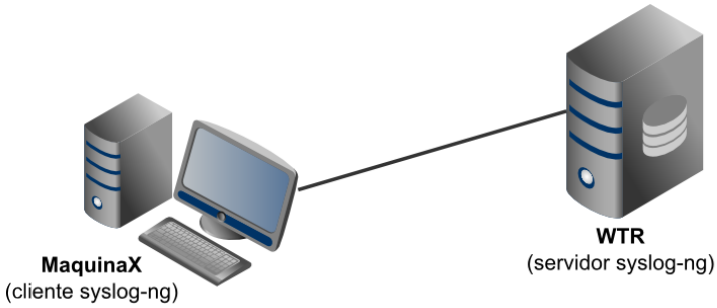
Prática 04: Configurando Servidor de Logs



Este laboratório visa apresentar aos alunos os passos para configuração de um servidor de logs remoto e um cliente usando o ***syslog-ng***. A figura acima ilustra a topologia lógica para configuração do ambiente. Nessa figura, a máquina ***MaquinaX*** a máquina virtual de um colega de laboratório que funcionará como cliente do serviço enviando os logs, enquanto que ***WTR*** representa sua máquina virtual que funcionará como servidor de logs.

Obs.: Substitua o ***X*** abaixo por um identificador único fornecido pelo instrutor (valor natural de 0 à 255).

Objetivo da Prática

- Configurar um servidor de logs com syslog-ng
- Configurar um cliente para envio de logs para o servidor remoto

Parte 01: Configuração do servidor de logs

Passos para configuração (os comandos a seguir devem ser executados na máquina ***WTR*** a menos que diga-se explicitamente o contrário):

- Desabilite o firewall da máquina (caso esteja habilitado):

```
iptables -F
iptables -t nat -F
rmmod iptable_filter
rmmod iptable_nat
rmmod ip_tables
```

- Certifique-se que o syslog-ng já está instalado em sua máquina. Para isso execute o seguinte comando (a parte em negrito são os dados fornecidos pelo usuário):

```
root@wtr:~# dpkg -l syslog-ng
Desejado=U=Desconhecido/Instalar/Remover/exPurgar/H=Reter
| Estado=Não/Inst/arqs-Cfg/U=Descomp/Falhou-cfg/H=semi-inst/W=trig-adiado/Trig-pend
|/ Erro?=(nenhum)/H=Ret/precisa-Reinst/X=ambos-problemas (Est,Err: maiúsculas=ruim)
||/ Nome         Versão       Descrição
+++-==============-==============-
=============================================
ii  syslog-ng     2.0.9-4.1    Next generation logging daemon
```

Caso não esteja instalado, execute o seguinte comando:

aptitude install syslog-ng

- Edite o arquivo `/etc/syslog-ng/syslog-ng.conf` e adicione o seguinte ao seu final (para evitar o trabalho de digitar o conteúdo abaixo, foi disponibilizado o arquivo de configuração do syslog-ng em `/root/arquivos/syslog-ng.conf`. Copie-o para o `/etc/syslog-ng/` – ***cp /root/arquivos/syslog-ng.conf /etc/syslog-ng/*** - e substitua o X pelo valor apropriado):

```
# Definicao da origem
source servidores {udp(ip(0.0.0.0) port(514));};

# Definicao do destino
destination dr_messages { file("/var/log/servidores/$HOST/messages.log"); };
destination dr_auth { file("/var/log/servidores/$HOST/auth.log"); };
destination dr_daemon { file("/var/log/servidores/$HOST/daemon.log"); };
destination dr_kern { file("/var/log/servidores/$HOST/kern.log"); };
destination dr_syslog { file("/var/log/servidores/$HOST/syslog.log"); };
destination dr_debug { file("/var/log/servidores/$HOST/debug.log"); };
destination dr_local { file("/var/log/servidores/$HOST/$FACILITY.log"); };
destination dr_mail { file("/var/log/servidores/$HOST/mail.log"); };
destination dr_mail_err { file("/var/log/servidores/$HOST/mail-err.log"); };

# Filtro para as facilidades local*
filter f_local {
    facility(local0,local1,local2,local3,local4,local5,local6,local7);
};

# Arquivo messages
log {
        source(servidores);
        filter(f_messages);
        destination(dr_messages);
};

# Arquivo auth.log
log {
        source(servidores);
        filter(f_auth);
        destination(dr_auth);
};

# Regra do syslog
log {
        source(servidores);
        filter(f_syslog);
        destination(dr_syslog);
};

# Arquivo daemon.log
log {
        source(servidores);
        filter(f_daemon);
```

Apoio:

```
        destination(dr_daemon);
};

# Arquivo kern.log
log {
        source(servidores);
        filter(f_kern);
        destination(dr_kern);
};

# Arquivo mail.log
log {
        source(servidores);
        filter(f_mail);
        destination(dr_mail);
};

# Arquivo mail.err
log {
        source(servidores);
        filter(f_mail_err);
        destination(dr_mail_err);
};

# Arquivo das facilities
log {
        source(servidores);
        filter(f_local);
        destination(dr_local);
};

# Arquivo debug
log {
        source(servidores);
        filter(f_debug);
        destination(dr_debug);
};
```

- Reinicie o servidor syslog-ng para carregar as novas configurações:
  /etc/init.d/syslog-ng restart

Parte 02: Configuração do cliente

Configure sua máquina como cliente do syslog-ng enviando os logs para o servidor de algum colega do laboratório (consulte-o sobre o endereço global da interface eth0 no servidor ***WTR*** dele. Para saber esse endereço peça-o para executar: ***ifconfig eth0***).

- Edite o arquivo `/etc/syslog-ng/syslog-ng.conf` e adicione o seguinte ao seu final:

```
destination loghost {
        udp("IP_DO_COLEGA" port(514));
};

log {
        source(s_all);
        destination(loghost);
};
```

- Reinicie o syslog-ng para carregar a nova configuração:

Apoio:


/etc/init.d/syslog-ng restart

- Verifique se seu servidor *syslog-ng* está armazenando corretamente os logs do seu colega. Para isso verifique no `/var/log/servidores/IP_DO_COLEGA/` se os arquivos de log foram criados corretamente.

Boa prática! Em caso de dúvidas, não hesite em consultar o instrutor.