

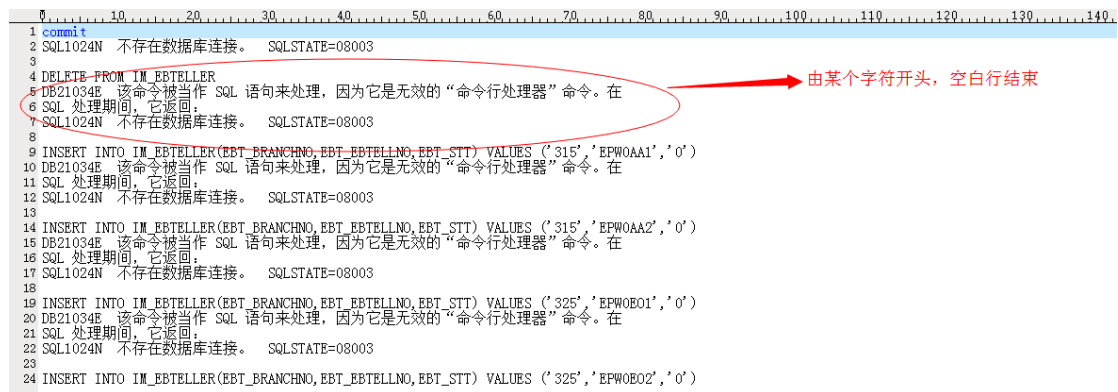
第一轮日志解析的总结

一、 日志的几种类型：

1. 段落式

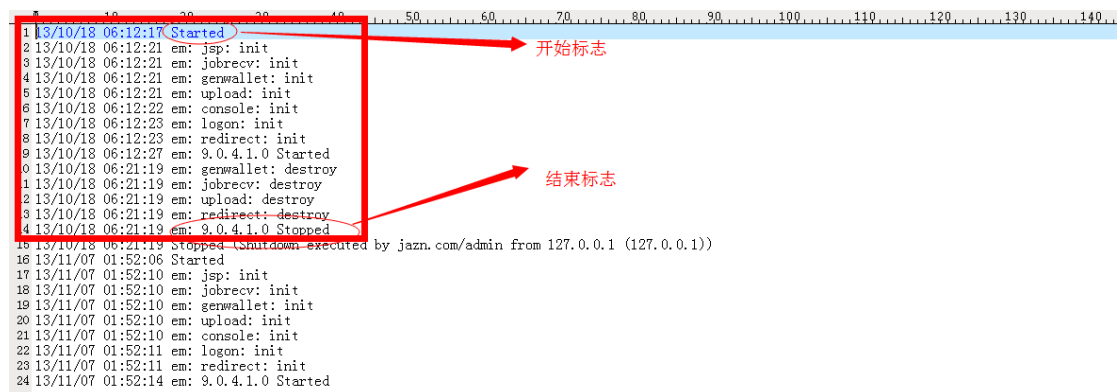
段落式的特点是，有某种特殊的标记开头，中间有多行日志，其中多行日志都是内容相关的，然后按照标记结束（通常都是一个空白行或者是某种结束标记）

log2.log



```
1 commit
2 SQL1024N 不存在数据库连接。 SQLSTATE=08003
3
4 DELETE FROM IM_EBTELLER
5 DB21034E 该命令被当作 SQL 语句来处理，因为它是无效的“命令行处理器”命令。在
6 SQL 处理期间，它返回。
7 SQL1024N 不存在数据库连接。 SQLSTATE=08003
8
9 INSERT INTO IM_EBTELLER(EBT_BRANCHNO,EBT_EBTELLNO,EBT_STT) VALUES ('315','EPW0AA1','0')
10 DB21034E 该命令被当作 SQL 语句来处理，因为它是无效的“命令行处理器”命令。在
11 SQL 处理期间，它返回。
12 SQL1024N 不存在数据库连接。 SQLSTATE=08003
13
14 INSERT INTO IM_EBTELLER(EBT_BRANCHNO,EBT_EBTELLNO,EBT_STT) VALUES ('315','EPW0AA2','0')
15 DB21034E 该命令被当作 SQL 语句来处理，因为它是无效的“命令行处理器”命令。在
16 SQL 处理期间，它返回。
17 SQL1024N 不存在数据库连接。 SQLSTATE=08003
18
19 INSERT INTO IM_EBTELLER(EBT_BRANCHNO,EBT_EBTELLNO,EBT_STT) VALUES ('325','EPW0E01','0')
20 DB21034E 该命令被当作 SQL 语句来处理，因为它是无效的“命令行处理器”命令。在
21 SQL 处理期间，它返回。
22 SQL1024N 不存在数据库连接。 SQLSTATE=08003
23
24 INSERT INTO IM_EBTELLER(EBT_BRANCHNO,EBT_EBTELLNO,EBT_STT) VALUES ('325','EPW0E02','0')
```

em-application.log



```
1 13/10/18 06:12:17 Started
2 13/10/18 06:12:21 em: jsp: init
3 13/10/18 06:12:21 em: jobrecv: init
4 13/10/18 06:12:21 em: genwallet: init
5 13/10/18 06:12:21 em: upload: init
6 13/10/18 06:12:22 em: console: init
7 13/10/18 06:12:23 em: logon: init
8 13/10/18 06:12:23 em: redirect: init
9 13/10/18 06:12:27 em: 9.0.4.1.0 Started
10 13/10/18 06:21:19 em: genwallet: destroy
11 13/10/18 06:21:19 em: jobrecv: destroy
12 13/10/18 06:21:19 em: upload: destroy
13 13/10/18 06:21:19 em: redirect: destroy
14 13/10/18 06:21:19 em: 9.0.4.1.0 Stopped
15 13/10/18 06:21:19 Stopped (Shutdown executed by jazn.com/admin from 127.0.0.1 (127.0.0.1))
16 13/11/07 01:52:06 Started
17 13/11/07 01:52:10 em: jsp: init
18 13/11/07 01:52:10 em: jobrecv: init
19 13/11/07 01:52:10 em: genwallet: init
20 13/11/07 01:52:10 em: upload: init
21 13/11/07 01:52:10 em: console: init
22 13/11/07 01:52:11 em: logon: init
23 13/11/07 01:52:11 em: redirect: init
24 13/11/07 01:52:14 em: 9.0.4.1.0 Started
```

sqlnet.log

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\1
VERSION INFORMATION:
TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
Time: 06-11月-2013 16:35:51
Tracing not turned on.
Tns error struct:
  ns main err code: 12543
  TNS-12543: TNS: 无法连接目标主机
  ns secondary err code: 12560
  nt main err code: 513
  TNS-00513: 不能连接的终点主机
  nt secondary err code: 51
  nt OS err code: 0
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\1

```

Udev.log

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
1 monitor will print the received events for:
2 UDEV - the event which udev sends out after rule processing
3 KERNEL - the kernel uevent
4
5 KERNEL[6.805881] add /devices/LNXSYSTM:00 (acpi)
6 ACTION=add
7 DEVPATH=/devices/LNXSYSTM:00
8 MODALIAS=acpi:LNXSYSTM:
9 SEQNUM=1421
10 SUBSYSTEM=acpi
11 UDEV_LOG=3
12
13 KERNEL[6.805894] add /devices/LNXSYSTM:00/LNXCPU:00 (acpi)
14 ACTION=add
15 DEVPATH=/devices/LNXSYSTM:00/LNXCPU:00
16 DRIVER=processor
17 MODALIAS=acpi:LNXCPU:
18 SEQNUM=1422
19 SUBSYSTEM=acpi
20 UDEV_LOG=3
21
22 KERNEL[6.805901] add /devices/LNXSYSTM:00/LNXCPU:01 (acpi)
23 ACTION=add
24 DEVPATH=/devices/LNXSYSTM:00/LNXCPU:01

```

2. 头部固定式

头部固定式，是比较常见的一种日志格式，特点是，一条记录由几个字段构成，其中前面几个字段的形式都是固定的，例如都是日期+线程号+级别+内容组成。其中最后的内容可以是一行也可以是多行。

defmsg.log

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
2013-11-29 22:08:10 [00001812 : 00001828] open \\.\DgSafe ok.
2013-11-29 22:08:10 [00001812 : 00001828] open device succeeded.
2013-11-29 22:08:10 [00001812 : 00001828] register event succeeded.
2013-11-29 22:17:52 [00001812 : 00001816] open \\.\DgSafe ok.
2013-11-29 22:17:52 [00001812 : 00001816] open device succeeded.
2013-11-29 22:17:52 [00001812 : 00001816] register event succeeded.
2013-11-29 22:29:27 [00001816 : 00001888] open \\.\DgSafe ok.
2013-11-29 22:29:27 [00001816 : 00001888] open device succeeded.
2013-11-29 22:29:27 [00001816 : 00001888] register event succeeded.
2013-11-29 22:39:32 [00003312 : 00005780] open \\.\DgSafe ok.
2013-11-29 22:39:32 [00003312 : 00005780] open device succeeded.
2013-11-29 22:39:32 [00003312 : 00005780] register event succeeded.
2013-11-29 23:01:24 [00003312 : 00004272] open \\.\DgSafe ok.
2013-11-29 23:01:24 [00003312 : 00004272] open device succeeded.
2013-11-29 23:01:24 [00003312 : 00004272] register event succeeded.
2013-11-29 23:03:18 [00002804 : 00003928] open \\.\DgSafe ok.
2013-11-29 23:03:18 [00002804 : 00003928] open device succeeded.
2013-11-29 23:03:18 [00002804 : 00003928] register event succeeded.
2013-11-29 23:54:20 [00002804 : 00002824] open \\.\DgSafe ok.
2013-11-29 23:54:20 [00002804 : 00002824] open device succeeded.
2013-11-29 23:54:20 [00002804 : 00002824] register event succeeded.
2013-11-29 23:55:45 [00002244 : 00002268] open \\.\DgSafe ok.
2013-11-29 23:55:45 [00002244 : 00002268] open device succeeded.
2013-11-29 23:55:45 [00002244 : 00002268] register event succeeded.

```

tomcat.log

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
1 2012.09.19 18:15:04 ERROR Digest(1472):? Parse Fatal Error at line 0 column 0: The encoding "GBK" is not supported.
2 org.xml.sax.SAXParseException: The encoding "GBK" is not supported.
3 at org.apache.xerces.framework.XMLParser.reportError(XMLParser.java:1213)
4 at org.apache.xerces.readers.DefaultEntityHandler.startReadingFromDocument(DefaultEntityHandler.java:546)
5 at org.apache.xerces.framework.XMLParser.parseSourceEntity(XMLParser.java:314)
6 at org.apache.xerces.framework.XMLParser.parse(XMLParser.java:1087)
7 at org.apache.tomcat.util.digester.Digester.parse(Digester.java:190)
8 at org.apache.catalina.startup.ContextConfig.applicationConfig(ContextConfig.java:339)
9 at org.apache.catalina.startup.ContextConfig.start(ContextConfig.java:1031)
10 at org.apache.catalina.startup.ContextConfig.lifecycleEvent(ContextConfig.java:255)
11 at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119)
12 at org.apache.catalina.core.StandardContext.start(StandardContext.java:4053)
13 at org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBase.java:759)
14 at org.apache.catalina.core.ContainerBase.addChild(ContainerBase.java:739)
15 at org.apache.catalina.core.StandardHost.addChild(StandardHost.java:524)
16 at org.apache.catalina.startup.HostConfig.deployDescriptor(HostConfig.java:589)
17 at org.apache.catalina.startup.HostConfig.deployDescriptors(HostConfig.java:536)
18 at org.apache.catalina.startup.HostConfig.deployApps(HostConfig.java:471)
19 at org.apache.catalina.startup.HostConfig.start(HostConfig.java:1102)
20 at org.apache.catalina.startup.HostConfig.lifecycleEvent(HostConfig.java:311)
21 at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119)
22 at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1020)
23 at org.apache.catalina.core.StandardHost.start(StandardHost.java:713)
24 at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1012)

```

3. 表格式

这种形式的日志，类似于一个表格，分为有表头的与无表头的两种。有表头的会在日志中，包括一个对每个字段的说明。无表头的则只包含数据。

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
1 Active Internet connections (only servers)
2 Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
3 tcp 0 0 0.0.0.0:445 0.0.0.0:* LISTEN -
4 tcp 0 0 0.0.0.0:993 0.0.0.0:* LISTEN -
5 tcp 0 0 0.0.0.0:995 0.0.0.0:* LISTEN -
6 tcp 0 0 0.0.0.0:902 0.0.0.0:* LISTEN -
7 tcp 0 0 0.0.0.0:12615 0.0.0.0:* LISTEN 6005/java
8 tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN -
9 tcp 0 0 0.0.0.0:6379 0.0.0.0:* LISTEN -
10 tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN -
11 tcp 0 0 0.0.0.0:110 0.0.0.0:* LISTEN -
12 tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN -
13 tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN -
14 tcp 0 0 0.192.168.122.1:53 0.0.0.0:* LISTEN -
15 tcp 0 0 0.10.1.1.227:53 0.0.0.0:* LISTEN -
16 tcp 0 0 0.127.0.0.1:53 0.0.0.0:* LISTEN -
17 tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN -
18 tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
19 tcp 0 0 0.127.0.0.1:631 0.0.0.0:* LISTEN -
20 tcp 0 0 0.0.0.0:5559 0.0.0.0:* LISTEN 6006/java
21 tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN -
22 tcp 0 0 0.0.0.0:5560 0.0.0.0:* LISTEN 6006/java
23 tcp 0 0 0.0.0.0:5561 0.0.0.0:* LISTEN 6006/java
24 tcp 0 0 0.127.0.0.1:953 0.0.0.0:* LISTEN -

```

last.log

```

0 10 20 30 40 50 60 70 80 90 100 110 120 130 140
1 monitor pts/6 10.1.1.112 Thu Mar 27 09:35 still logged in
2 monitor pts/5 10.1.1.112 Thu Mar 27 09:14 - 09:16 (00:02)
3 monitor pts/3 10.1.1.155 Thu Mar 27 07:09 still logged in
4 monitor pts/2 10.1.1.244 Thu Mar 27 07:03 still logged in
5 monitor pts/5 10.1.1.119 Wed Mar 26 07:22 - 11:37 (04:15)
6 monitor pts/4 10.1.1.159 Wed Mar 26 04:07 - 11:34 (07:26)
7 monitor pts/3 10.1.1.155 Wed Mar 26 03:32 - 13:44 (10:12)
8 monitor pts/2 whosyourdaddy.lo Wed Mar 26 03:32 - 13:44 (10:11)
9 monitor pts/6 10.1.1.159 Tue Mar 25 05:37 - 11:36 (05:59)
10 monitor pts/5 whosyourdaddy.lo Tue Mar 25 03:35 - 13:06 (09:31)
11 monitor pts/4 whosyourdaddy.lo Tue Mar 25 03:35 - 11:47 (08:11)
12 monitor pts/3 10.1.1.125 Tue Mar 25 03:33 - 11:34 (08:00)
13 monitor pts/2 10.1.1.156 Tue Mar 25 03:19 - 11:42 (08:22)
14 monitor pts/5 10.1.1.155 Mon Mar 24 09:27 - 13:46 (04:19)
15 monitor pts/4 10.1.1.116 Mon Mar 24 07:16 - 11:47 (04:31)
16 monitor pts/2 10.1.1.156 Mon Mar 24 05:28 - 11:43 (06:14)
17 monitor pts/3 10.1.1.155 Mon Mar 24 03:49 - 13:46 (09:56)
18 monitor pts/2 10.1.1.156 Mon Mar 24 02:58 - 05:27 (02:28)
19 monitor pts/3 10.1.1.244 Fri Mar 21 11:19 - 11:47 (00:27)
20 monitor pts/10 10.1.1.156 Fri Mar 21 09:26 - 11:45 (02:18)
21 monitor pts/9 10.1.1.155 Fri Mar 21 09:21 - 11:37 (02:16)
22 monitor pts/8 10.1.1.155 Fri Mar 21 09:20 - 13:30 (04:10)
23 monitor pts/6 10.1.1.155 Fri Mar 21 09:19 - 13:30 (04:11)
24 monitor pts/6 10.1.1.155 Fri Mar 21 09:19 - 09:19 (00:00)

```

4. 重复式

字段以某种相同的形式重复。

vmenu.log

No	field1	field2	field3	field4
1	13/10/18 06:12:17	13/10/18 06:12:21 em: jsp: init 13/10/18 06:12:21 em: jobrecv: init 13/10/18 06:12:21 em: genwallet: init 13/10/18 06:12:21 em: upload: init 13/10/18 06:12:22 em: console: init 13/10/18 06:12:23 em: logon: init 13/10/18 06:12:23 em: redirect: init 13/10/18 06:12:27 em: 9.0.4.1.0 Started 13/10/18 06:21:19 em: genwallet: destroy 13/10/18 06:21:19 em: jobrecv: destroy 13/10/18 06:21:19 em: upload: destroy 13/10/18 06:21:19 em: redirect: destroy 13/10/18 06:21:19 em: 9.0.4.1.0 Stopped	13/10/18 06:21:19	Shutdown executed by jazn.com/admin from 127.0.0.1 (127.0.0.1)
2	13/11/07 01:52:06	13/11/07 01:52:10 em: jsp: init 13/11/07 01:52:10 em: jobrecv: init 13/11/07 01:52:10 em: genwallet: init 13/11/07 01:52:10 em: upload: init 13/11/07 01:52:10 em: console: init 13/11/07 01:52:11 em: logon: init 13/11/07 01:52:11 em: redirect: init 13/11/07 01:52:14 em: 9.0.4.1.0 Started 13/11/07 03:02:22 em: genwallet: destroy 13/11/07 03:02:22 em: jobrecv: destroy 13/11/07 03:02:22 em: upload: destroy 13/11/07 03:02:22 em: redirect: destroy 13/11/07 03:02:22 em: 9.0.4.1.0 Stopped	13/11/07 03:02:22	JVM termination

sqlnet.log

```

*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator))))
  VERSION INFORMATION:
  TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
  Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
  Time: 06-11月-2013 16:35:51
  Tracing not turned on.
  Tns error struct:
    ns main err code: 12543
      TNS-12543: TNS: 无法连接目标主机
    ns secondary err code: 12560
    nt main err code: 513
      TNS-00513: 不能连接的终点主机
    nt secondary err code: 51
    nt OS err code: 0
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator))))
  VERSION INFORMATION:
  TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
  Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
  Time: 06-11月-2013 16:35:51
  Tracing not turned on.
  Tns error struct:
    ns main err code: 12543
      TNS-12543: TNS: 无法连接目标主机
    ns secondary err code: 12560
    nt main err code: 513
      TNS-00513: 不能连接的终点主机
    nt secondary err code: 51
    nt OS err code: 0
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator))))
  VERSION INFORMATION:
  TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
  Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
  Time: 06-11月-2013 16:35:51
  Tracing not turned on.
  Tns error struct:
    ns main err code: 12543
      TNS-12543: TNS: 无法连接目标主机
    ns secondary err code: 12560
    nt main err code: 513
      TNS-00513: 不能连接的终点主机
    nt secondary err code: 51
    nt OS err code: 0
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator))))
  VERSION INFORMATION:
  TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
  Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
  Time: 06-11月-2013 16:35:51
  Tracing not turned on.
  Tns error struct:
    ns main err code: 12543
      TNS-12543: TNS: 无法连接目标主机
    ns secondary err code: 12560
    nt main err code: 513
      TNS-00513: 不能连接的终点主机
    nt secondary err code: 51
    nt OS err code: 0
*****
Fatal NI connect error 12543, connecting to:
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator))))
  VERSION INFORMATION:
  TNS for 32-bit Windows: Version 10.2.0.1.0 - Production
  Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production
  Time: 06-11月-2013 16:35:51
  Tracing not turned on.
  Tns error struct:
    ns main err code: 12543
      TNS-12543: TNS: 无法连接目标主机
    ns secondary err code: 12560
    nt main err code: 513
      TNS-00513: 不能连接的终点主机
    nt secondary err code: 51
    nt OS err code: 0
*****

```

field1

Fatal NI connect error 12543, connecting to: (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator)))) VERSION INFORMATION: TNS for 32-bit Windows: Version 10.2.0.1.0 - Production Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production Time: 06-11月-2013 16:35:51 Tracing not turned on. Tns error struct: ns main err code: 12543 TNS-12543: TNS: 无法连接目标主机 ns secondary err code: 12560 nt main err code: 513 TNS-00513: 不能连接的终点主机 nt secondary err code: 51 nt OS err code: 0

Fatal NI connect error 12543, connecting to: (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator)))) VERSION INFORMATION: TNS for 32-bit Windows: Version 10.2.0.1.0 - Production Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production Time: 06-11月-2013 16:36:05 Tracing not turned on. Tns error struct: ns main err code: 12543 TNS-12543: TNS: 无法连接目标主机 ns secondary err code: 12560 nt main err code: 513 TNS-00513: 不能连接的终点主机 nt secondary err code: 51 nt OS err code: 0

Fatal NI connect error 12543, connecting to: (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.1.200)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=test)(CID=(PROGRAM=F:\Database\oracle\product\10.2.0.1\jdk\jre\bin\java.exe)(HOST=RAOLIANG)(USER=Administrator)))) VERSION INFORMATION: TNS for 32-bit Windows: Version 10.2.0.1.0 - Production Windows NT TCP/IP NT Protocol Adapter for 32-bit Windows: Version 10.2.0.1.0 - Production Time: 06-11月-2013 16:35:54 Tracing not turned on. Tns error struct: ns main err code: 12543 TNS-12543: TNS: 无法连接目标主机 ns secondary err code: 12560 nt main err code: 513 TNS-00513: 不能连接的终点主机 nt secondary err code: 51 nt OS err code: 0

2. 头部固定式

能够做到的：能够在日志中，很准确的识别此记录；

能够准确的提取，头部字段中的值；

能够获得不固定的尾部的文本信息。

不能做到的：无法对尾部的信息做出进一步的提取与分解。

defmsg.log

```

2013-11-29 22:08:10 [00001812 : 00001828] open \\.\DgSafe ok.
2013-11-29 22:08:10 [00001812 : 00001828] open device succeeded.
2013-11-29 22:08:10 [00001812 : 00001828] register event succeeded.
2013-11-29 22:17:52 [00001812 : 00001816] open \\.\DgSafe ok.
2013-11-29 22:17:52 [00001812 : 00001816] open device succeeded.
2013-11-29 22:17:52 [00001812 : 00001816] register event succeeded.
2013-11-29 22:29:27 [00001816 : 00001888] open \\.\DgSafe ok.
2013-11-29 22:29:27 [00001816 : 00001888] open device succeeded.
2013-11-29 22:29:27 [00001816 : 00001888] register event succeeded.
2013-11-29 22:39:32 [00003312 : 00005780] open \\.\DgSafe ok.
2013-11-29 22:39:32 [00003312 : 00005780] open device succeeded.
2013-11-29 22:39:32 [00003312 : 00005780] register event succeeded.
2013-11-29 23:01:24 [00003312 : 00004272] open \\.\DgSafe ok.
2013-11-29 23:01:24 [00003312 : 00004272] open device succeeded.
2013-11-29 23:01:24 [00003312 : 00004272] register event succeeded.
2013-11-29 23:03:18 [00002804 : 00003928] open \\.\DgSafe ok.
2013-11-29 23:03:18 [00002804 : 00003928] open device succeeded.
2013-11-29 23:03:18 [00002804 : 00003928] register event succeeded.
2013-11-29 23:54:20 [00002804 : 00002824] open \\.\DgSafe ok.
2013-11-29 23:54:20 [00002804 : 00002824] open device succeeded.
2013-11-29 23:54:20 [00002804 : 00002824] register event succeeded.
2013-11-29 23:55:45 [00002244 : 00002268] open \\.\DgSafe ok.
2013-11-29 23:55:45 [00002244 : 00002268] open device succeeded.
2013-11-29 23:55:45 [00002244 : 00002268] register event succeeded.

```

No	field1	field2	field3	field4	field5
1	2013-11-29	22:08:10	00001812	00001828	open \\.\DgSafe ok.
2	2013-11-29	22:08:10	00001812	00001828	open device succeeded.
3	2013-11-29	22:08:10	00001812	00001828	register event succeeded.
4	2013-11-29	22:17:52	00001812	00001816	open \\.\DgSafe ok.
5	2013-11-29	22:17:52	00001816	00001816	open device succeeded.
6	2013-11-29	22:17:52	00001812	00001816	register event succeeded.
7	2013-11-29	22:29:27	00001816	00001888	open \\.\DgSafe ok.
8	2013-11-29	22:29:27	00001816	00001888	open device succeeded.
9	2013-11-29	22:29:27	00001816	00001888	register event succeeded.

tomcat.log

No	field1	field2	field3	field4	field5
1	2012.09.19 18:15:04	ERROR	Digester(1472):?	Parse Fatal Error at line 0 column 0: The encoding "GBK" is not supported.	
2	org.xml.sax.SAXParseException: The encoding "GBK" is not supported.				
3	at org.apache.xerces.framework.XMLParser.reportError(XMLParser.java:1213)				
4	at org.apache.xerces.readers.DefaultEntityHandler.startReadingFromDocument(DefaultEntityHandler.java:546)				
5	at org.apache.xerces.framework.XMLParser.parseSomeSetup(XMLParser.java:314)				
6	at org.apache.xerces.framework.XMLParser.parse(XMLParser.java:1097)				
7	at org.apache.tomcat.util.digester.Digester.parse(Digester.java:1561)				
8	at org.apache.catalina.startup.ContextConfig.applicationWebConfig(ContextConfig.java:339)				
9	at org.apache.catalina.startup.ContextConfig.start(ContextConfig.java:1031)				
10	at org.apache.catalina.startup.ContextConfig.lifecycleEvent(ContextConfig.java:255)				
11	at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119)				
12	at org.apache.catalina.core.StandardContext.start(StandardContext.java:4053)				
13	at org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBase.java:759)				
14	at org.apache.catalina.core.ContainerBase.addChild(ContainerBase.java:739)				
15	at org.apache.catalina.core.StandardHost.addChild(StandardHost.java:524)				
16	at org.apache.catalina.startup.HostConfig.deployDescriptor(HostConfig.java:589)				
17	at org.apache.catalina.startup.HostConfig.deployDescriptors(HostConfig.java:536)				
18	at org.apache.catalina.startup.HostConfig.deployApps(HostConfig.java:471)				
19	at org.apache.catalina.startup.HostConfig.start(HostConfig.java:1102)				
20	at org.apache.catalina.startup.HostConfig.lifecycleEvent(HostConfig.java:311)				
21	at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119)				
22	at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1020)				
23	at org.apache.catalina.core.StandardHost.start(StandardHost.java:718)				
24	at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1012)				

No	field1	field2	field3	field4	field5
1	2012.09.19 18:15:04	ERROR	Digester(1472):?	Parse Fatal Error at line 0 column 0: The encoding "GBK" is not supported.	org.xml.sax.SAXParseException: The encoding "GBK" is not supported. at org.apache.xerces.framework.XMLParser.reportError(XMLParser.java:1213) at org.apache.xerces.readers.DefaultEntityHandler.startReadingFromDocument(DefaultEntityHandler.java:546) at org.apache.xerces.framework.XMLParser.parseSomeSetup(XMLParser.java:314) at org.apache.xerces.framework.XMLParser.parse(XMLParser.java:1097) at org.apache.tomcat.util.digester.Digester.parse(Digester.java:1561) at org.apache.catalina.startup.ContextConfig.applicationWebConfig(ContextConfig.java:339) at org.apache.catalina.startup.ContextConfig.start(ContextConfig.java:1031) at org.apache.catalina.startup.ContextConfig.lifecycleEvent(ContextConfig.java:255) at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119) at org.apache.catalina.core.StandardContext.start(StandardContext.java:4053) at org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBase.java:759) at org.apache.catalina.core.ContainerBase.addChild(ContainerBase.java:739) at org.apache.catalina.core.StandardHost.addChild(StandardHost.java:524) at org.apache.catalina.startup.HostConfig.deployDescriptor(HostConfig.java:589) at org.apache.catalina.startup.HostConfig.deployDescriptors(HostConfig.java:536) at org.apache.catalina.startup.HostConfig.deployApps(HostConfig.java:471) at org.apache.catalina.startup.HostConfig.start(HostConfig.java:1102) at org.apache.catalina.startup.HostConfig.lifecycleEvent(HostConfig.java:311) at org.apache.catalina.util.LifecycleSupport.fireLifecycleEvent(LifecycleSupport.java:119) at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1020) at org.apache.catalina.core.StandardHost.start(StandardHost.java:718) at org.apache.catalina.core.ContainerBase.start(ContainerBase.java:1012) at org.apache.catalina.core.StandardEngine.start(StandardEngine.java:442) at org.apache.catalina.core.StandardService.start(StandardService.java:450) at org.apache.catalina.core.StandardServer.start(StandardServer.java:683) at org.apache.catalina.startup.Catalina.start(Catalina.java:537) at

3. 表格式

能够做到的：能够很好的解析记录。

包含的 BUG：在左对齐与右对齐相邻的情况下，会出现解析错误的 bug；

在记录长度小于期望的长度（表头的长度），会出现空指针异常。

Last.log

[illegible]

4. 重复式

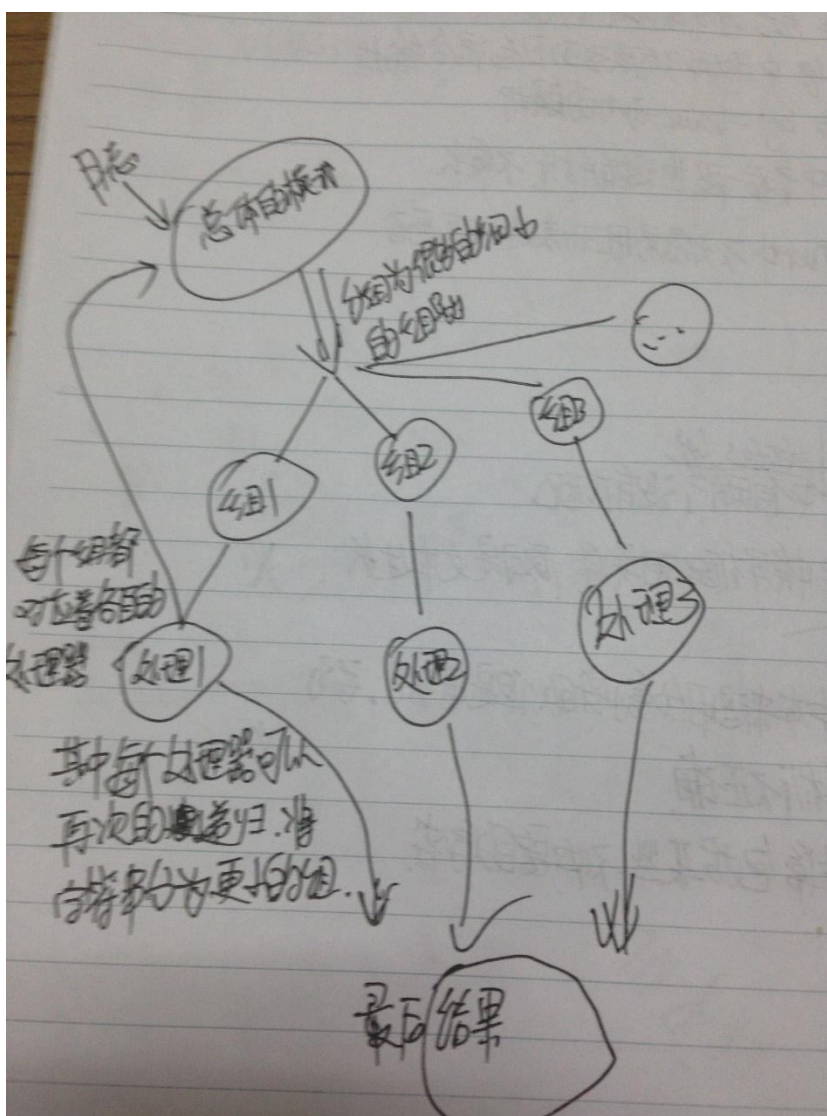
不能做到的：在此模式中，只要稍微有点点变化，都会出现不能匹配的情况；

base domain.log

field1	field2	field3	field4	field5	field6	field7	field8	field9	field10	field11	field12
2012-3-1 下午08:58分27秒 CST	Notice	Security	wolf-haiyi	AdminServer	[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)'	WLS Kernel			1330585107274	BEA-090082	Security initializing using security realm myrealm.
2012-3-1 下午08:58分28秒 CST	Notice	WebLogicServer	wolf-haiyi	AdminServer	main	WLS Kernel			1330585108870	BEA-000365	Server state changed to STANDBY
2012-3-1 下午08:58分28秒 CST	Notice	WebLogicServer	wolf-haiyi	AdminServer	main	WLS Kernel			1330585108870	BEA-000365	Server state changed to STARTING

三、 下个阶段的目标

1. 在原有的基础上，增加对每个字段进行单独处理的功能。
大体思路是这样的：



2. 解决掉表格解析器中两个 bug。
3. 优化重复式的配置。