Relatório de Atividade – Servidor de Logs com Rsyslog (Linux)
Paulo Murilo Matielo de Oliveira
BV3031918
Sistema: Arch Linux
Atividade: Configuração de um servidor de log centralizado usando o rsyslog

Nesta atividade, foi configurado um servidor de logs com três clientes) enviando mensagens para esse servidor via protocolo TCP. Utilizou-se o rsyslog como ferramenta principal para recepção, roteamento e armazenamento dos logs gerados pelos clientes.

Procedimentos Realizados no Servidor ->

Instalação do rsyslog via pacman;

Edição do arquivo /etc/rsyslog.conf para ativar os módulos imudp e imtcp;

Criação do diretório /var/log/clients para armazenar logs por host;

Configuração do arquivo /etc/rsyslog.d/10-client-logs.conf com template personalizado;

Reinicialização do serviço com sudo systemctl restart rsyslog.

Procedimentos Realizados nos Clientes
Edição do arquivo /etc/rsyslog.conf para adicionar a linha de envio via TCP:

graphql
Copiar
Editar
. @@10.108.5.176:514
Reinicialização do rsyslog.

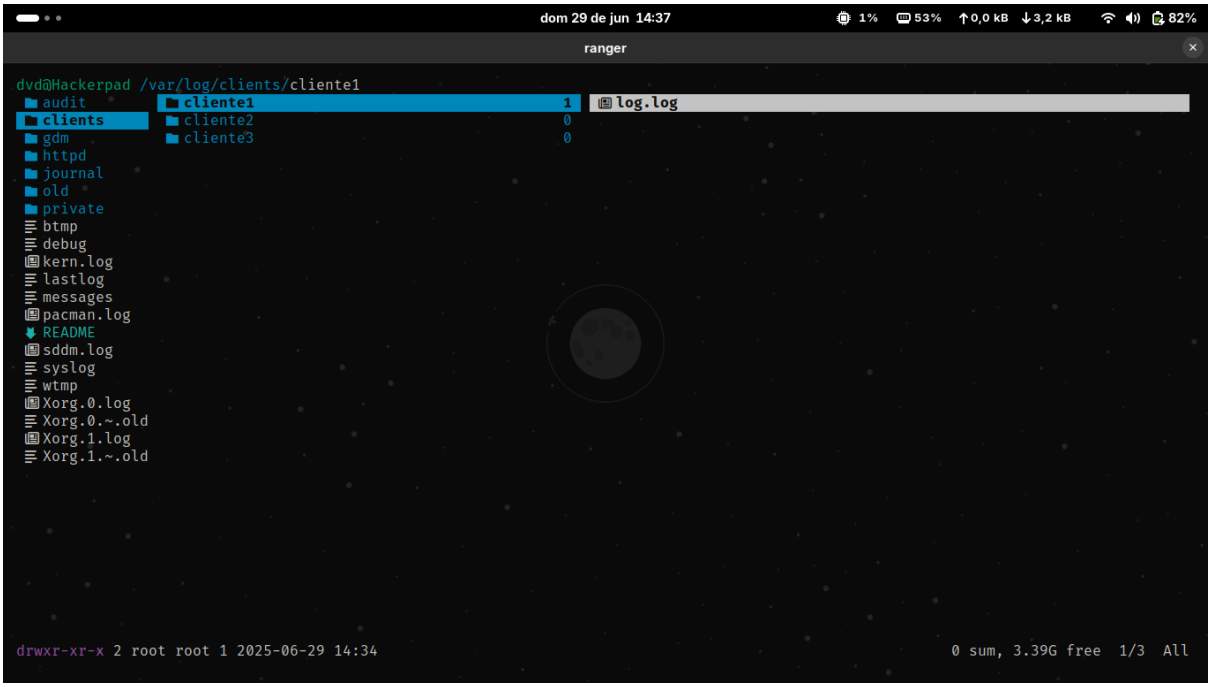
Geração de logs de teste com o comando:

bash
Copiar
Editar
logger "Teste de envio de log para o servidor central"

Verificação no Servidor
Confirmou-se a criação de subpastas dentro de /var/log/clients/ para cada host cliente;

Verificou-se a presença dos arquivos .log gerados e a mensagem enviada com o comando logger.

Logs


dom 29 de jun 14:37
1%
53%
0,0 kB
3,2 kB
82%
ranger
dvd@Hackerpad /var/log/clients/cliente1
audit
clients
gdm
httpd
journal
old
private
btmp
debug
kern.log
lastlog
messages
pacman.log
README
sddm.log
syslog
wtmp
Xorg.0.log
Xorg.0.~.old
Xorg.1.log
Xorg.1.~.old
cliente1 1
cliente2 0
cliente3 0
log.log
drwxr-xr-x 2 root root 1 2025-06-29 14:34
0 sum, 3.39G free 1/3 All