



Configurando Syslog/RSyslog no Linux

Data última revisão: 24/03/2009

versão: 1.1

Descrição: Como configurar uma distribuição GNU/Linux para enviar corretamente os logs do syslog ou rsyslog para o OpMon(OpLogs).

AVISO: Em caso de problemas em qualquer passo do procedimento, enviar o conteúdo da tela para a OpServices pelo email (suporte@opservices.com.br).

Dependências:

O sistema em questão deve ter instalado e ativo o serviço syslog/rsyslog

1. Procedimentos de configuração

a) Logar como usuário administrador(root) no servidor alvo.

b) Editar o arquivo de configuração do syslog/rsyslog, conforme mostra a figura abaixo editando um arquivo de configuração do syslog(/etc/syslog.conf).

```
root@COMPAQ-PC:~# vim /etc/syslog.conf
```

c) Realize as alterações até a linha 'FIM da configuração', conforme mostra na figura abaixo.

```
# /etc/syslog.conf
# OpLogs(inicio do arquivo)
*.warn;*.err;*.crit;*.emerg @IP_do_OpMon # Exemplo: *.warn;*.err;*.crit;*.emerg @10.10.10.1
# FIM da configuracao

# Uncomment this to see kernel messages on the console.
#kern.* /dev/console

# Log anything 'info' or higher, but lower than 'warn'.
# Exclude authpriv, cron, mail, and news. These are logged elsewhere.
*.info;*.!warn;\
    authpriv.none;cron.none;mail.none;news.none -/var/log/messages
```

d) Reinicie o serviço com o comando abaixo, conforme mostra a figura, ou utilize scripts nativos da distribuição para fazê-lo.

```
root@COMPAQ-PC:~# killall -HUP syslogd
root@COMPAQ-PC:~#
```

e) Para testar se a alteração foi realizada corretamente, utilize o comando abaixo na figura.

```
root@COMPAQ-PC:~# tcpdump -i eth0 port 514
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
```

IMPORTANTE: O retorno deste comando deve apresentar o fluxo de saída para o OpMon, como no exemplo abaixo:

```
14:05:30.743427 IP 192.168.10.1.47819 > 10.10.10.1.514
```

```
14:06:34.743427 IP 192.168.10.1.47819 > 10.10.10.1.514
```

```
14:07:23.743427 IP 192.168.10.1.47819 > 10.10.10.1.514
```

As configurações para o Rsyslog no arquivo de configuração do serviço segue o mesmo padrão, modificando somente o arquivo a ser editado, bem como o serviço que será reiniciado no sistema.

Após a conclusão do procedimento, informar a OpServices através do email suporte@opservices.com.br para que possa ser feito os testes necessários e a configuração dos itens a serem monitorados no referido servidor.