GNU/Linux
分析和存储日志

GNU/Linux
分析和存储日志

Rsyslog

实现集中管理日志

目的：

将 B 主机 (client) 的指定日志信息发送至 A 主机 (Server). 在 A 主机上可以集中查看 A 和 B 主机的全部信息

IP 说明

host-A:192.168.10.1

host-B:192.168.10.2

GNU/Linux
分析和存储日志

Rsyslog
Server 端 (A 主机) 实现
1) 配置 rsyslog.conf
#vim /etc/rsyslog.conf
将下列注释开启
$ModLoad imudp ← 开启 UDP syslog 输入插件
$UDPServerRun 514 ←- 开启 UDP 监听端口 514
$ModLoad imtcp ← 开启 TCP syslog 输入插件
$InputTCPServerRun 514 ← 开启 TCP 监听端口

GNU/Linux
分析和存储日志

Rsyslog

rsyslog 的传统传送日志方式的有 3 种

1. UDP 传输， 但信息有损耗

2. 基于 TCP 明文的传输，只在特定情况下丢失信息，并被广泛使用

3. RELP 传输，不会丢失信息，但只在 rsyslogd 3.15.0 及以上版本中可用

GNU/Linux
分析和存储日志

Rsyslog

如果准备使用 RELP 传输，需要手动添加以下内容：

```
$ModLoad imrelp
$InputRELPServerRun 2514
```

GNU/Linux
分析和存储日志

Rsyslog

2) 启用监听服务

#vim /etc/sysconfig/rsyslog

改为

SYSLOGD_OPTIONS="-r514 -c2"

GNU/Linux
分析和存储日志

Rsyslog

参数：

-c 指定运行兼容模式（兼容 syslog）

-r 指定监听端口

-x 再接收客户端时，禁用 DNS 查找（与 -r 配合）

-m 标记时间戳．单位：分钟，为 0 时，表示禁用。（即每个多少分钟，在日志文件里增加一MARK--，以便于确认 syslog 守护进程没有停止）

GNU/Linux
分析和存储日志

Rsyslog

参数：

-s ip：表示仅允许接收来自指定的 IP 信息

-s 192.168.10.1:192.168.10.2

GNU/Linux
分析和存储日志

Rsyslog

3) 重启主机 A 的 rsyslog 服务

```
#systemctl restart rsyslog
```

GNU/Linux
分析和存储日志

Rsyslog
Client(Host B) 配置
1) 配置 rsyslog.conf
#vim /etc/rsyslog.conf
在下面添加一行如下配置
. @192.168.10.1

注：
UDP 传输 在主机名前加 "@"
TCP 传输 在主机名前加 "@@"
RELP 传输 在主机名前加 ":omrelp:"

GNU/Linux
分析和存储日志

Rsyslog

Client(Host B) 配置

2）启动 rsyslog

#systemctl restart rsyslog.service

GNU/Linux
分析和存储日志

Rsyslog
测试
1)Server 端 (Host-A)
#tail -f /var/log/messages

2)Client 端 (Host-B)
#logger -t kern -p err “Messages From HostB”