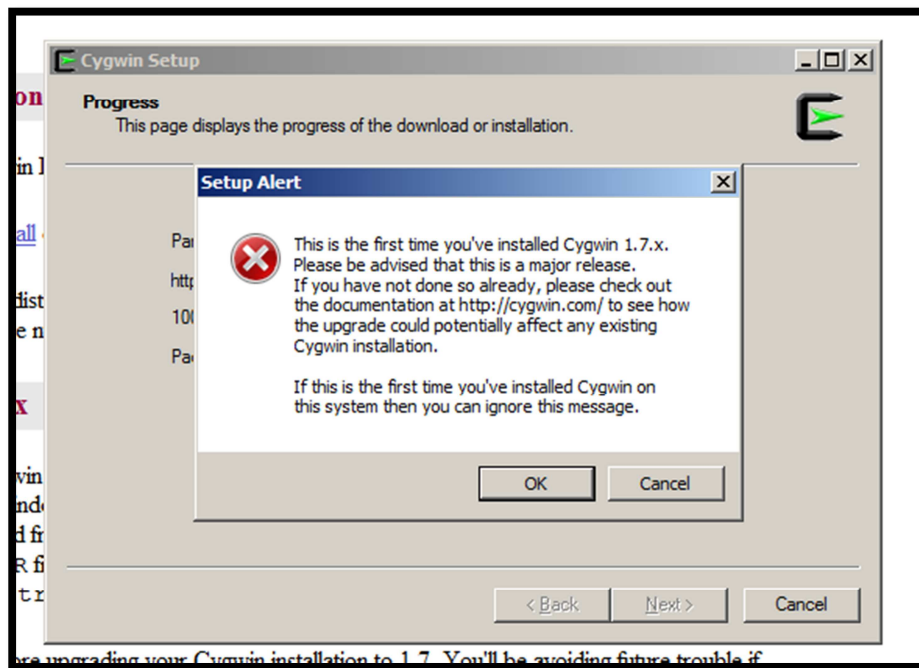
Selecione o diretório que o cygwin instalará os pacotes. A documentação do produto NÃO recomenda a alteração do caminho (\cygwin), porém, caso a quantidade de logs a serem armazenados seja grande, recomendo trocar a unidade para uma com espaço suficiente.



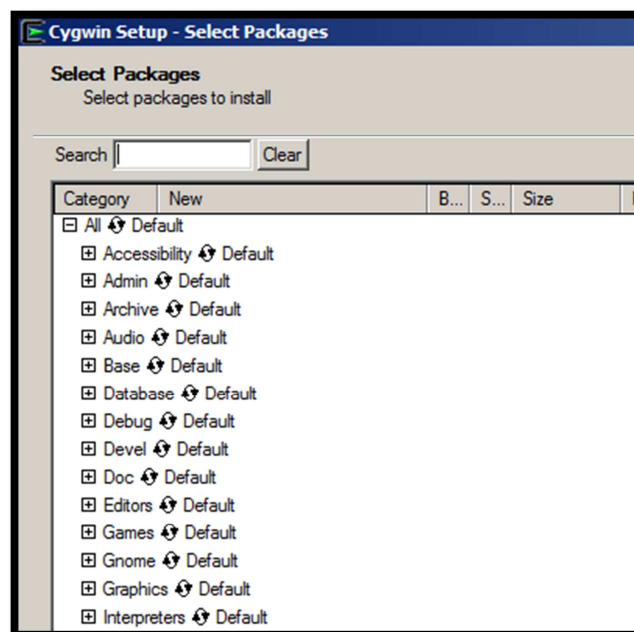
Selecione o mirror que o cygwin utilizará para baixar os pacotes



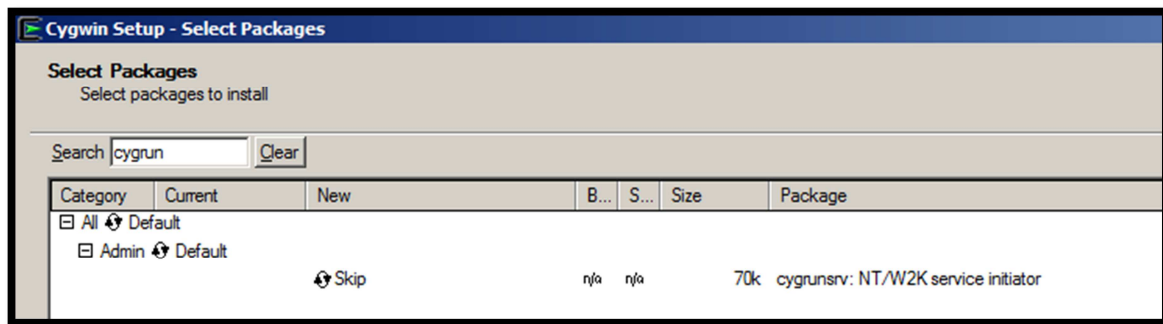
Confirme a mensagem clicando em OK



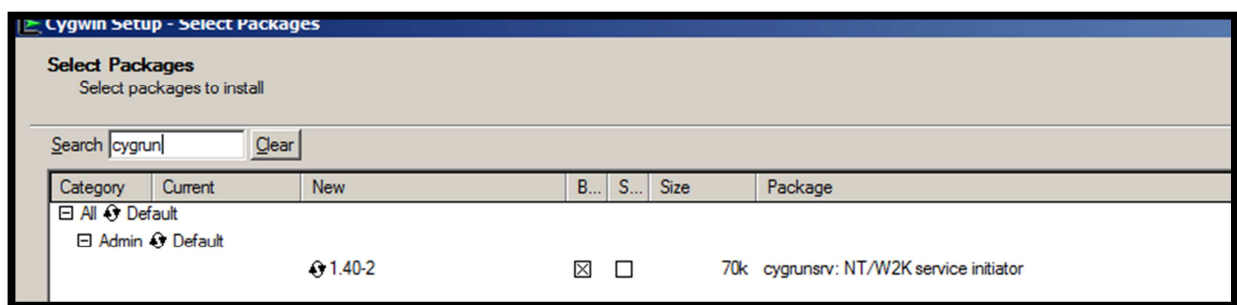
Após fazer o download dos pacotes disponíveis, o instalador perguntará quais são os pacotes adicionais que você quer instalar.



Para a nossa configuração, vamos precisar do **syslog-ng**, **cron**, **cygrun** e o **vim**



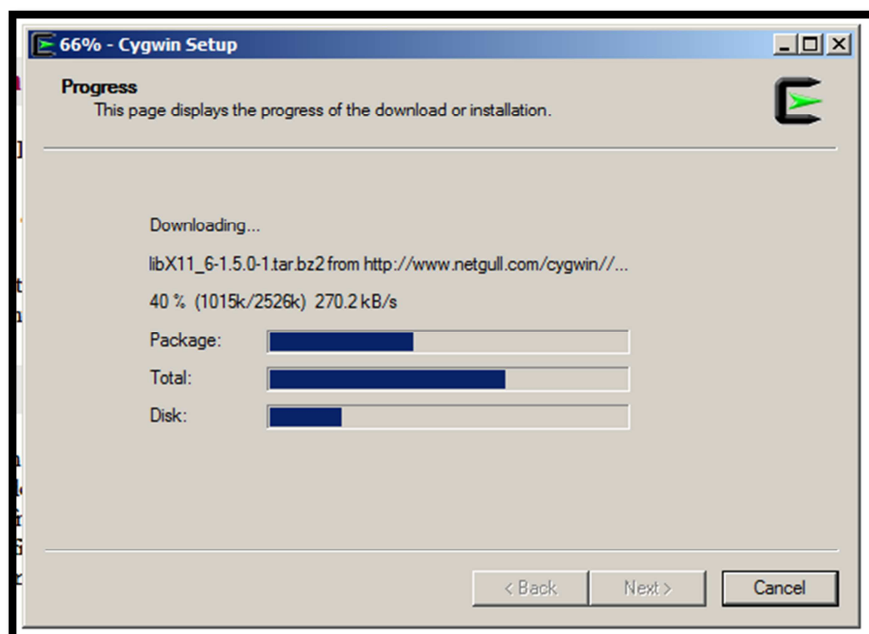
Entre com o nome de cada um deles e clique no “Skip” de forma que troque a palavra Skip para a versão do produto, desta forma:



Repita esse passo para os 4 pacotes:

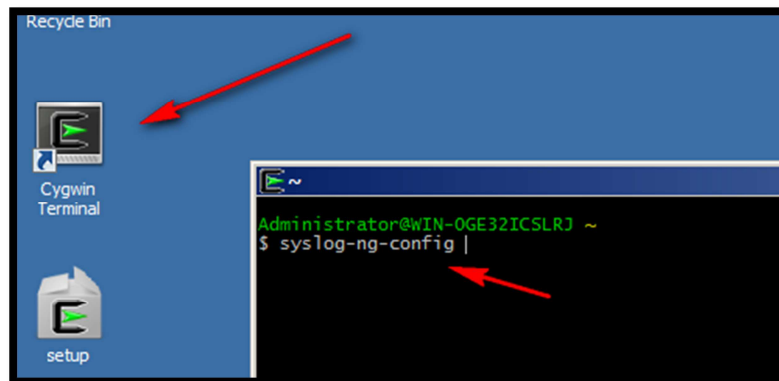
E por fim clique em Next.

O instalador ira baixar os pacotes selecionados bem como as dependencias necessárias para o funcionamento do produto

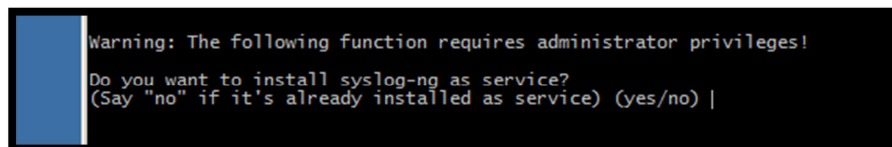


## Configuração do syslog server

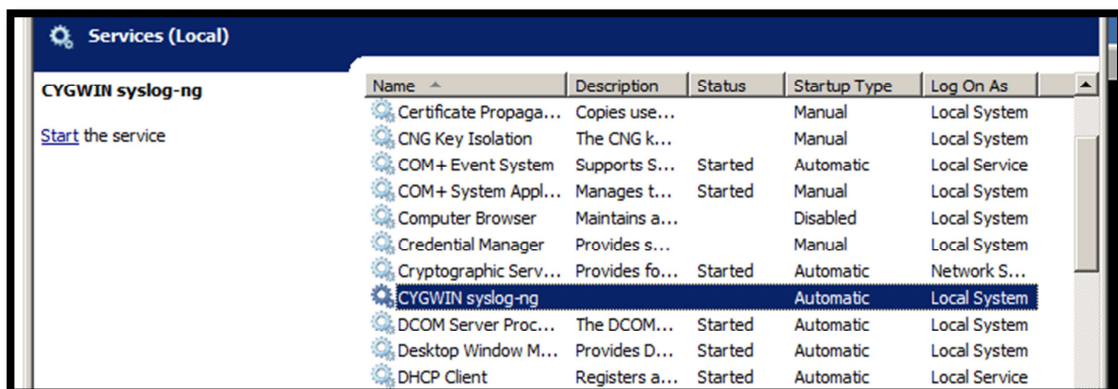
Uma vez finalizada a instalação, execute o programa **Cygwin Terminal** com privilégios de administrador (ou com o próprio usuário ou com a opção “Run As”)



E execute o comando `syslog-ng-config` e digite **yes** (sim, a palavra completa) para as 3 perguntas do configurador e por fim **yes** para registrar o syslog como um serviço do windows (inicialização automática entre outras coisas)

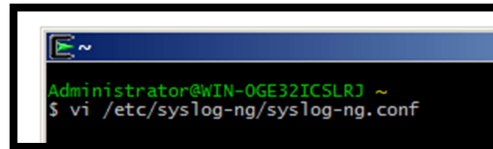


Quando ele finalizar a configuração o serviço deve estar listado no “services” do windows, desta forma:

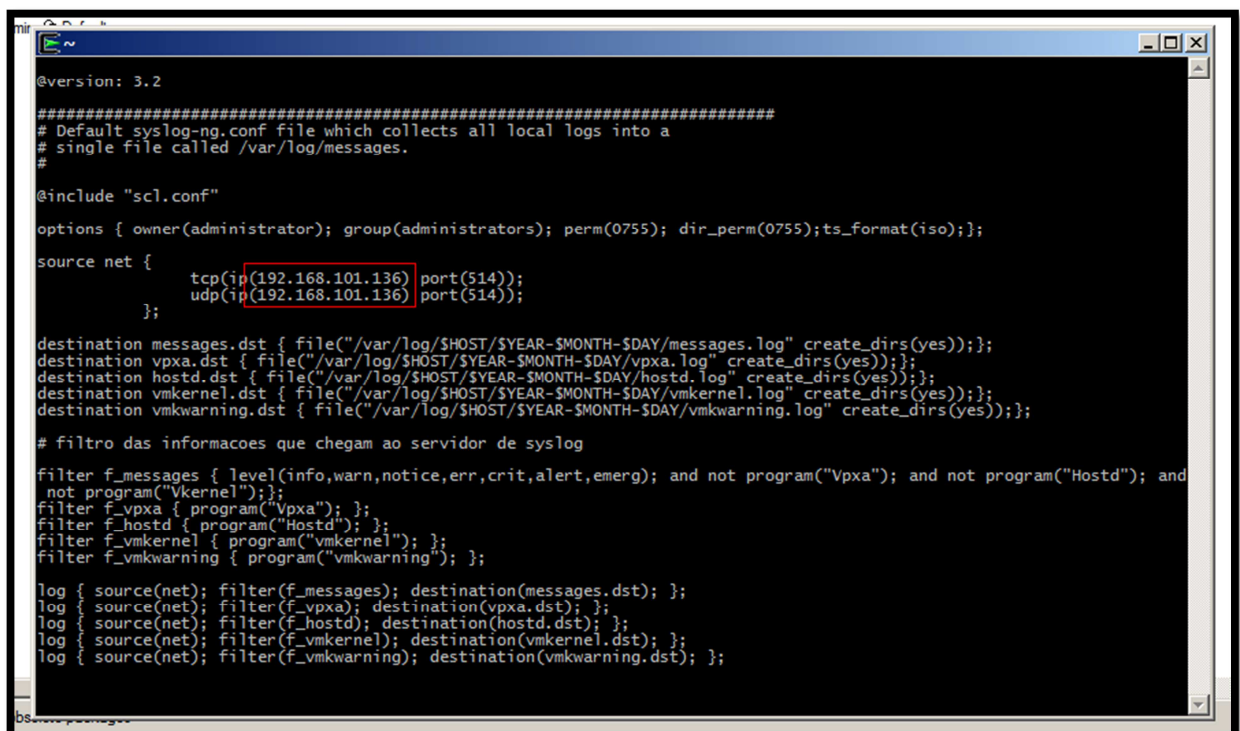


Finalmente com o serviço instado podemos fazer a configuração para o syslog-ng receber os logs dos servidores da rede.

Edite o arquivo /etc/syslog-ng/syslog-ng.conf com o vi.



E altere toda a configuração desta forma:



Obviamente voce tem que trocar o endereçamento IP para o correspondente da sua rede

```
@version: 3.2

#####
# Default syslog-ng.conf file which collects all local logs into a
# single file called /var/log/messages.
#

@include "scl.conf"

options { owner(administrator); group(administrators); perm(0755); dir_perm(0755);ts_format(iso);};

source net {
    tcp(ip(192.168.101.136) port(514));
    udp(ip(192.168.101.136) port(514));
};

destination messages.dst { file("/var/log/$HOST/$YEAR-$MONTH-$DAY/messages.log" create_dirs(yes));};
destination vpxa.dst { file("/var/log/$HOST/$YEAR-$MONTH-$DAY/vpxa.log" create_dirs(yes));};
destination hostd.dst { file("/var/log/$HOST/$YEAR-$MONTH-$DAY/hostd.log" create_dirs(yes));};
destination vmkernel.dst { file("/var/log/$HOST/$YEAR-$MONTH-$DAY/vmkernel.log" create_dirs(yes));};
destination vmkwarning.dst { file("/var/log/$HOST/$YEAR-$MONTH-$DAY/vmkwarning.log" create_dirs(yes));};

# filtro das informacoes que chegam ao servidor de syslog

filter f_messages { level(info,warn,notice,err,crit,alert,emerg); and not program("Vpxa"); and not program("Hostd"); and not
program("Vmkernel");};
filter f_vpxa { program("Vpxa"); };
filter f_hostd { program("Hostd"); };
filter f_vmkernel { program("vmkernel"); };
filter f_vmkwarning { program("vmkwarning"); };

log { source(net); filter(f_messages); destination(messages.dst); };
log { source(net); filter(f_vpxa); destination(vpxa.dst); };
log { source(net); filter(f_hostd); destination(hostd.dst); };
log { source(net); filter(f_vmkernel); destination(vmkernel.dst); };
log { source(net); filter(f_vmkwarning); destination(vmkwarning.dst); };

# filtro das informacoes que chegam ao servidor de syslog

filter f_messages { level(info,warn,notice,err,crit,alert,emerg); and not program("Vpxa"); and not program("Hostd"); and not
program("Vmkernel");};
filter f_vpxa { program("Vpxa"); };
filter f_hostd { program("Hostd"); };
filter f_vmkernel { program("vmkernel"); };
filter f_vmkwarning { program("vmkwarning"); };

log { source(net); filter(f_messages); destination(messages.dst); };
```



```
log { source(net); filter(f_vpxa); destination(vpxa.dst); };
log { source(net); filter(f_hostd); destination(hostd.dst); };
log { source(net); filter(f_vmkernel); destination(vmkernel.dst); };
log { source(net); filter(f_vmkernelwarning); destination(vmkernelwarning.dst); };
```

Finalmente, após a alteração do arquivo, basta subir o serviço no Windows.

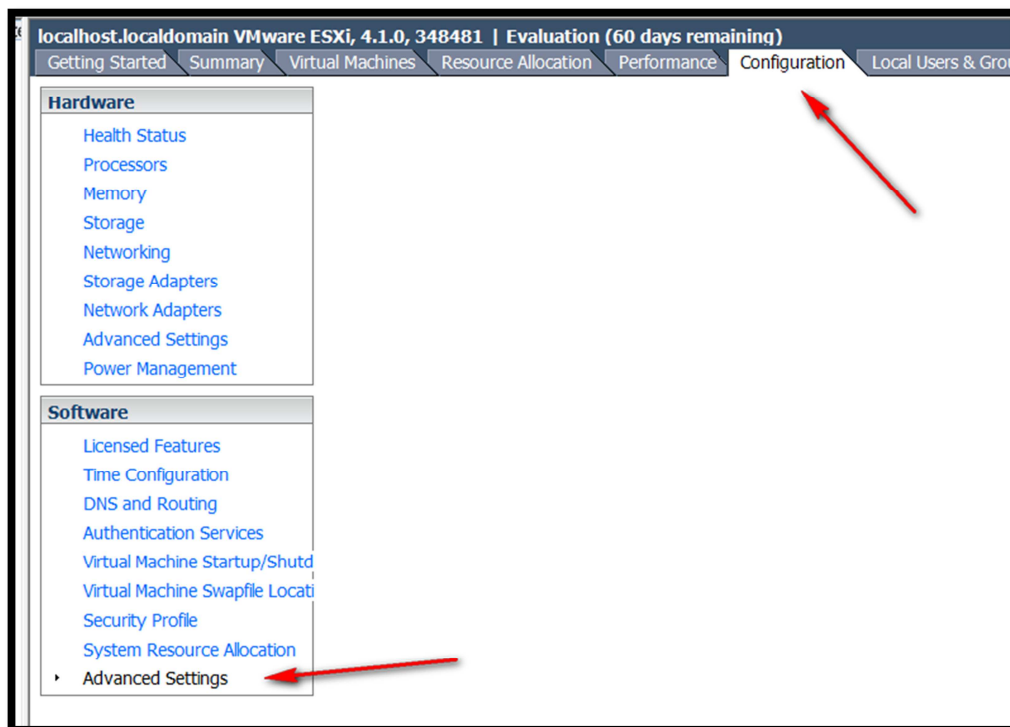
Cryptographic Serv...	Provides fo...	Started	Automatic	Network S...
CYGIN syslog-ng		Started	Automatic	Local System
DCOM Server Proc...	The DCOM...	Started	Automatic	Local System

## Configurando os ESX

Após a configuração do servidor de syslog, temos que apontar os servidores que queremos armazenar os logs. A configuração é bastante simples, basta apontar o endereço ip do servidor de log e liberar ao firewall do ESX, como vemos a seguir:

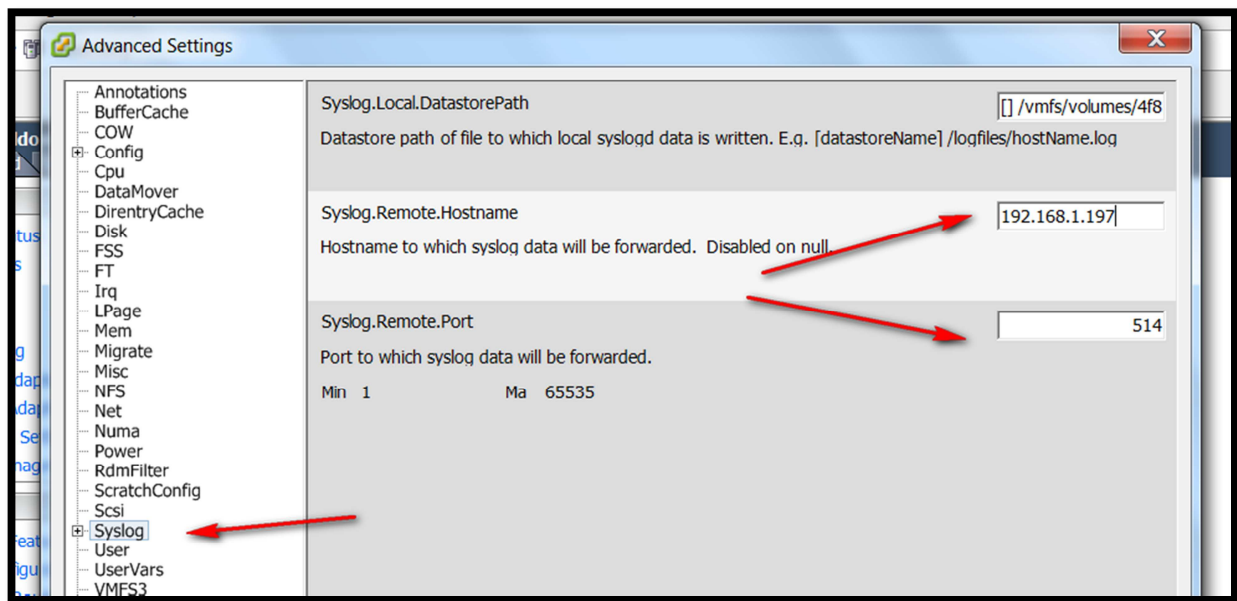
### Hosts ESX 4.x

Na aba Configuration vá na opção Advanced Settings



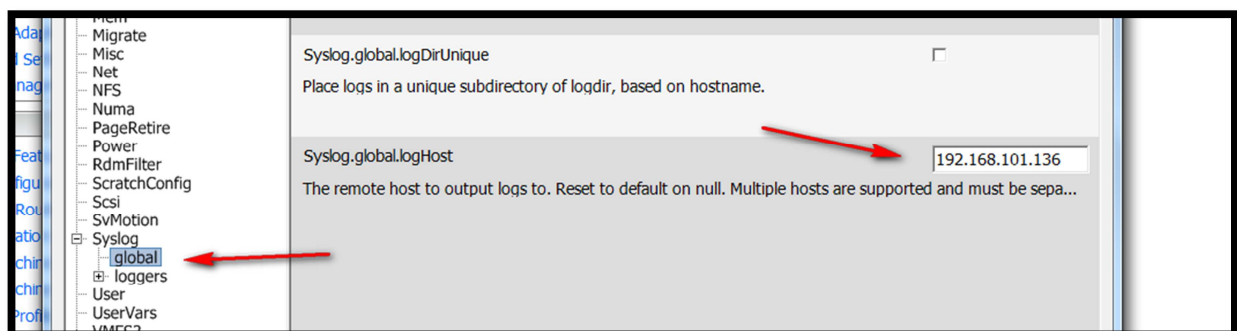
Configure o campo **syslog.remote.hostname** com o endereço ip do servidor de syslog configurado anteriormente e confirme a porta que será utilizada para esta conexão (default 514)



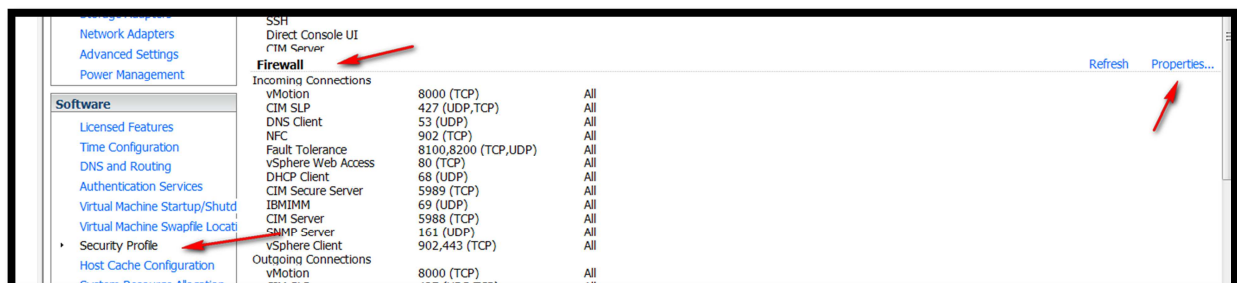


## Host ESX 5.x

Vá na mesma opção Configuration/Advanced Settings/Syslog/global e no syslog.global.logHost configure com o ip do syslog



No ESX 5 também é necessário liberar a porta 514 no firewall. Para isto vá novamente em Configuration e clique nas propriedades de Security Profile/Firewall.

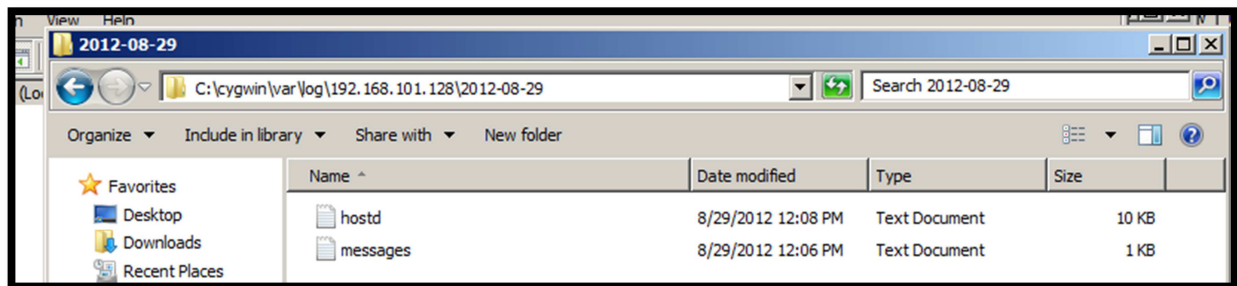


E selecione o check box Syslog

<input checked="" type="checkbox"/>	vSphere Web Access	80		TCP	N/A
<input checked="" type="checkbox"/>	syslog		514,1514	UDP,T...	N/A
<input type="checkbox"/>	DVSSync	8301,8302	8302,8301	UDP	N/A

Uma vez liberado no firewall os logs serão enviados para o syslogserver e serão armazenados no windows dentro do diretório

c:\cygwin\var\log\<hostname>\<data>\



Para usar o hostname ao invés do endereço IP basta configurar o DNS ou criar as entradas no arquivo hosts.

## Retenção e armazenamento de log

Para a compressão e armazenamento dos logs antigos do ambiente desenvolvi um simples script em shell que comprime e retira do diretório os logs antigos (mais velho que 2 semanas), dando um ganho de espaço em disco no servidor.

Crie o diretório /log\_arch – onde serão armazenados os logs compactados com o comando `mkdir /log_arch`

Crie com o vi o arquivo /limpa\_log.sh e deixe-o como indicado abaixo

```
#!/bin/bash
for i in `ls -d /var/log/*`;
do
    find $i -type f -mtime +14 | xargs tar zcf /log_arch/`echo $i | cut -d/ -f4`_`date +%F-%T`.tar.gz --remove-files
done
```

Instale o cron (agendador de tarefas do linux) com o comando

`cron-config`

Responda *yes* para a primeira pergunta:

```
Do you want to install the cron daemon as a service? (yes/no) yes
```

Não responda nada na segunda, simplesmente dê Enter

```
Enter the value of CYGWIN for the daemon: [ ]
```

*no*

```
Do you want the cron daemon to run as yourself? (yes/no) no
```

*yes*

```
are you using the cyglsa package ? (yes/no) yes  
The cron daemon will run as SYSTEM
```

E finalmente *yes*

```
... no problem found.  
Do you want to start the cron daemon as a service now? (yes/no) yes  
OK. The cron daemon is now running.
```

Uma vez configurado, execute o editor do cron com o comando `crontab -e` e configure desta forma:

```
0 3 * * 4 /limpa_log.sh
```

O editor usa o VI para sua configuração, então quando finalizar saia com Esc :x.

Valide a configuração executando o comando `crontab -l`

```
$ crontab -l  
# DO NOT EDIT THIS FILE - edit the master and reinstall.  
# (/tmp/crontab.pINAcUkyz9 installed on Thu Aug 30 07:10:18 2012)  
# (Cron version V5.0 -- $Id: crontab.c,v 1.12 2004/01/23 18:56:42 vixie Exp $)  
0 3 * * 4 /limpa_log.sh
```

O cron executará o script às 3 da manhã toda quarta-feira.

## Conclusão

Este documento apresenta uma maneira simples de resolver a necessidade de um servidor de syslog em ambientes Microsoft.