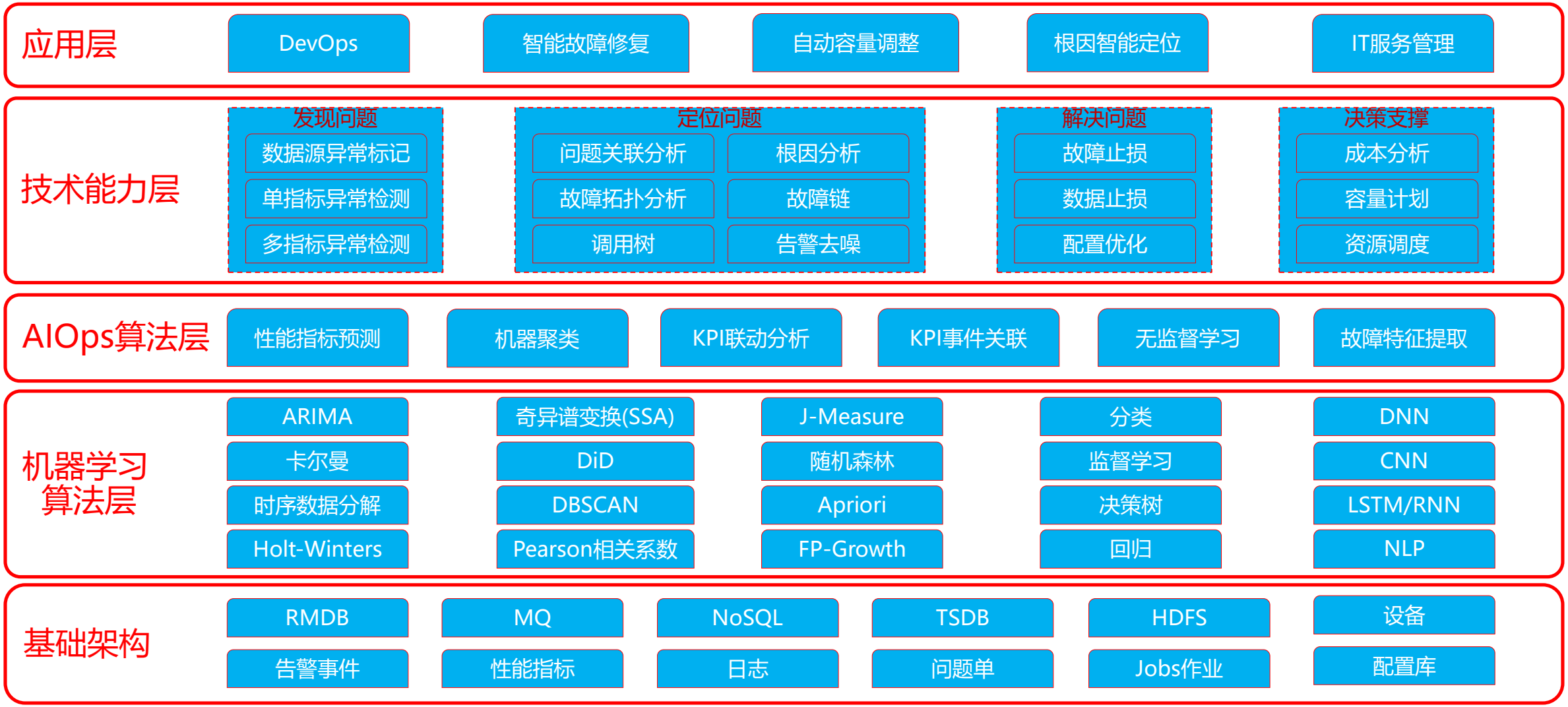
基于人工智能的数字化IT管理



IT运维之日常

传统运维关注	管理效果	问题出在哪儿?	解决方法
故障	故障的数量没有改善，甚至不断上升	缺少对问题和异常的洞察和预判，运维管理后知后觉。	1. 通过机器学习算法的辅助，提升对IT问题和异常的洞察力。 2. 通过机器预测，提升对性能故障的预警能力
配置	人为事故频发	对配置的属性以及合规性缺少洞察和管控。	1. 实时掌控IT配置的变化，洞察配置的属性及其关联关系。 2. 对配置的合规性进行管理，尽可能通过自动化手段进行配置，避免人为事故。
性能	用户体验难以控制，业务投诉多	缺少用户体验管理，同时缺乏性能与系统容量计划的管理	1. 通过成熟的技术实时监控用户端的操作和页面响应时延。 2. 实时洞察页面错误。 3. 构建应用性能和系统容量的模型，消除瓶颈
安全	各类木马和勒索病毒难以防范	缺少统一视图管理和查看各类安全事件。	1. 对各类型安全事件进行统一管理，统一分析，统一视图。 2. 通过规则库自动发现和定义高危操作，高危用户和高危资产。

IT运维之日常

传统运维关注	管理效果	问题出在哪儿?	解决方法
故障	故障的数量没有改善，甚至不断上升	缺少对问题和异常的洞察和预判，运维管理后知后觉。	1. 通过机器学习算法的辅助，提升对IT问题和异常的洞察力。 2. 通过机器预测，提升对性能故障的预警能力
配置	人为事故频发	对配置的属性以及合规性缺少洞察和管控。	1. 实时掌控IT配置的变化，洞察配置的属性及其关联关系。 2. 对配置的合规性进行管理，尽可能通过自动化手段进行配置，避免人为事故。
性能	用户体验难以控制，业务投诉多	缺少用户体验管理，同时缺乏性能与系统容量计划的管理	1. 通过成熟的技术实时监控用户端的操作和页面响应时延。 2. 实时洞察页面错误。 3. 构建应用性能和系统容量的模型，消除瓶颈
安全	各类木马和勒索病毒难以防范	缺少统一视图管理和查看各类安全事件。	1. 对各类型安全事件进行统一管理，统一分析，统一视图。 2. 通过规则库自动发现和定义高危操作，高危用户和高危资产。

IT运维之日常

传统运维关注	管理效果	问题出在哪儿?	解决方法
故障	故障的数量没有改善，甚至不断上升	缺少对问题和异常的洞察和预判，运维管理后知后觉。	1. 通过机器学习算法的辅助，提升对IT问题和异常的洞察力。 2. 通过机器预测，提升对性能故障的预警能力
配置	人为事故频发	对配置的属性以及合规性缺少洞察和管控。	1. 实时掌控IT配置的变化，洞察配置的属性及其关联关系。 2. 对配置的合规性进行管理，尽可能通过自动化手段进行配置，避免人为事故。
性能	用户体验难以控制，业务投诉多	缺少用户体验管理，同时缺乏性能与系统容量计划的管理	1. 通过成熟的技术实时监控用户端的操作和页面响应时延。 2. 实时洞察页面错误。 3. 构建应用性能和系统容量的模型，消除瓶颈
安全	各类木马和勒索病毒难以防范	缺少统一视图管理和查看各类安全事件。	1. 对各类型安全事件进行统一管理，统一分析，统一视图。 2. 通过规则库自动发现和定义高危操作，高危用户和高危资产。

IT运维之日常

传统运维关注	管理效果	问题出在哪儿?	解决方法
故障	故障的数量没有改善，甚至不断上升	缺少对问题和异常的洞察和预判，运维管理后知后觉。	1. 通过机器学习算法的辅助，提升对IT问题和异常的洞察力。 2. 通过机器预测，提升对性能故障的预警能力
配置	人为事故频发	对配置的属性以及合规性缺少洞察和管控。	1. 实时掌控IT配置的变化，洞察配置的属性及其关联关系。 2. 对配置的合规性进行管理，尽可能通过自动化手段进行配置，避免人为事故。
性能	用户体验难以控制，业务投诉多	缺少用户体验管理，同时缺乏性能与系统容量计划的管理	1. 通过成熟的技术实时监控用户端的操作和页面响应时延。 2. 实时洞察页面错误。 3. 构建应用性能和系统容量的模型，消除瓶颈
安全	各类木马和勒索病毒难以防范	缺少统一视图管理和查看各类安全事件。	1. 对各类型安全事件进行统一管理，统一分析，统一视图。 2. 通过规则库自动发现和定义高危操作，高危用户和高危资产。

Oracle Management Cloud 管理云

由统一大数据平台和机器学习驱动的实时运营洞察

- 用户体验/行为
- 应用
- 中间层
- 数据层
- 虚拟化层
- 基础设施层

ORACLE

- 云访问
  身份
  全局威胁汇集
- 真实用户
  复合用户
- 应用指标
  交易
- 服务器指标
  诊断日志
- 主机指标
  虚机指标
  容器指标
- 配置
  合规
  传票与报警
- 安全与网络
  事件

- 智能化
  统一平台
- 强大机器
  学习能力
- 全面完整的
  数据集
- 支持异构与开放

某客户生产日志智能分析

简单收集4种日志文件

WebLogic
Access Logs
83,878,896 条日志

WebLogic
Server Logs
1,084,007 条日志

Database
Alert Logs
810,720 条日志

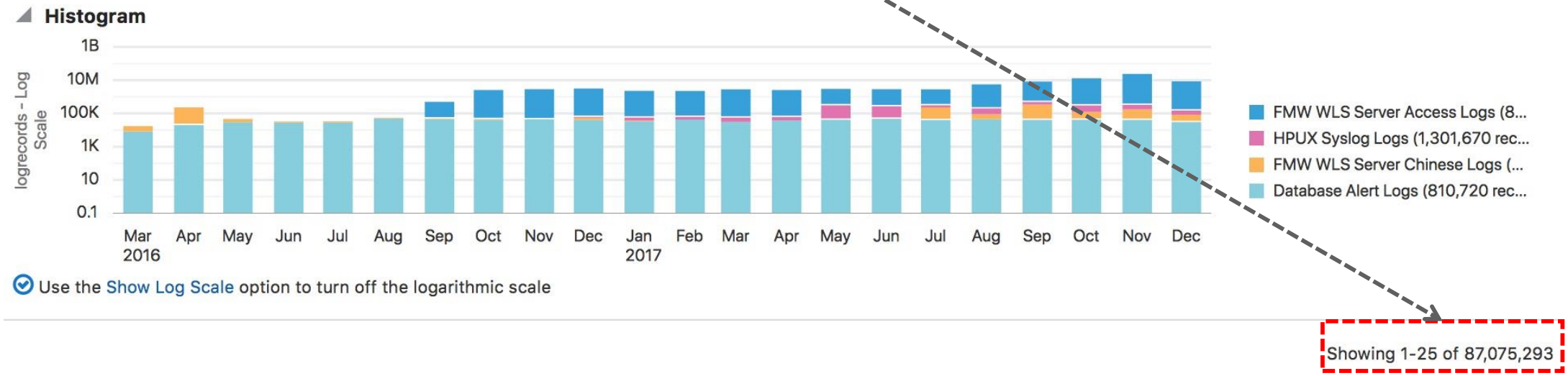
HPUX
Syslog
1,301,670 条日志

通过 OnDemand Upload (ODU) 的方法

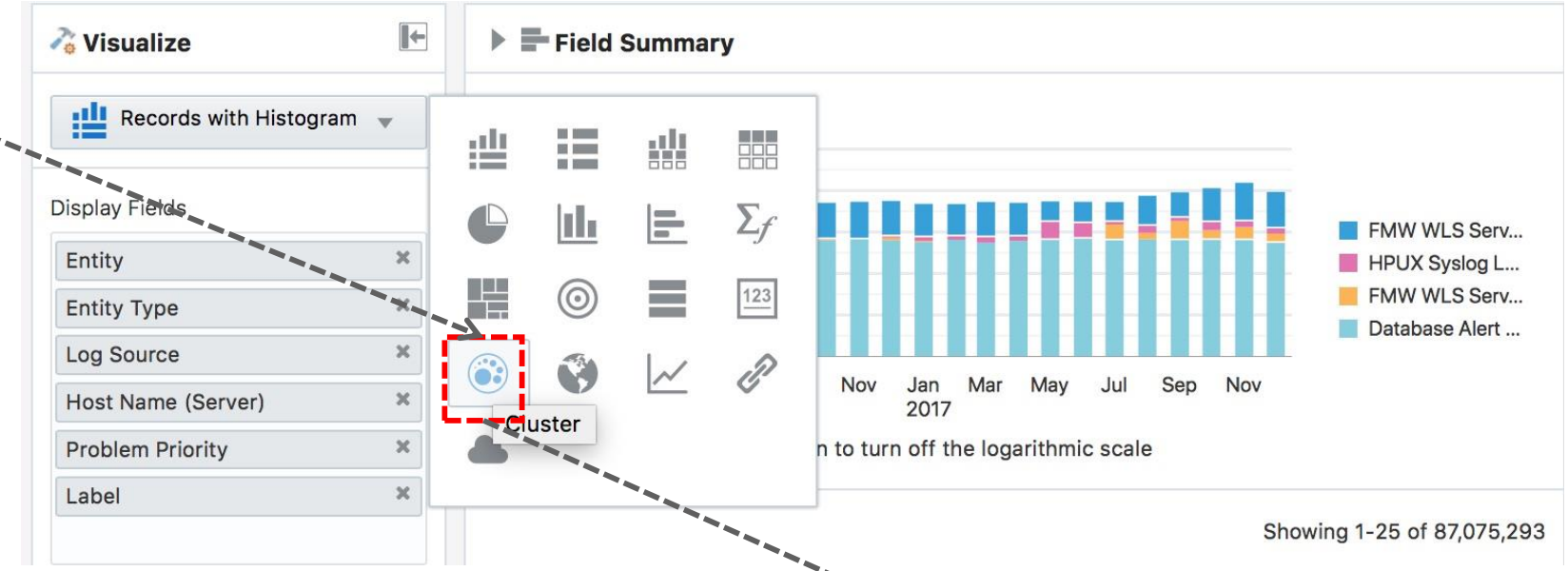
人工上载这3个日志文件

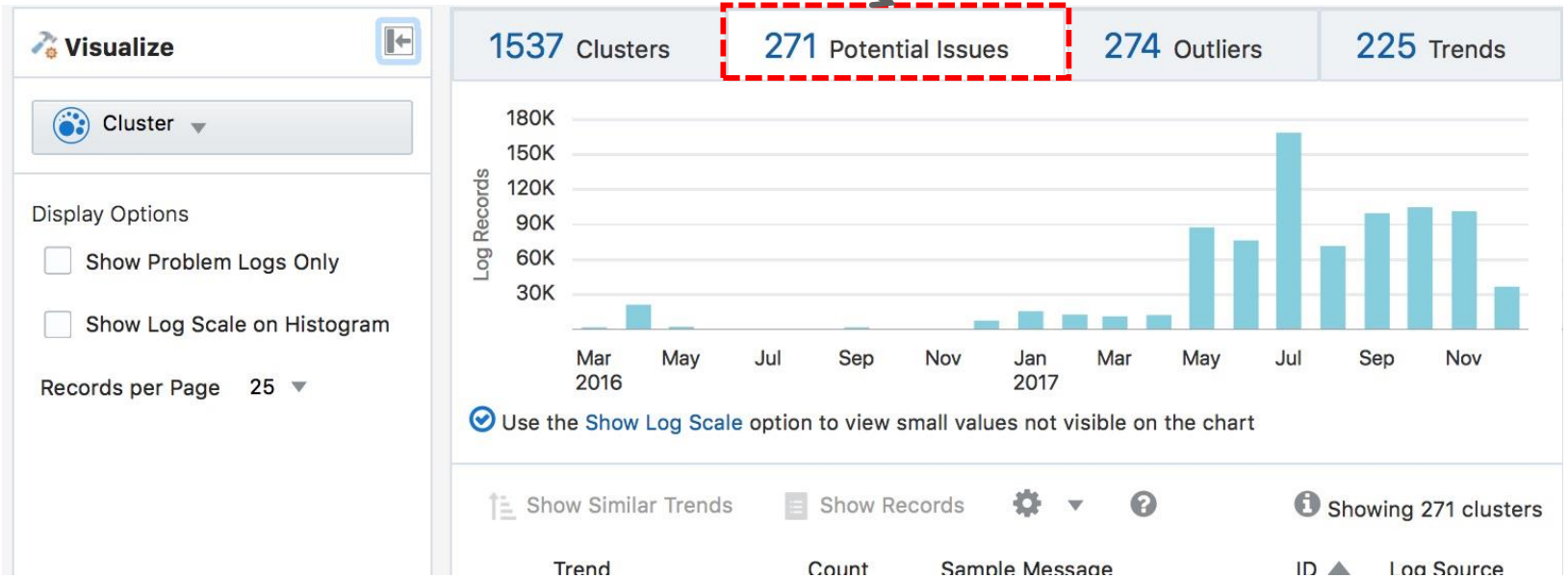
只使用了OMC七个模块中的日志分析模块

问题：在2016-3-1 到 2017-12-31里，共有8707万条日志，有什么潜在问题?



点击Cluster（机器学习的一种），OMC自动从8707万条日志万条日志里找到271个潜在问题





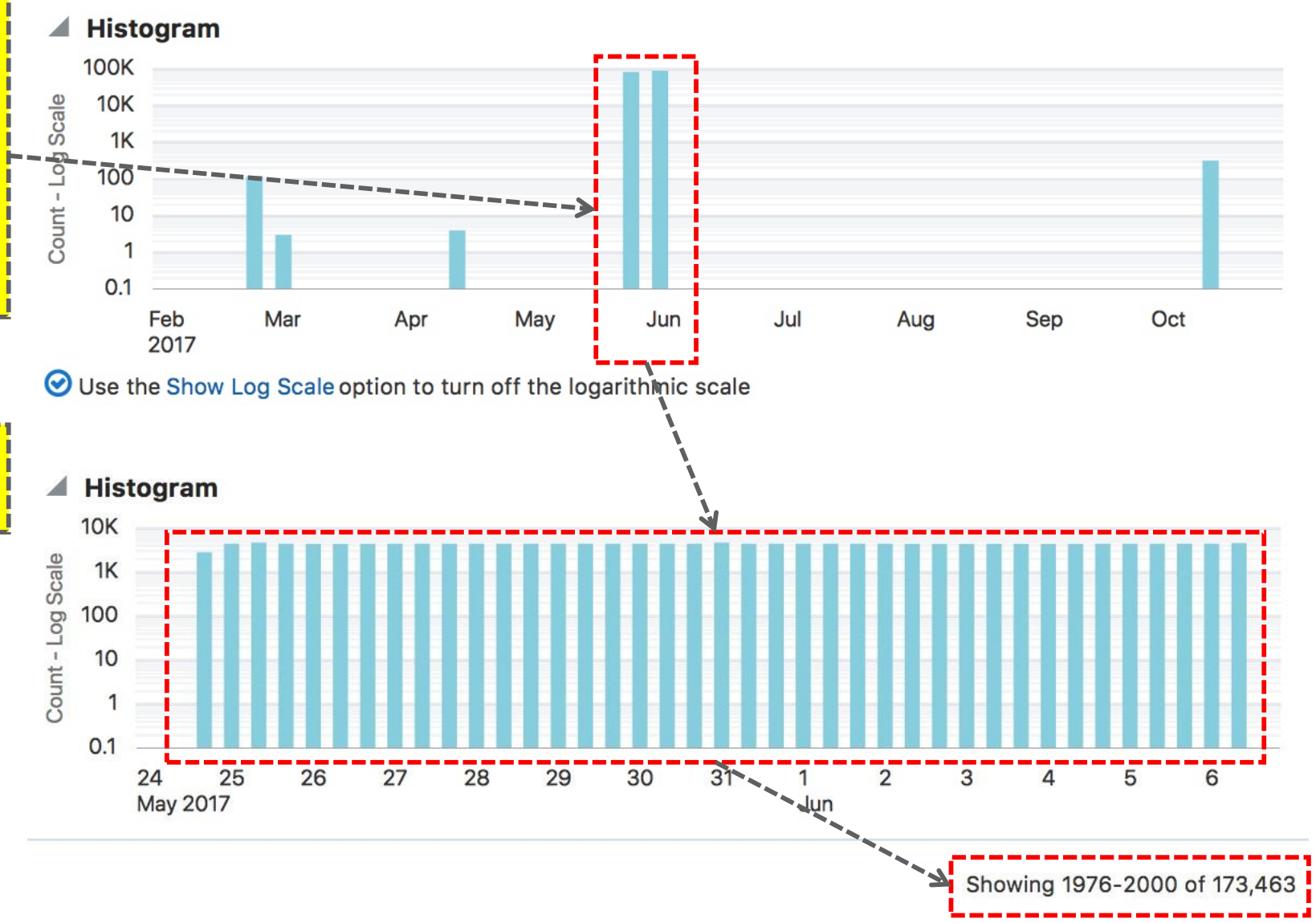
操作系统日志分析

176,519 **次无效用户登入**

主要集中在2017-5-24到2017-6-6，每天受到4,480次登入尝试攻击，共173,463次登入尝试攻击

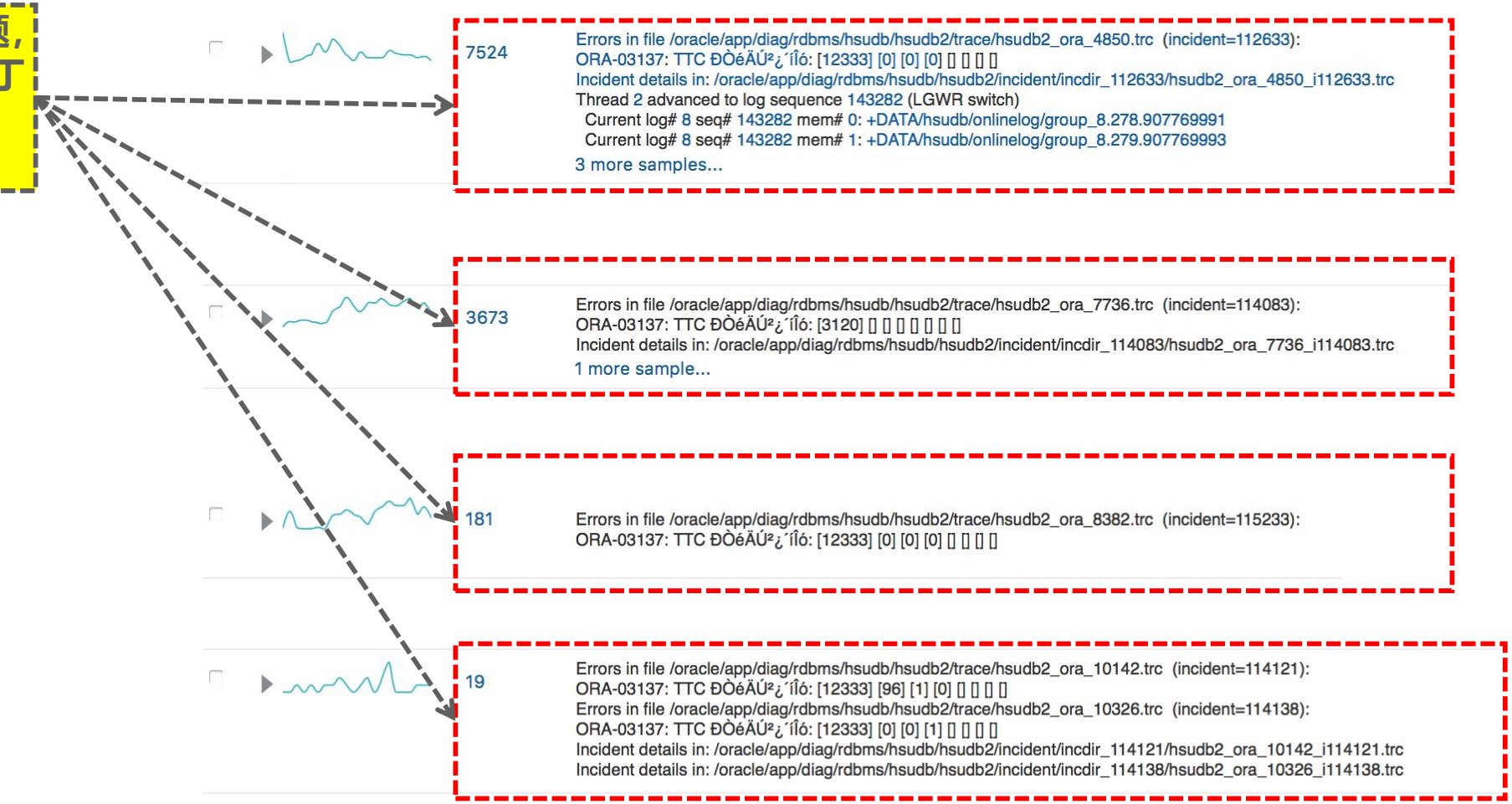
来源： 10.xxx.xxx.230
目标： xxx.xxx.49.11
账号： admin

建议设置告警或拦截这类攻击。

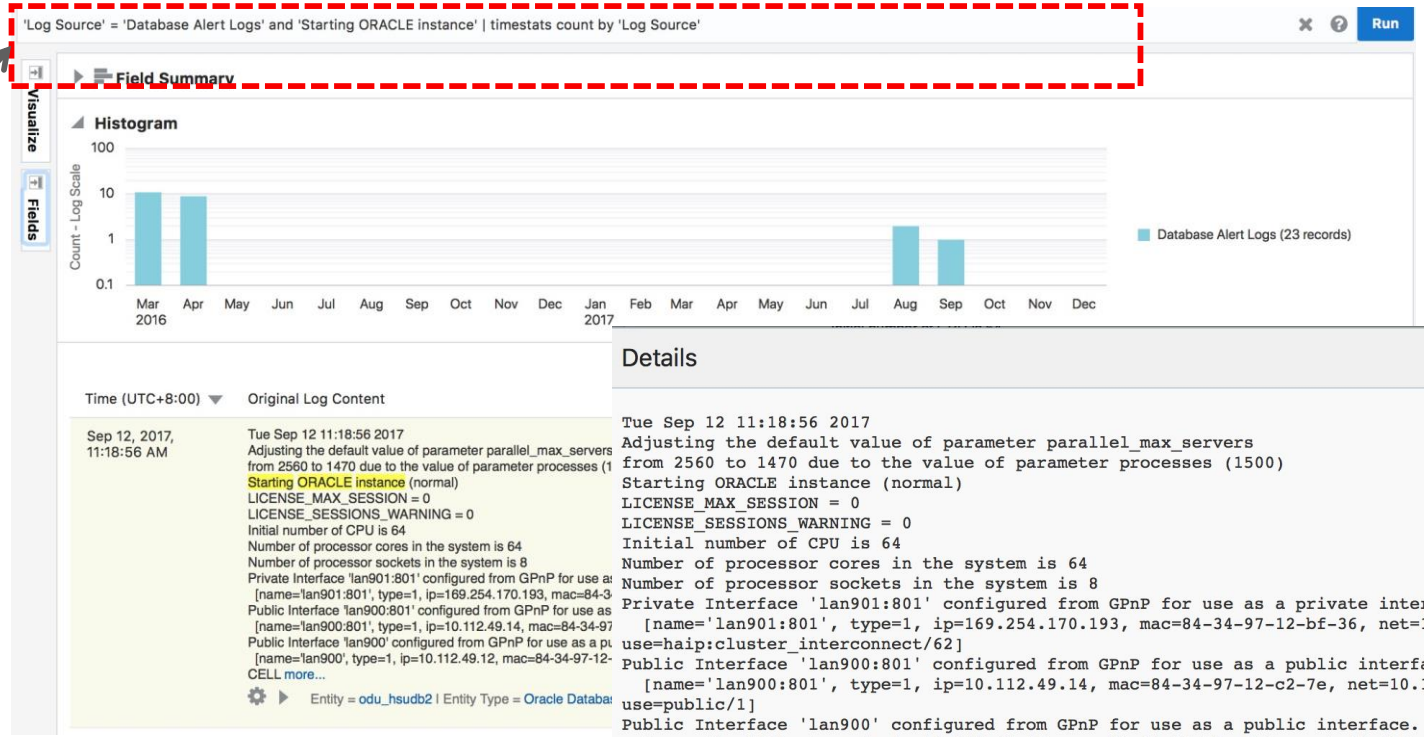


数据库日志分析

上万次的ORA-03137问题，通常是BUG，有没有下补丁？



查询数据库启动日志，我们发现



Details

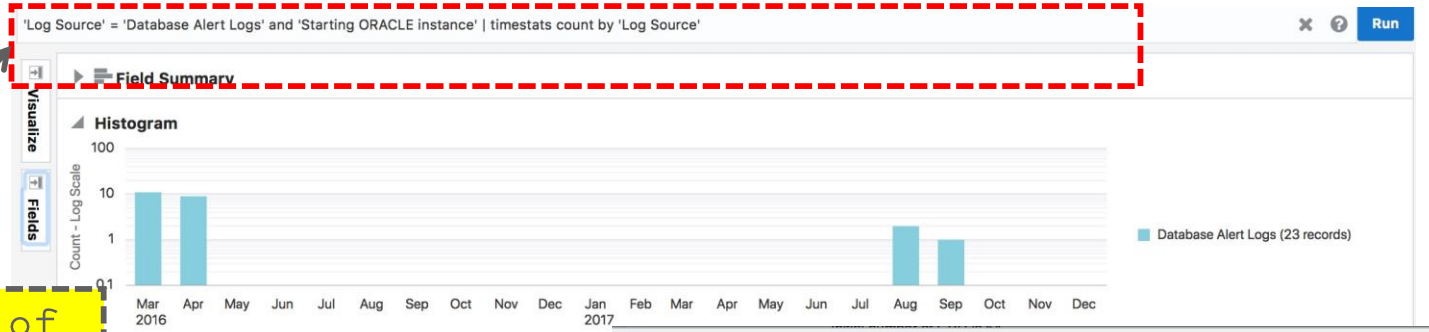
```
Tue Sep 12 11:18:56 2017
Adjusting the default value of parameter parallel_max_servers
from 2560 to 1470 due to the value of parameter processes (1500)
Starting ORACLE instance (normal)
LICENSE_MAX_SESSION = 0
LICENSE_SESSIONS_WARNING = 0
Initial number of CPU is 64
Number of processor cores in the system is 64
Number of processor sockets in the system is 8
Private Interface 'lan901:801' configured from GPnP for use as a private interconnect.
  [name='lan901:801', type=1, ip=169.254.170.193, mac=84-34-97-12-bf-36, net=169.254.0.0/16, mask=255.255.0.0,
use=haip:cluster_interconnect/62]
Public Interface 'lan900:801' configured from GPnP for use as a public interface.
  [name='lan900:801', type=1, ip=10.112.49.14, mac=84-34-97-12-c2-7e, net=10.112.49.0/24, mask=255.255.255.0,
use=public/1]
Public Interface 'lan900' configured from GPnP for use as a public interface.
  [name='lan900', type=1, ip=10.112.49.12, mac=84-34-97-12-c2-7e, net=10.112.49.0/24, mask=255.255.255.0, use=public/1]
CELL communication is configured to use 0 interface(s):
CELL IP affinity details:
    NUMA status: NUMA system w/ 8 process groups
    cellaffinity.ora status: cannot find affinity map at '/etc/oracle/cell/network-config/cellaffinity.ora' (see trace
file for details)
CELL communication will use 1 IP group(s):
    Grp 0:
Picked latch-free SCN scheme 3
WARNING: db_recovery_file_dest is same as db_create_file_dest
Autotune of undo retention is turned on.
LICENSE_MAX_USERS = 0
SYS auditing is disabled
NUMA system with 8 nodes detected
Oracle NUMA support not enabled
The parameter _enable_NUMA_support should be set to TRUE to enable Oracle NUMA support
Starting up:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, Real Application Clusters, OLAP, Data Mining
and Real Application Testing options.
ORACLE_HOME = /oracle/app/product/11.2.4/db_1
System name:    HP-UX
Node name:      hsu02
Release:        B.11.31
Version:        U
```

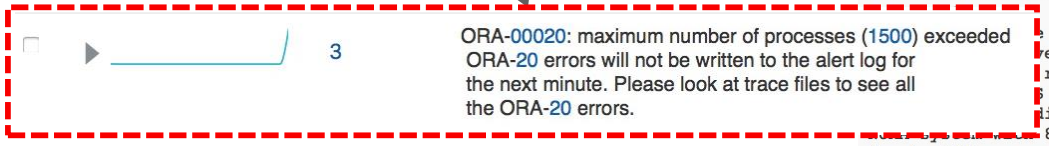
1．数据库版本为11.2.0.4.0，大约在2015年发布，期间已发布了很多的补丁。

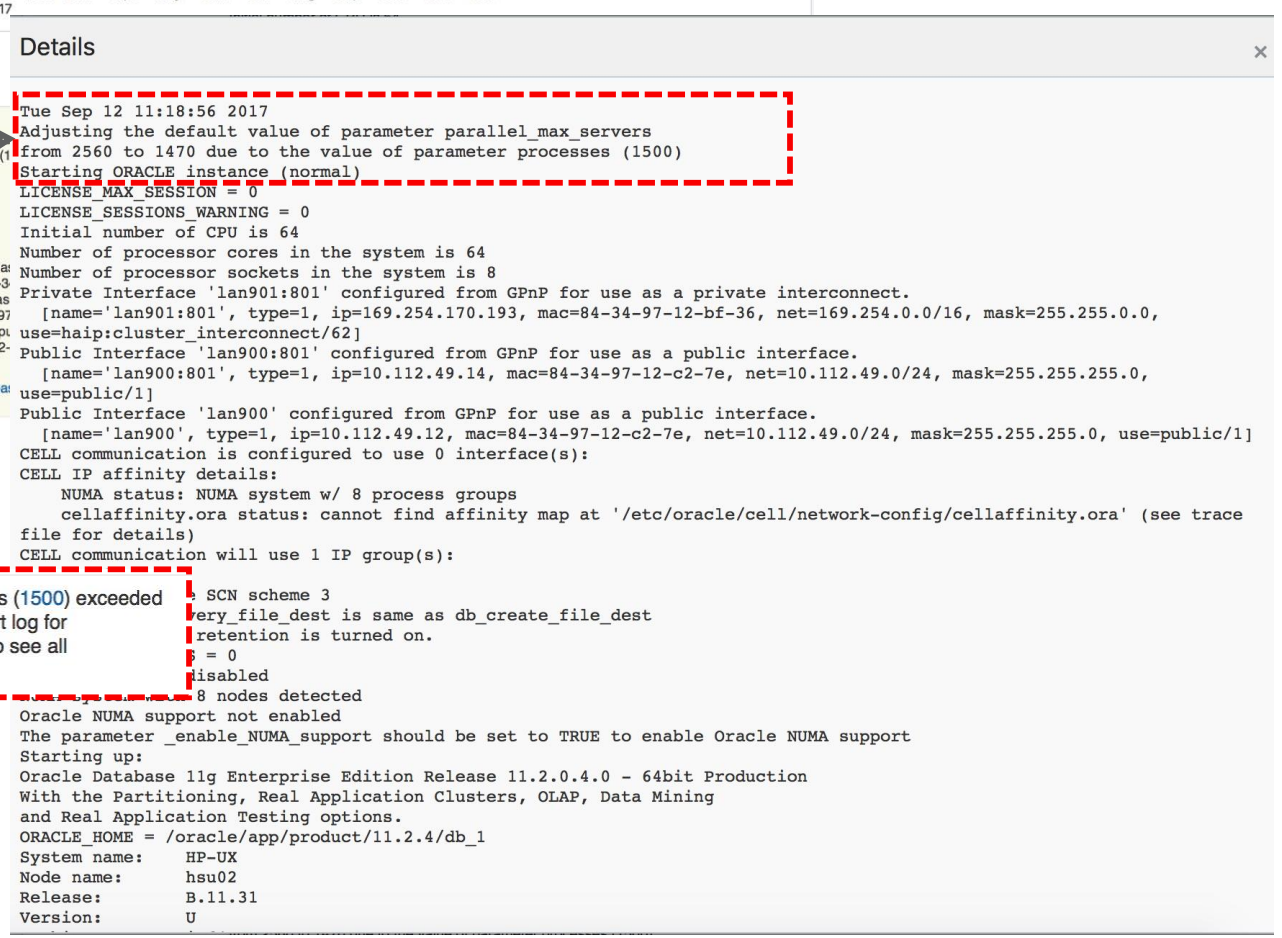
查询数据库启动日志，我们发现

2. 因为 maximum number of processes 被设定为1500，parallel_max_servers 被自动调节为1470。对数据库有影响吗？

答案是有的。

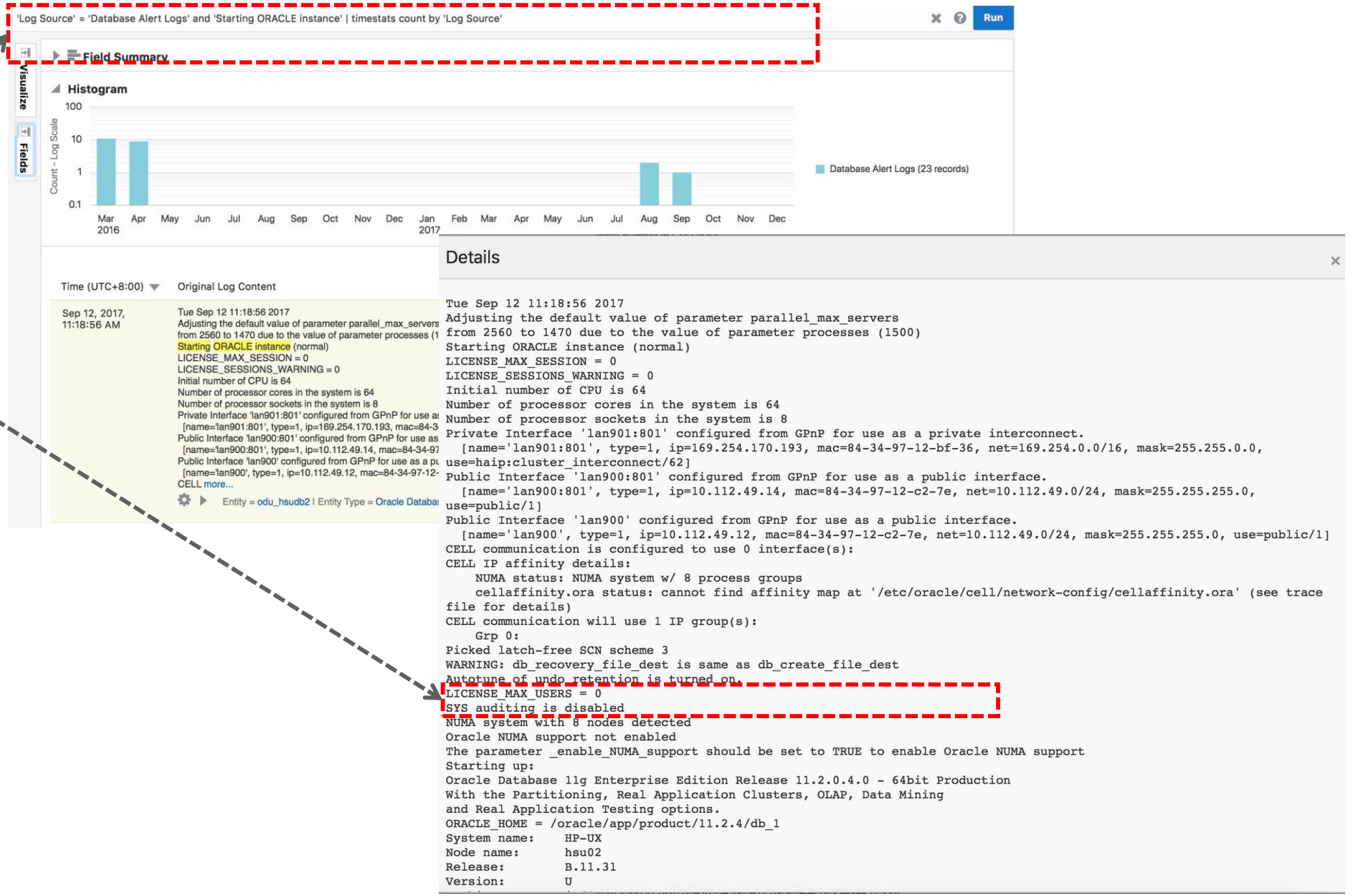




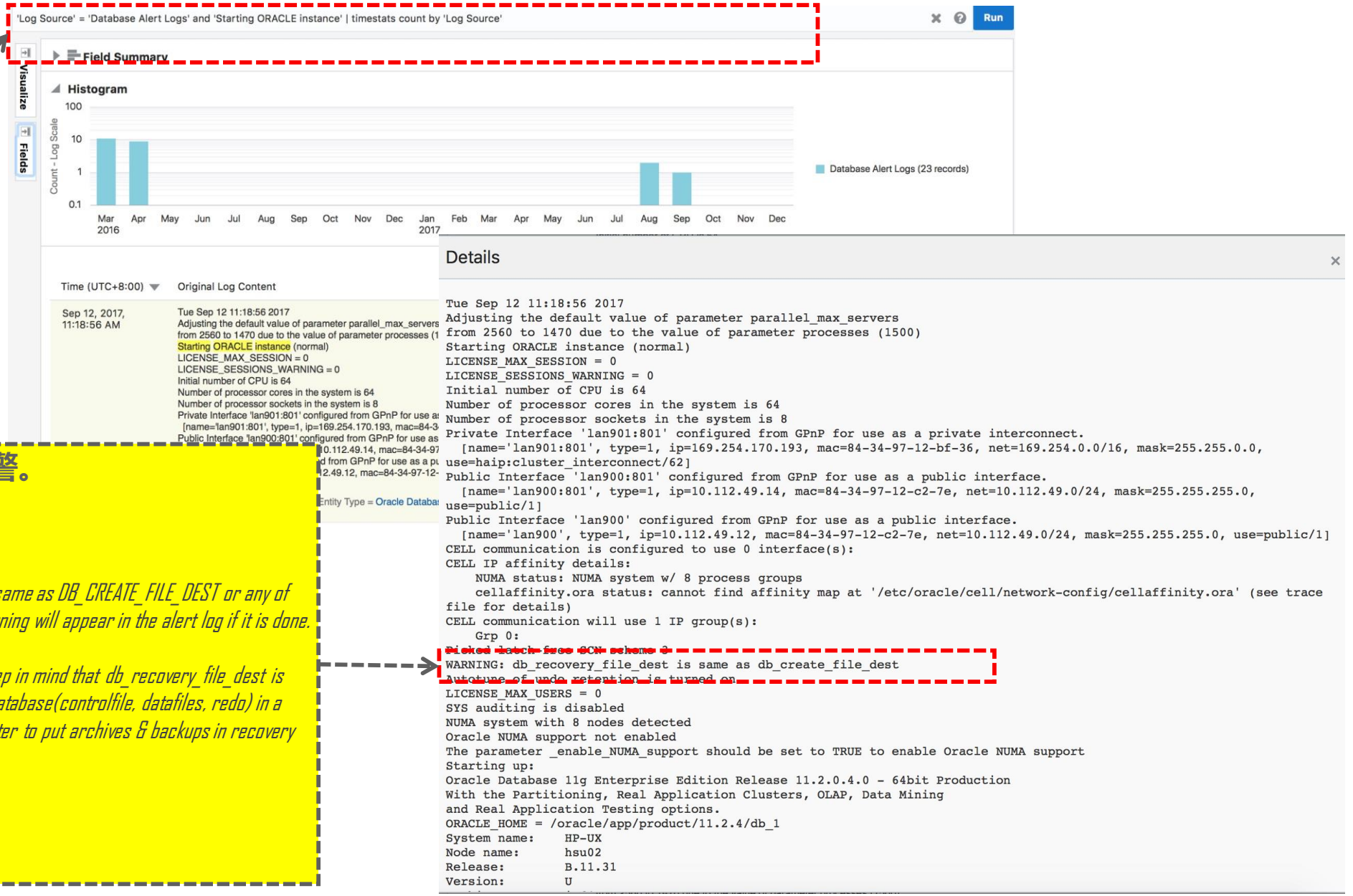


查询数据库启动日志，我们发现

3．系统审计被关闭



查询数据库启动日志，我们发现



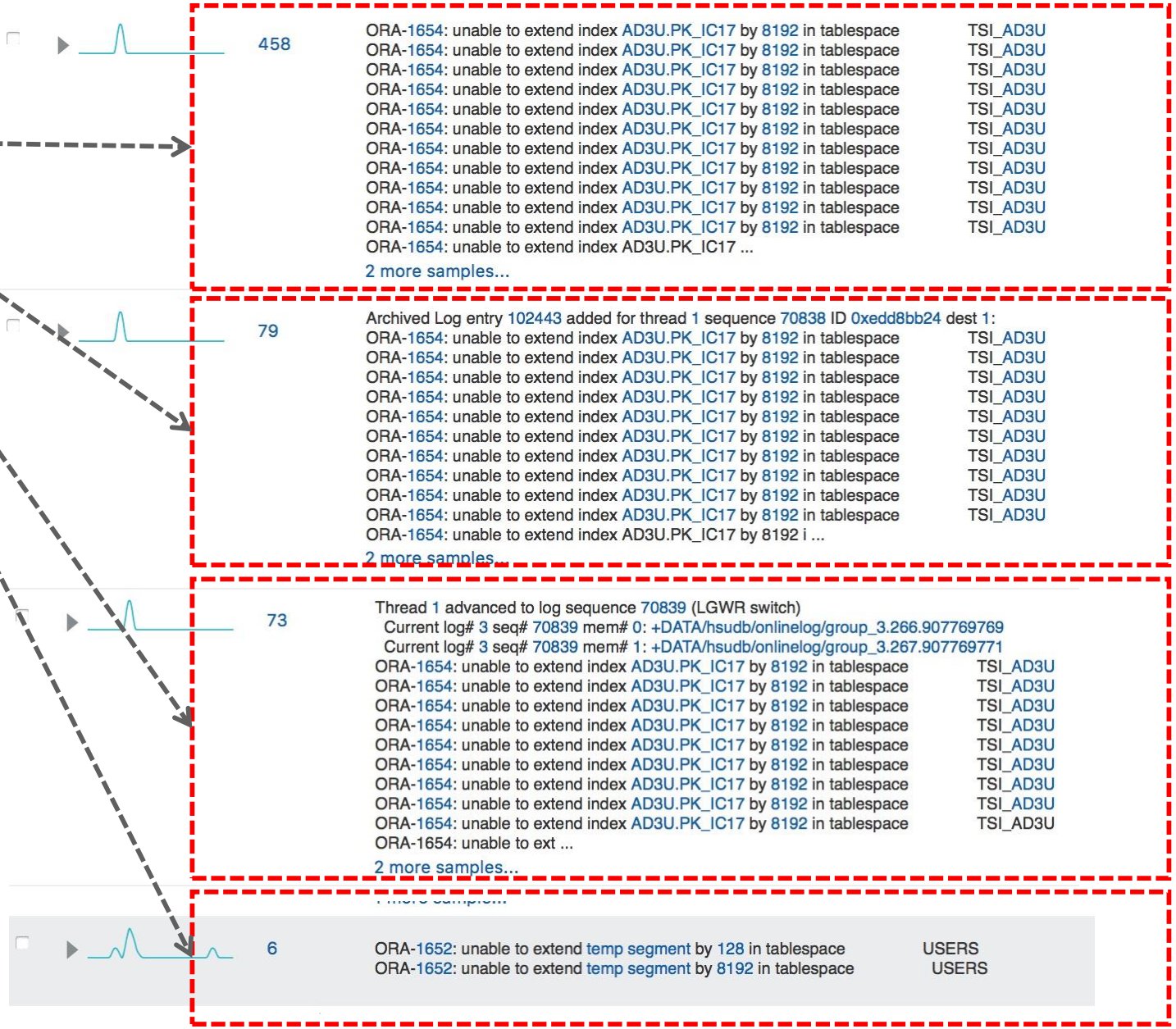
4． 数据库文件存放位置的告警。

As MOS note 2201064.1 says:

Oracle recommends that DB_RECOVERY_FILE_DEST not same as DB_CREATE_FILE_DEST or any of the DB_CREATE_ONLINE_LOG_DEST_n parameters. A warning will appear in the alert log if it is done.

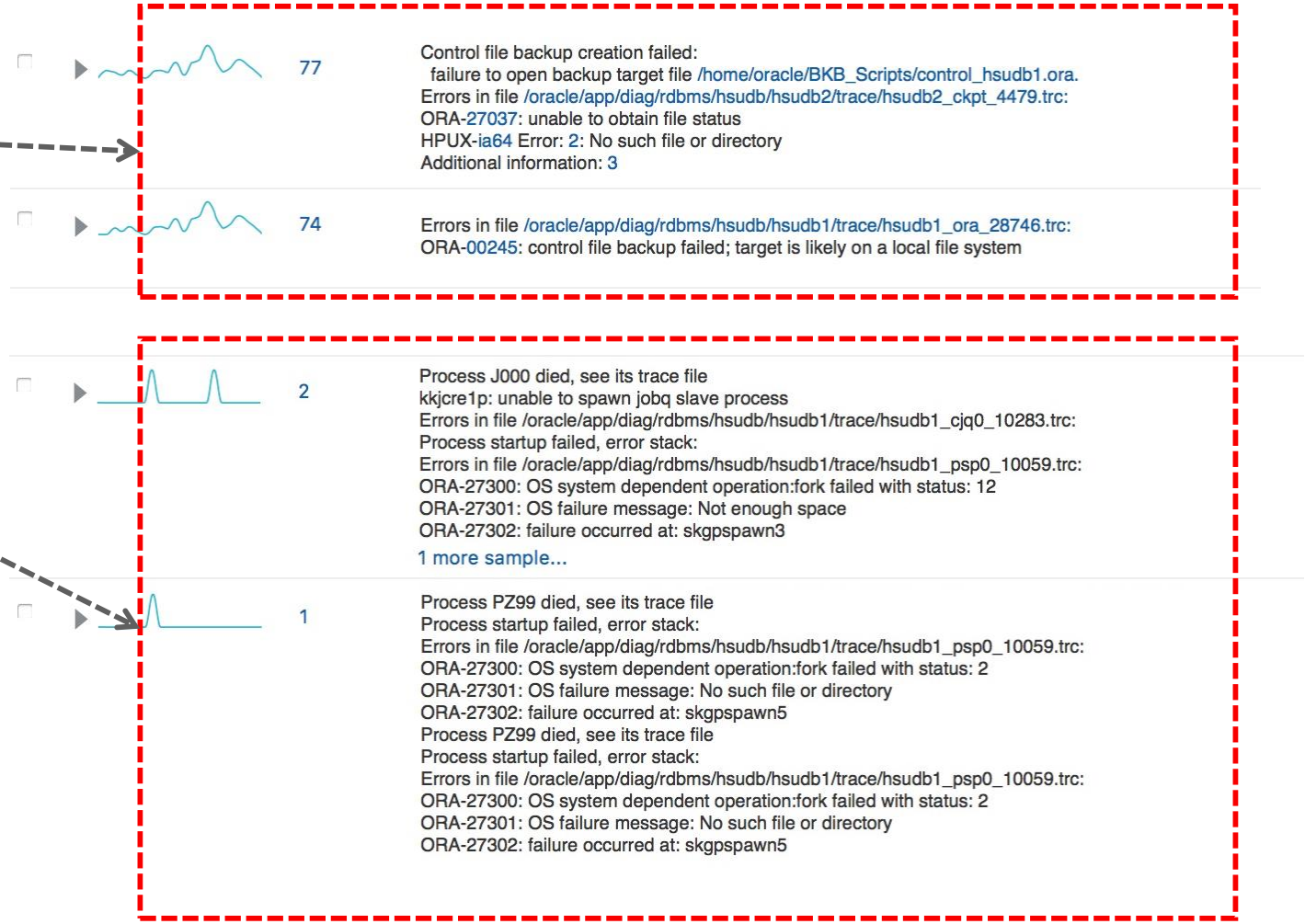
This is harmless warning, can be ignored. But please keep in mind that db_recovery_file_dest is Flash recovery area, It is always recommended to put database(controlfile, datafiles, redo) in a different location that is DB_CREATE_FILE_DEST, and better to put archives & backups in recovery location that is DB_RECOVERY_FILE_DEST.

我们还发现：不能获取更多空间，可能影响数据库性能或导致停机。

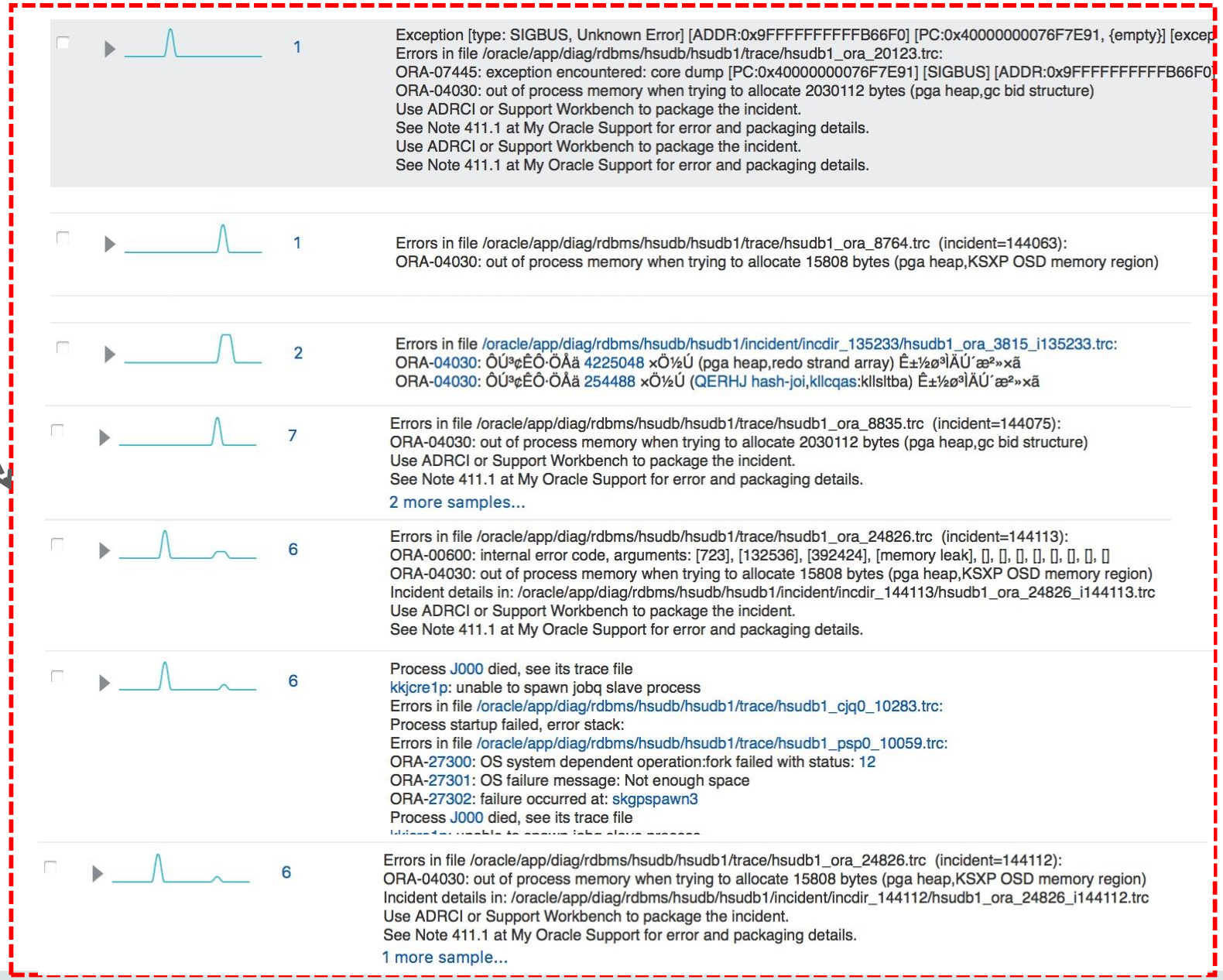


可能是目录被删除，不能备份control file

OS上的空间不够，进程终止。



内存不足，进程终止。请参考 411.1



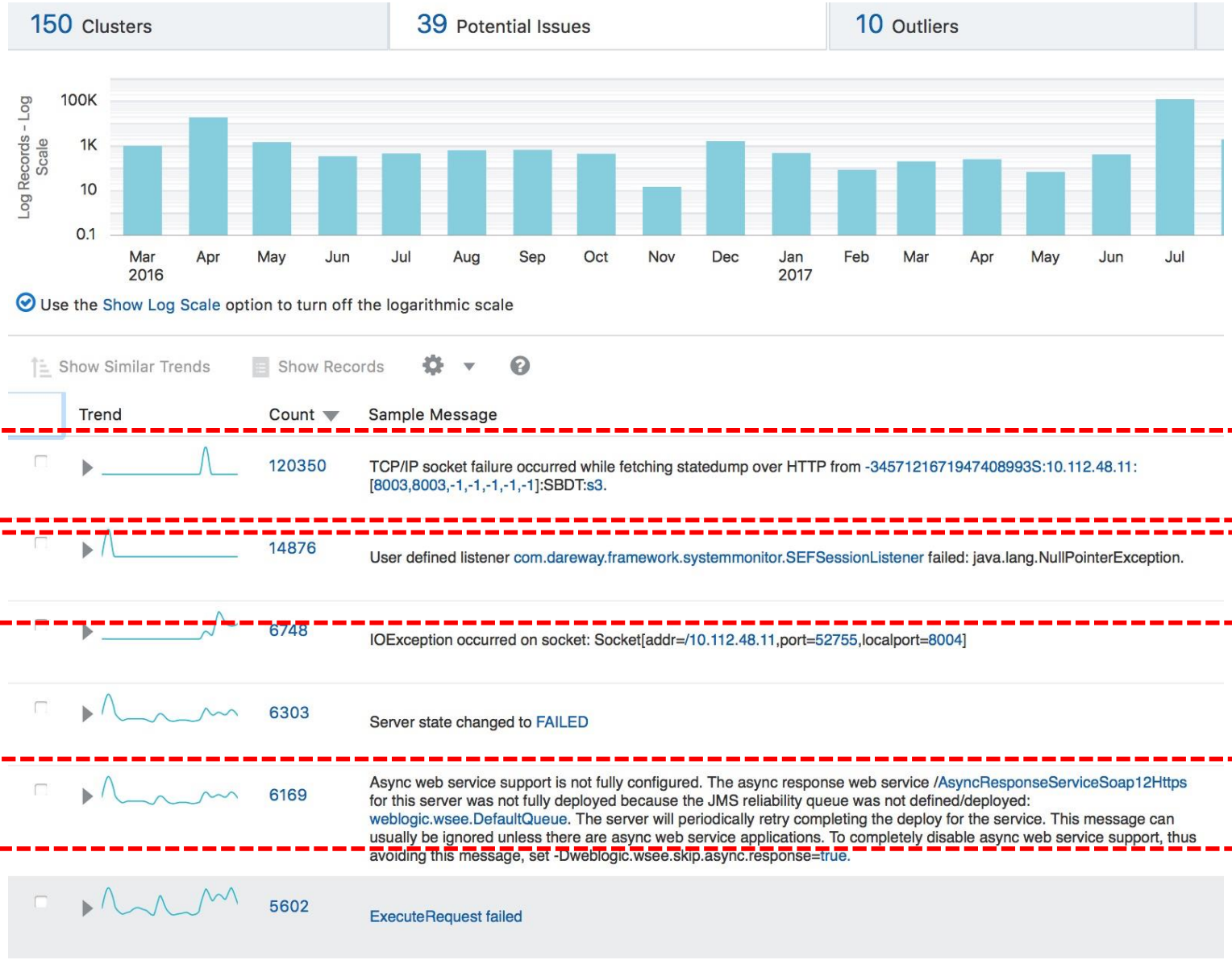
1	Exception [type: SIGBUS, Unknown Error] [ADDR:0x9FFFFFFFFFB66F0] [PC:0x40000000076F7E91, {empty}] [excep Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_ora_20123.trc: ORA-07445: exception encountered: core dump [PC:0x40000000076F7E91] [SIGBUS] [ADDR:0x9FFFFFFFFFB66F0] ORA-04030: out of process memory when trying to allocate 2030112 bytes (pga heap,gc bid structure) Use ADRCI or Support Workbench to package the incident. See Note 411.1 at My Oracle Support for error and packaging details. Use ADRCI or Support Workbench to package the incident. See Note 411.1 at My Oracle Support for error and packaging details.
1	Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_ora_8764.trc (incident=144063): ORA-04030: out of process memory when trying to allocate 15808 bytes (pga heap,KSXP OSD memory region)
2	Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/incident/incdir_135233/hsudb1_ora_3815_i135233.trc: ORA-04030: ÔÚ³¢ÊÔ·ÖÅä 4225048 ×Ö½Ú (pga heap,redo strand array) Ê±½ø³]ÄÚ´æ²»×ã ORA-04030: ÔÚ³¢ÊÔ·ÖÅä 254488 ×Ö½Ú (QERHJ hash-joi,kllcqas:kllsltba) Ê±½ø³]ÄÚ´æ²»×ã
7	Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_ora_8835.trc (incident=144075): ORA-04030: out of process memory when trying to allocate 2030112 bytes (pga heap,gc bid structure) Use ADRCI or Support Workbench to package the incident. See Note 411.1 at My Oracle Support for error and packaging details. 2 more samples...
6	Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_ora_24826.trc (incident=144113): ORA-00600: internal error code, arguments: [723], [132536], [392424], [memory leak], [], [], [], [], [], [], [], [] ORA-04030: out of process memory when trying to allocate 15808 bytes (pga heap,KSXP OSD memory region) Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb1/incident/incdir_144113/hsudb1_ora_24826_i144113.trc Use ADRCI or Support Workbench to package the incident. See Note 411.1 at My Oracle Support for error and packaging details.
6	Process J000 died, see its trace file kkjcre1p: unable to spawn jobq slave process Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_cjq0_10283.trc: Process startup failed, error stack: Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_psp0_10059.trc: ORA-27300: OS system dependent operation:fork failed with status: 12 ORA-27301: OS failure message: Not enough space ORA-27302: failure occurred at: skgpspawn3 Process J000 died, see its trace file
6	Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1_ora_24826.trc (incident=144112): ORA-04030: out of process memory when trying to allocate 15808 bytes (pga heap,KSXP OSD memory region) Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb1/incident/incdir_144112/hsudb1_ora_24826_i144112.trc Use ADRCI or Support Workbench to package the incident. See Note 411.1 at My Oracle Support for error and packaging details. 1 more sample...

WebLogic 日志分析

TPC/IP Socket Failures

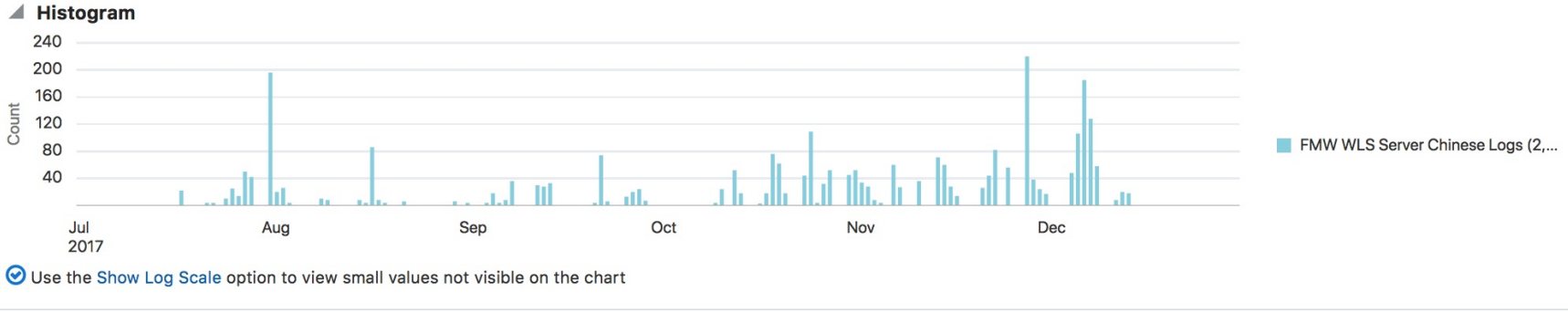
为什么使用自定义的Listener?

不完全支持Async Web Service



2870 次 Stuck Thread 错误

2870 [STUCK] ExecuteThread: '13' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "6,361" seconds working on the request "Workmanager: default, Version: 40, Scheduled=true, Started=true, Started time: 6361162 ms



不支持 Reliable SOAP

1029 The server does not support reliable SOAP messaging.

400 Web server: s8, failed to perform batched update for replicated sessions against jndiname: null on the secondary server: t3://10.112.48.11:8003 http-port: 0 https-port: 0

336 [ServletContext@612570291[app:hsu module:hsu.war path:/hsu spec-version:2.5]] Servlet failed with IOException

100 An unexpected error occurred while doing a batched update of last accessed time attribute of updated sessions in application /hsu

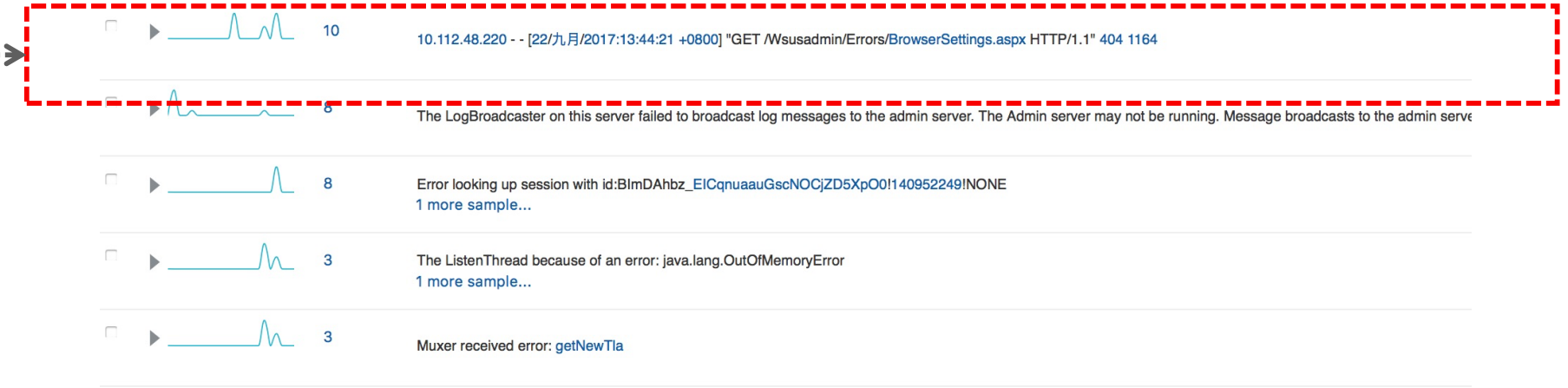
92 at weblogic.security.acl.internal.AuthenticatedSubject.doAs(AuthenticatedSubject.java:321)

RMI 错误

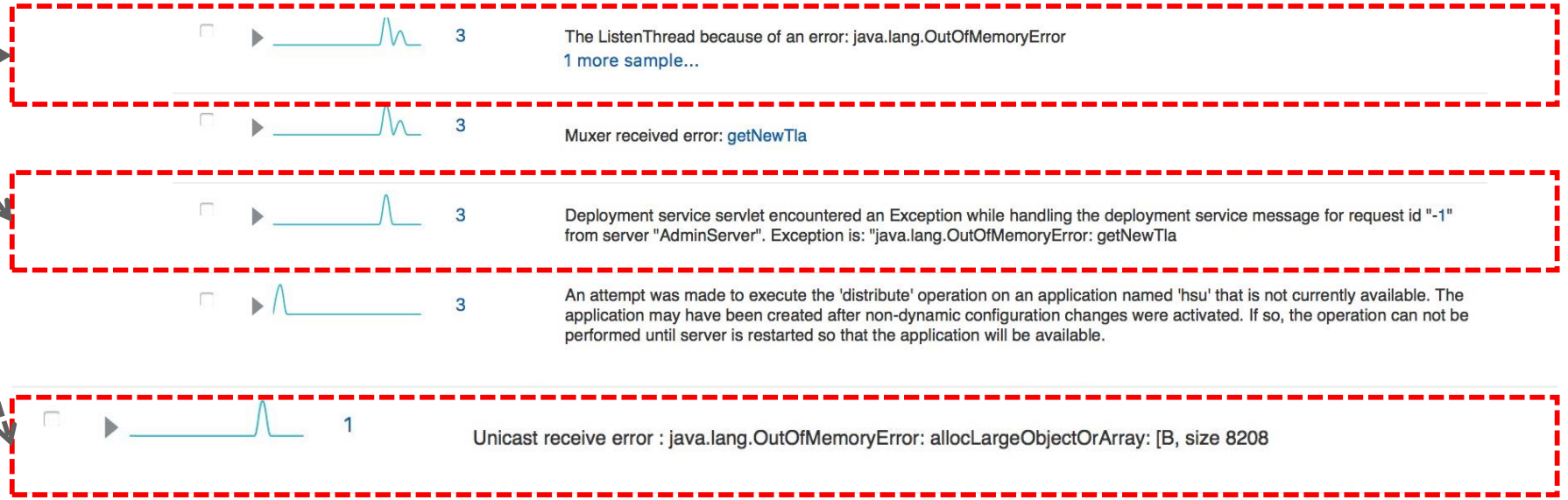
69 An error was thrown by rmi server: weblogic.cluster.replication.ReplicationManager.create(Lweblogic.rmi.spi.HostID;ILweblogic.cluster.replication.ROID;Lweblogic.cluster.replication.Replicatable;)
1 more sample...

66 This server does not have deployment for the Web application with context path: /hsu. The callback: becomeSecondary

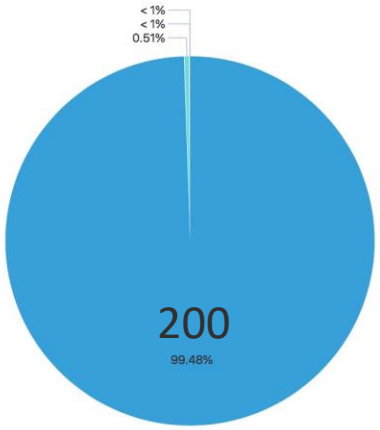
有做漏洞扫描？还是被扫描？



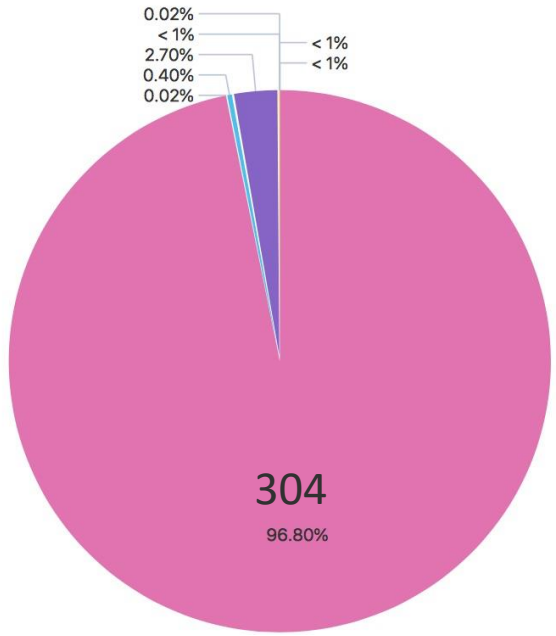
OutOfMemoryError



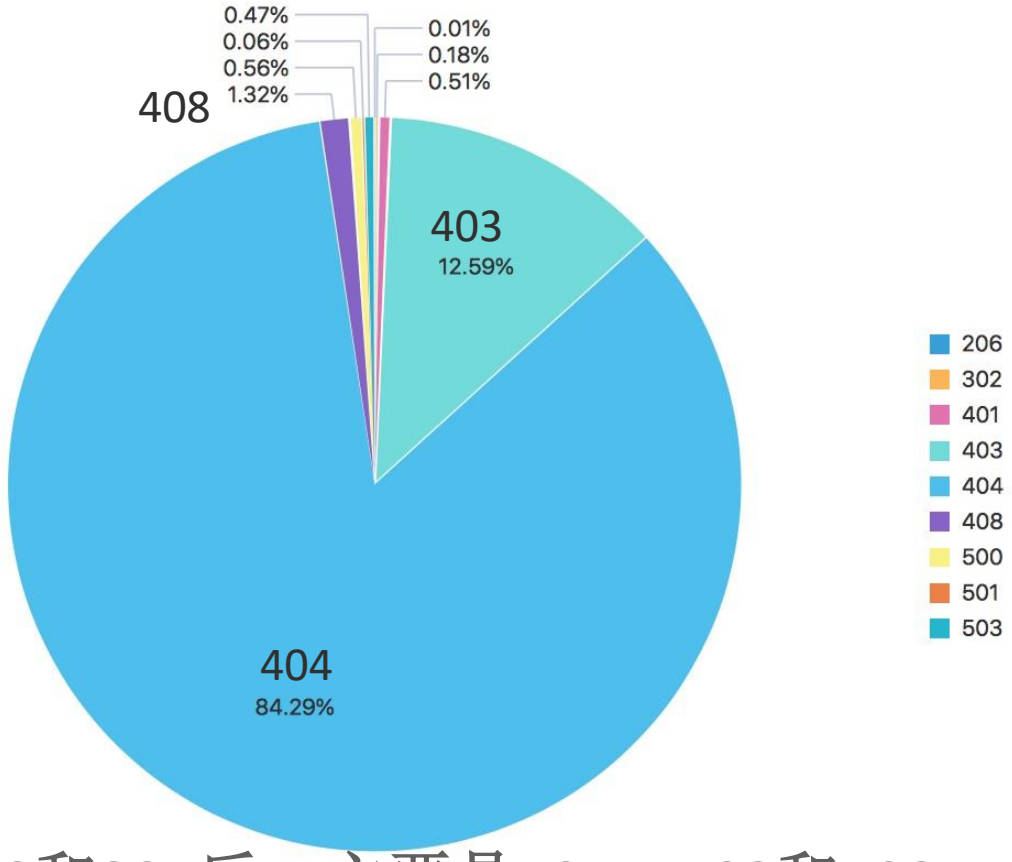
HTTP 状态分布



主要是200



撇除200后，主要是304



撇除200和304后，主要是404、403和408

发现部分安全问题

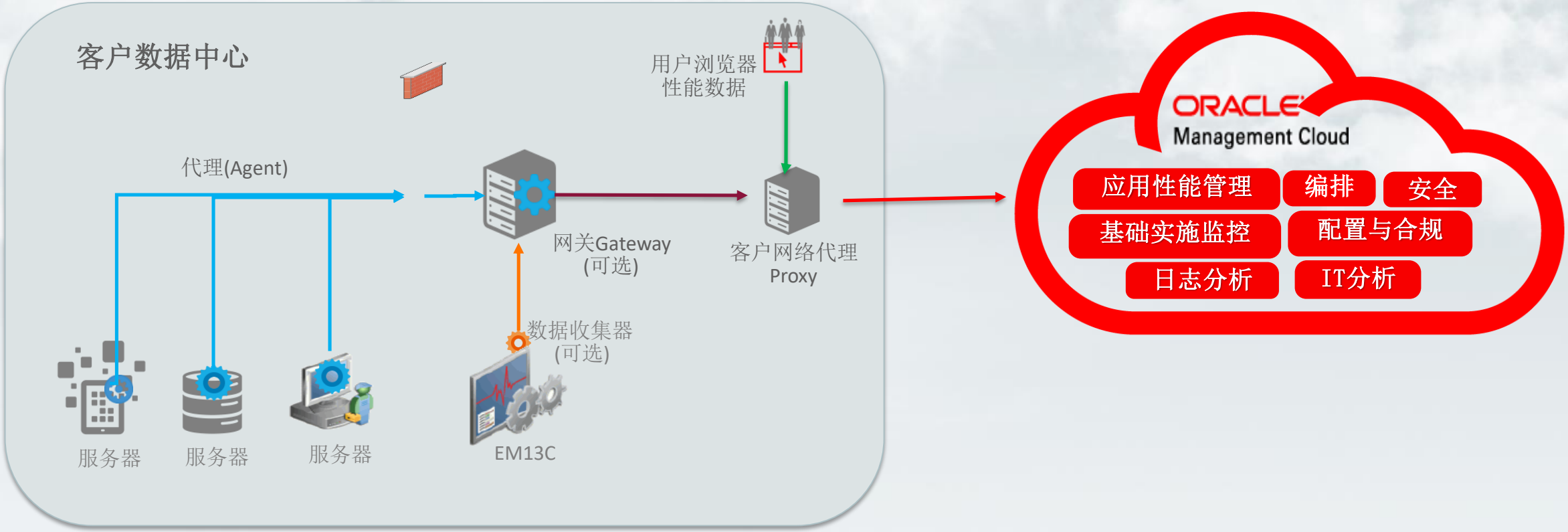
Directory Travel 攻击， 尝试获取密码。失败。

Jul 1, 2017, 12:00:00 AM	../../../../../etc/passwd	2
Sep 1, 2017, 12:00:00 AM	../../../../../etc/passwd	3
Feb 1, 2017, 12:00:00 AM	../../../../../etc/passwd	4
Jul 1, 2017, 12:00:00 AM	..\..\..\..\..\..\windows\win.ini	2
Sep 1, 2017, 12:00:00 AM	..\..\..\..\..\..\windows\win.ini	4
Feb 1, 2017, 12:00:00 AM	..\..\..\..\..\..\windows\win.ini	4
Jul 1, 2017, 12:00:00 AM	..\..\..\..\..\..\winnt\win.ini	2
Sep 1, 2017, 12:00:00 AM	..\..\..\..\..\..\winnt\win.ini	4
Feb 1, 2017, 12:00:00 AM	..\..\..\..\..\..\winnt\win.ini	4
Sep 1, 2017, 12:00:00 AM	/	55
Sep 1, 2017, 12:00:00 AM	/%../../../../../../../../../../boot.ini	1
Jul 1, 2017, 12:00:00 AM	/%00	2
Sep 1, 2017, 12:00:00 AM	/%00	3
Feb 1, 2017, 12:00:00 AM	/%00	4
Jul 1, 2017, 12:00:00 AM	/%00/	4
Feb 1, 2017, 12:00:00 AM	/%00/	8
Sep 1, 2017, 12:00:00 AM	/%00/	9
Jul 1, 2017, 12:00:00 AM	/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd	2

代码注入攻击，失败。

Feb 1, 2017, 12:00:00 AM	0).chr(105).chr(114).chr(32).chr(47).chr(65).chr(58).chr(72).chr(32).chr(99).chr(58))%7d%7d%7b%24%7bexit()%7d%7d	4
Jul 1, 2017, 12:00:00 AM	/awstatstotals.php?sort=%7b%24%7bpassthru(chr(99).chr(97).chr(116).chr(32).chr(47).chr(101).chr(116).chr(99).chr(47).chr(112).chr(97).chr(115).chr(115).chr(119).chr(100))%7d%7d%7b%24%7bexit()%7d%7d	2
Sep 1, 2017, 12:00:00 AM	/awstatstotals.php?sort=%7b%24%7bpassthru(chr(99).chr(97).chr(116).chr(32).chr(47).chr(101).chr(116).chr(99).chr(47).chr(112).chr(97).chr(115).chr(115).chr(119).chr(100))%7d%7d%7b%24%7bexit()%7d%7d	3
Feb 1, 2017, 12:00:00 AM	/awstatstotals.php?sort=%7b%24%7bpassthru(chr(99).chr(97).chr(116).chr(32).chr(47).chr(101).chr(116).chr(99).chr(47).chr(112).chr(97).chr(115).chr(115).chr(119).chr(100))%7d%7d%7b%24%7bexit()%7d%7d	4
Jul 1, 2017, 12:00:00 AM	/awstatstotals/awstatstotals.php?sort=%7b%24%7bpassthru(chr(100).chr(105).chr(114).chr(32).chr(47).chr(65).chr(58).chr(72).chr(32).chr(99).chr(58))%7d%7d%7b%24%7bexit()%7d%7d	2
Sep 1, 2017, 12:00:00 AM	/awstatstotals/awstatstotals.php?sort=%7b%24%7bpassthru(chr(100).chr(105).chr(114).chr(32).chr(47).chr(65).chr(58).chr(72).chr(32).chr(99).chr(58))%7d%7d%7b%24%7bexit()%7d%7d	3
Feb 1, 2017, 12:00:00 AM	/awstatstotals/awstatstotals.php?sort=%7b%24%7bpassthru(chr(100).chr(105).chr(114).chr(32).chr(47).chr(65).chr(58).chr(72).chr(32).chr(99).chr(58))%7d%7d%7b%24%7bexit()%7d%7d	4
Jul 1, 2017, 12:00:00 AM	/awstatstotals/awstatstotals.php?sort=%7b%24%7bpassthru(chr(99).chr(97).chr(116).chr(32).chr(47).chr(101).chr(116).chr(99).chr(47).chr(112).chr(97).chr(115).chr(115).chr(119).chr(100))%7d%7d%7b%24%7bexit()%7d%7d	2

OMC整体架构图



- 协议和端口：https/443

外网访问地址https://<tenantid>.itom.management.us2.oraclecloud.com/*
内网访问网关Gateway server (typically 1830)

OMC的服务模型