推荐阅读　中

设备日志转储

导读 网络管理中对于设备日志应有严格、谨慎的规定。其中保存日志是必不可少的一项工作内容。但在转储日志时总是不成功。为什么会发生这种情况呢？对此，本文讲述了如何解决的办法和配置命令。

■ 浙江 许杨春

由于Cisco设备的Flash有限，将日志转储到Unix PC是一种有效的方式。这方面的资料非常多，最权威当然是Cisco的产品说明书，但是在实践发现按“Catalyst 3750 Switch Software Configuration Guide”中的说明配置后不一定成功，尤其是Unix PC端的配置需要调整。

1. 在Switch操作

```
3750#configure terminal
3750#logging <host>
// 这 里 <host> 是Unix PC的IP地址(本例中为10.68.173.253)
```

其他的配置都使用缺省值，这样一个最简单的日志转储到Unix PC的配置已经完成。

2. 在Unix PC操作

```
[root@localhost]#vi/etc/syslog.conf
local7.debug/var/log/cisco.log
//Cisco 文 档 在 IOS Release 12.2 (55) SE 的描述中有文件名不一致的问题
[root@localhost]#touch/var/log/cisco.log
// 建立或刷新文件cisco.log
[root@localhost]#chmod 666 /var/log/cisco.log
// 修改文件权限
```

(1) 再重新启动sylog进程

```
[root@localhost]#kill -HUP 'cat /etc/syslog.pid'
cat:/etc/syslog.pid:No such file or directory
kill:usage:kill[-s sigspec | -n signum | -sigspec] pid | jobspec or kill -l [sigspec]
```

这里碰到了第一个问题，syslog原来没有启动，所以用以下命令启动。

```
[root@localhost#service syslog start
```

但是过一段时间后，检查/var/log/cisco.log文件，发现文件大小依然为0。

再回到Switch检查，用以下命令检查日志的设置是否正确。

```
3750#show logging
Syslog logging:enabled (0 messages dropped,0 messages rate-limited,0 flushes,
    0overruns, xml disabled, filtering disabled)
    <略去无关显示>
    Trap logging:level informational,52 message lines logged
    Logging to 10.68.173.253 (udp port 514, audit disabled, authentication disabled, encryption disabled, link up)
    2 message lines logged
    0 message lines rate-limited
    0 message lines dropped-by-MD
    xml disabled, sequence number disabled
    filtering disabled
```

显示说明Switch确实在向Unix PC发包，那么UDP数据包是否到了Unix PC呢？Unix PC上执行Tcpdump可以看到类似Syslog包。

这说明从Switch到Unix PC的通路是通畅的，可以排除防火墙之类的影响。由于UDP无连接特性，还需要检查接收方是否运行正常，Unix PC上用Netstat命令察看UDP监听端口。

```
[root@localhost]#netstat -l -u
```

【下转第48页】

推荐阅读 中

保障网络的高可用性

导读 如何保障网络的高可用性，一直是每位网管员思考的问题。只有网络持续、稳定地运行，各种应用服务才得以运行。本文讲解如何利用VRRP技术保障服务器前端网络的高可用性。

■ 陕西 刘广

随着信息化的不断深入，人们的日常工作已经与网络息息相关，如通过门户系统获取各种信息、通过OA进行公文的处理、通过Email与他人进行信息交互、通过网络教学平台进行授课等等，每天的许多工作活动都与网络紧密相连。除了在保证每个应用平台不间断的提供服务之外，如何保证服务器前端网络的高可用性更是重中之重。一台服务器出现故障，几乎不会影响应用平台服务的提供，或者影响很小，但是一旦服务器前端网络出现故障，将会导致所有的网络应用平台无法提供服务，单位的工作和教学都将受到巨大影响。为了保证服务器前端网络的高可用性，服务器前端的网络结构我们单位采取了如下的设计方案，如图1所示。

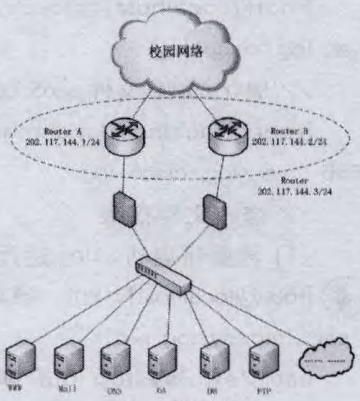

图1 网络拓扑图

首先，各种服务器通过二层交换机进行接入，二层交换机向上分别连接到两个路由器：Router A和Router B，服务器群的默认网关是：202.117.144.3，Router A的地址是：202.117.144.1，Router B的地址是：202.117.144.2，二层交换机与路由器之间串接了防火墙，防火墙以透传的方式进行工作。在这种拓扑设计中，充分利用了冗余路由协议

【上接第47页】

没有看到对应UDP端口(514)在监听。

检查后发现，原来该Linux版本的Syslog缺省设置是丢弃外来的数据，修改Syslog配置如下。

```
[root@localhost]#vi/etc/sysconfig/syslog
    #Options to syslogd
    #-m 0 disables 'MARK' messages.
    #-r enables logging from remote machines
    #-x disables DNS lookups on messages recieved with -r
    #See syslogd (8) for more details
    SYSLOGD_OPTIONS= "-m 0 -r"
```

再重启syslog，netstat就可以看syslog udp监听端口。

再检查检查/var/log/cisco.log文件大量数据包。

最后关闭Switch的日志输出，命令如下。

```
LTE_3750 (config) #no logging on
```