CONFIGURAR UM SERVIDOR RSYSLOG ENTRE UBUNTU E CENTOS 7

Propriedades do rsyslog 7 ( Versão testada neste exemplo)

http://www.rsyslog.com/doc/v7-stable/configuration/properties.html

No servidor (Ubuntu) :

#Instalar o pacote no servidor do syslog .

apt-get install -y rsyslog

#Descomentar os módulos abaixo do arquivo **/etc/rsyslog.conf**

$ModLoad imuxsock # provides support for local system logging

$ModLoad imklog # provides kernel logging support

$ModLoad imudp

$UDPServerRun 514

$ModLoad imtcp

$InputTCPServerRun 514

#Criando um template para envio de arquivos dinâmicos( Isso pode sr feito somente no host cliente, mas no meu caso preferi fazer em todos inclusive no servidor.

$template LogCustomizado,"/var/log/from-%fromhost-ip%/%$now%.log"

#Diga que para qualquer coisa será usado o template LogCustomizado.

\*.\* ?LogCustomizado

#Mude a linha abaixo de acordo com o nome do seu template .

$ActionFileDefaultTemplate LogCustomizado

#Reinicie o rsyslog

service rsyslog restart

Resultado:

root@prd-audit01:/var/log# ls

alternatives.log boot.log dist-upgrade dmesg.1.gz dpkg.log **from-127.0.0.1** installer mail.log udev wtmp

apt bootstrap.log dmesg dmesg.2.gz faillog **from-192.168.0.125** kern.log

No Cliente (Centos):

#Instalar o pacote do rsyslog

yum install -y rsyslog

#Descomentar as linhas abaixo no arquivo **/etc/rsyslog.conf**

$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)

$ModLoad imjournal # provides access to the systemd journal

$ModLoad imudp

$UDPServerRun 514

$ModLoad imtcp

$InputTCPServerRun 514

#Criar um template de gravação dos logs.

$template LogCustomizado,"/var/log/%fromhost-ip%/%$now%.log"

#Comentar a linha default , copiá-la e criar uma nova apontado para o template usado.

**#$ActionFileDefaultTemplate RSYSLOG\_TraditionalFileFormat**

$ActionFileDefaultTemplate LogCustomizado

#Diga que será usado esse template para todos.

\*.\* ?LogCustomizado

#Descomente a linha que mostra um exemplo de configurar um servidor remoto.

\*.\* @@192.168.0.105:514

OBS: @@ (Conexão TCP ), @ (COnexão UDP)

#Crie um arquivo de configuração dentro de /etc/rsyslog.d/

touch /etc/rsyslog.d/teste.conf

echo “\*.\* @@192.168.0.105:514” >> /etc/rsyslog.d/teste.conf

#Salve o arquivo e reinicie o rsyslog

systemctl restart rsyslog

#faça um teste para ver se o servidor está recebendo os logs.

logger teste

No Servidor acompanhe :

tail -f /var/log/syslog

/var/log/from-127.0.0.1/2017-04-15.log**/var/log/from-192.168.0.125/2017-04-15.log/var/log/from-192.168.0.125/2017-04-15.log**