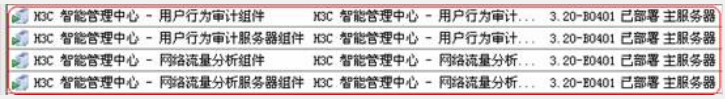
iMC NTA/UBA组件无法看到流量日志日志的排错思路

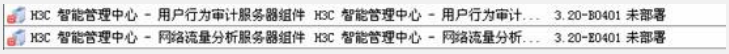
冯斯毅 2008-09-16 发表

> **iMC NTA/UBA组件无法查看流量日志时的解决思路**

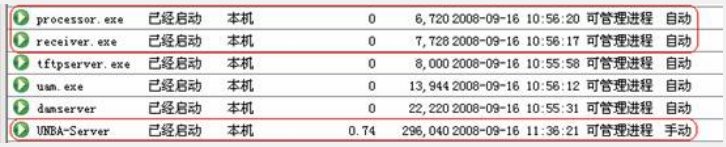
注意：
如果是分布式部署，则应该在部署UBA和NTA组件的服务器上进行以下操作

1. 查看NTA和UBA组件安装部署是否正常
在部署监控代理中检查



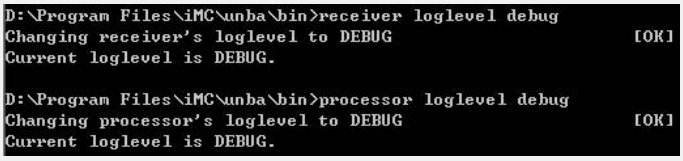


在iMC进程中检查processor.exe和receiver.exe，UNBA-Server.exe是否都正常运行。

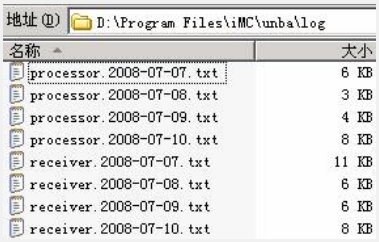


如果出现如下图标则表明相关进程没有运行失败。

2. 检查iMC服务器是否收到报文。
可以在服务器安装抓包软件，或者打开服务器调试日志分析，方法如下：
命令行进入iMC安装目录\unba\bin，执行receiver loglevel debug和processor loglevel debug



一段时间后，打开日志文件iMC安装目录\unba\log，找到当天的日志receiver.****.txt和processor.****.txt



其中会记录服务器每一个收发的报文

注意：
收集完信息以后，请通过receiver loglevel warning和processor loglevel warning将日志级别恢复到默认。

3. 检查服务器端口是否被占用
命令行输入netstat –a，可以看到当前所有活动端口。默认情况，端口是9020/9021。

```
C:\Documents and Settings\f5089>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    h3c-9942011015:epmap   h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:microsoft-ds  h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:2967    h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:3389    h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:9090    h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:netbios-ssn  h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:1655    10.153.50.87:microsoft-ds  ESTABLISHED
  TCP    h3c-9942011015:1026    h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:1036    h3c-9942011015:0       LISTENING
  TCP    h3c-9942011015:epmap   h3c-9942011015:0       LISTENING       0
  UDP    h3c-9942011015:microsoft-ds  *:*
```

如果想查看是什么进程占用某个端口，可以使用netstat –ab命令（此命令仅对2003/XP有效）

```
C:\Documents and Settings\f5089>netstat -ab

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    h3c-9942011015:epmap   h3c-9942011015:0       LISTENING       1312
  c:\windows\system32\WS2_32.dll
  C:\WINDOWS\system32\RPCRT4.dll
  c:\windows\system32\rpcss.dll
  C:\WINDOWS\system32\svchost.exe
  -- 未知组件 --
  [svchost.exe]

  TCP    h3c-9942011015:microsoft-ds  h3c-9942011015:0       LISTENING       4
  [System]

  TCP    h3c-9942011015:2967    h3c-9942011015:0       LISTENING       1704
  [Rtvscan.exe]
```

4. 检查数据库中是否产生原始数据表

在开始菜单中找到sqlserver 企业管理器（这个只针对SQL Server2000）

在左边的树上找到unba_slave数据库，在“表”中找到形如tbl_nat_yymmddhh(NAT 日志)或tbl_nets_yymmddhh（DIG和netstream日志），其中yymmddhh是8位数字，代表年月日小时，例如08071016表示2008年7月10日下午16点。正常情况应该实时产生最新的表，查看是否有当前的表。

NTA和UBA最常见的问题是时区问题和接口索引问题。

5. 如何判断是否有时区问题

承上，一般来说，每到一个正点，服务器就应该产生这个小时的原始表。

如果最新的表时间与当前时间不吻合，则说明极可能存在时区问题。

最典型的情况是，表的时间与当前时间相差8小时（因为中国在东八区），这就是最典型的时区问题。

时区问题的解决方法是，
在服务器上调整设备时区，并重新下发配置。

6. 如何判断是否有接口索引问题

打开unba_slave数据库中的tbl_unba_interface表，方法如下

看看其中if_index在原始表的if_index列和of_index列中是否存在。

if_index	if_name
1	Aux0 Interface
2	Encrypt11/0 Int
3	GigabitEthernet
4	GigabitEthernet
5	NULL0 Interface
6	GigabitEthernet
10	Analogmodem3/0
11	Serial4/0 Inter
13	Ethernet8/0 Int
14	Ethernet8/1 Int
15	Ethernet8/2 Int
16	Ethernet8/3 Int
17	Ethernet8/4 Int
18	Ethernet8/5 Int
19	Ethernet8/6 Int

注意：如果是交换机作netstream日志，服务器上只能添加三层端口，如要监控电口，则必须添加电口所在的vlan interface。