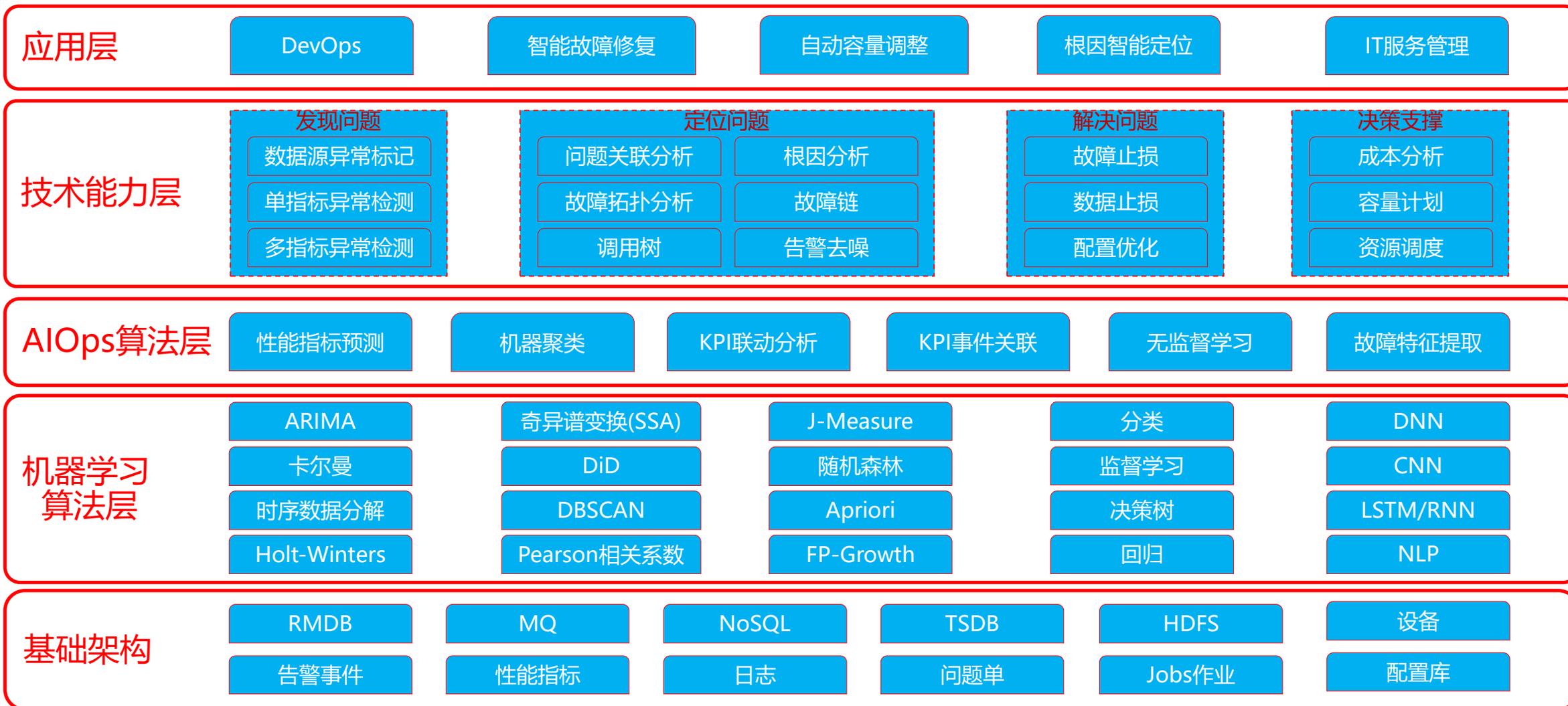


# 基于人工智能的数字化IT管理



## 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。

## 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。

## 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。

## 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 〕

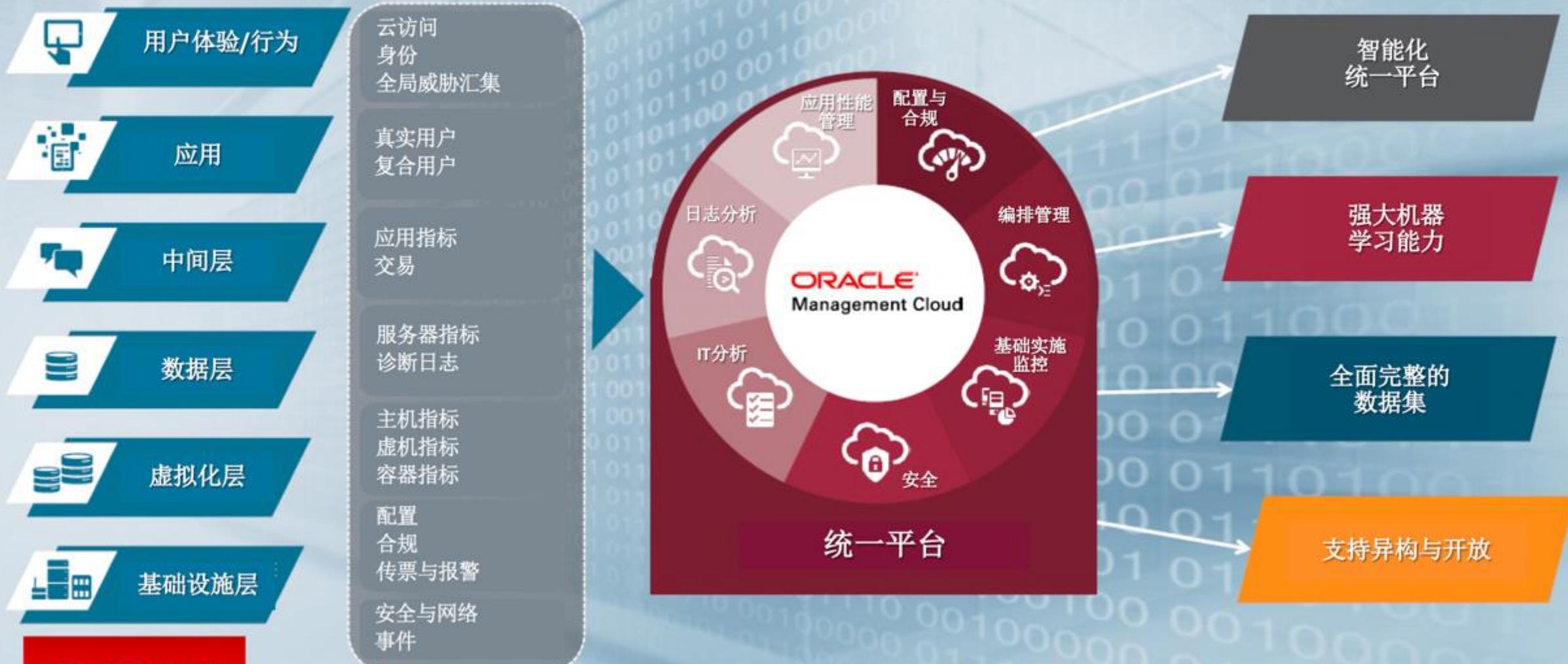
各类木马和勒索病毒难以防范

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

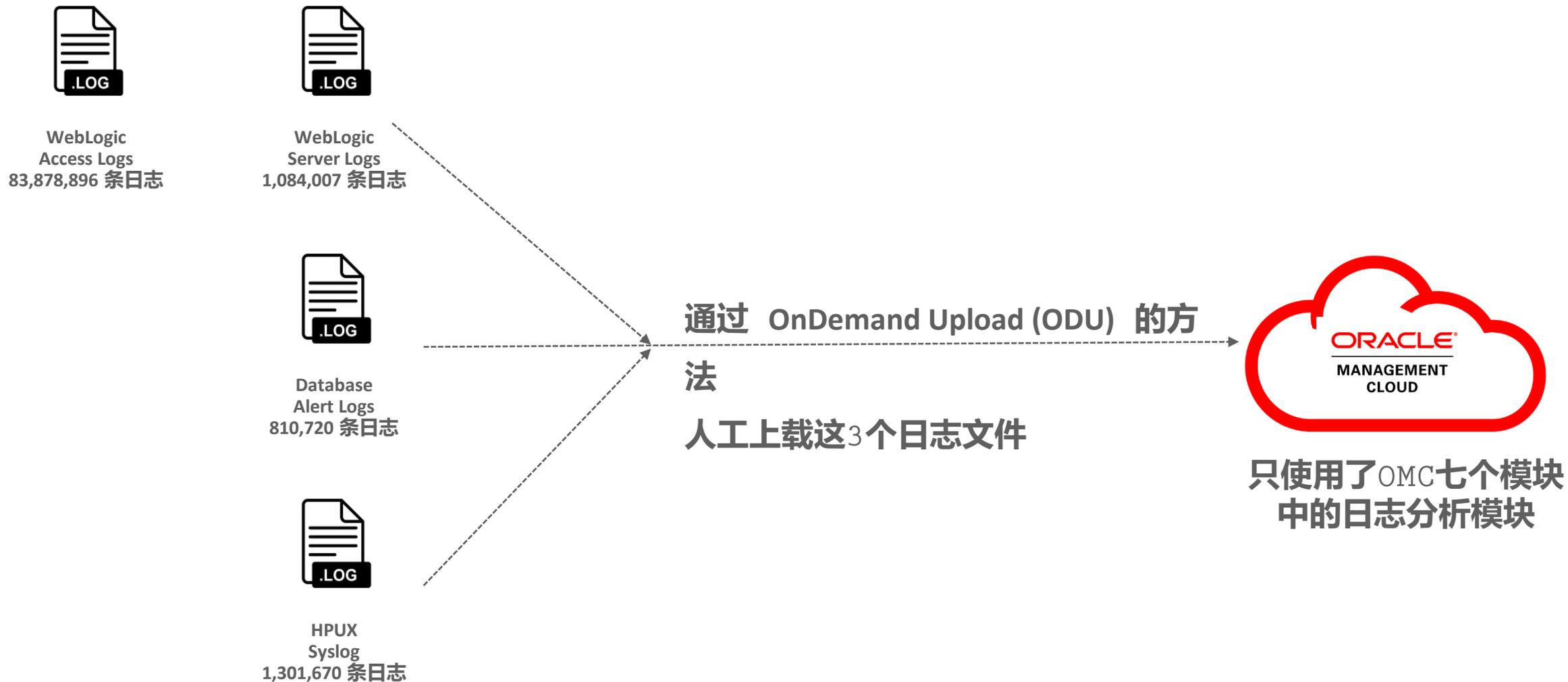
由统一大数据平台和机器学习驱动的实时运营洞察



A man with dark hair, wearing a light blue button-down shirt, is smiling and looking at a tablet computer. He is sitting at a white desk in a bright office with large windows in the background. The scene is well-lit, suggesting a sunny day. The overall mood is positive and professional.

# 某客户生产日志智能分析

# 简单收集4种日志文件



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？

### ▲ Histogram



🕒 Use the **Show Log Scale** option to turn off the logarithmic scale

Showing 1-25 of 87,075,293

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

Visualize

Records with Histogram

Display Fields

- Entity
- Entity Type
- Log Source
- Host Name (Server)
- Problem Priority
- Label

Field Summary

Cluster

Showing 1-25 of 87,075,293

Visualize

Cluster

Display Options

- Show Problem Logs Only
- Show Log Scale on Histogram

Records per Page 25

1537 Clusters 271 Potential Issues 274 Outliers 225 Trends

Log Records

Use the Show Log Scale option to view small values not visible on the chart

Showing 271 clusters

Trend	Count	Sample Message	ID	Log Source
-------	-------	----------------	----	------------

# 操作系统日志分析

176,519 次无效用户登入

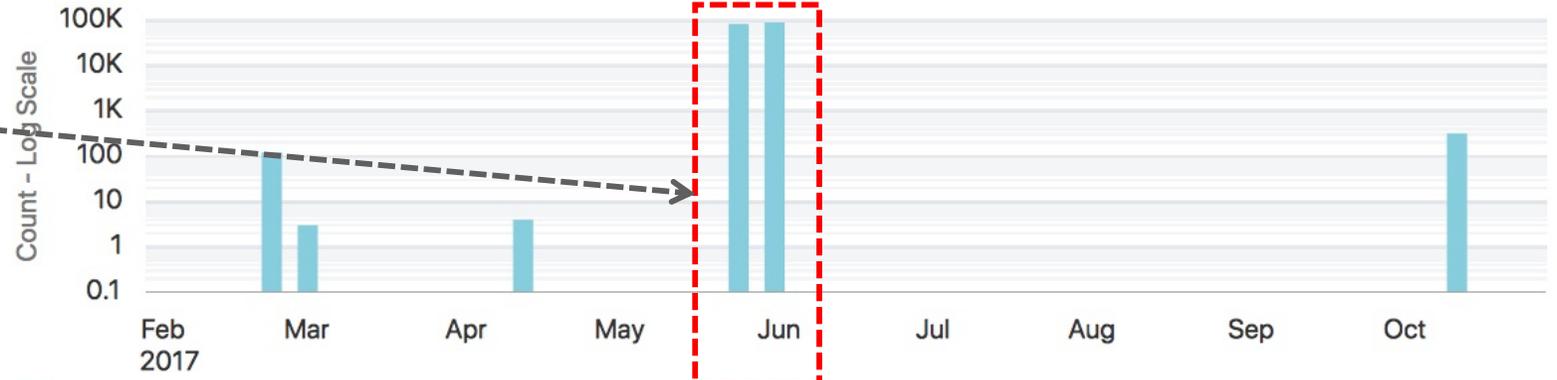
215198	Did not receive identification string from 10.112.48.230
107647	do_exec_no_pty: command = /usr/bin/df -kP /dev/vg00/lvol6 1 more sample...
89545	Failed none for invalid user admin from 10.112.48.230 port 49659 ssh2 3 more samples...
82421	do_exec_no_pty: command = /usr/bin/sar 3
46035	SSH: Server;Ltype: Kex;Remote: 10.112.29.30-62441;Enc: aes256-cbc;MAC: hmac-sha1;Comp: none
46034	SSH: Server;Ltype: Version;Remote: 10.112.48.230-60238;Protocol: 2.0;Client: libssh2_1.8.0 2 more samples...
46030	SSH: Server;Ltype: Authname;Remote: 10.112.48.230-49659;Name: admin 1 more sample...
43488	input_userauth_request: invalid user admin
43486	Invalid user admin from 10.112.48.230
43390	Received disconnect from 10.112.48.230: 11: Normal Shutdown, Thank you for playing

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

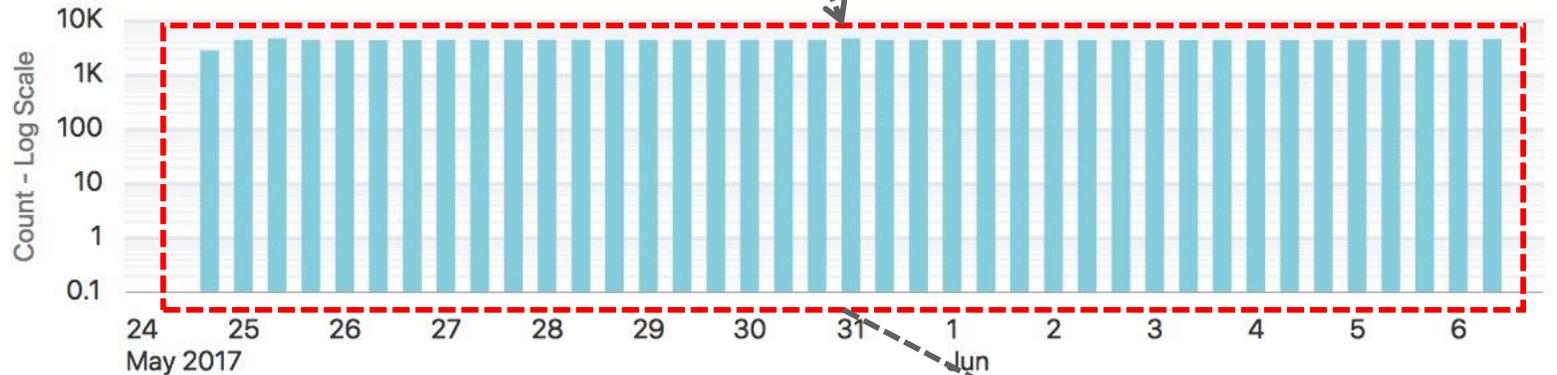
建议设置告警或拦截这类攻击。

▲ Histogram



🔍 Use the Show Log Scale option to turn off the logarithmic scale

▲ Histogram



Showing 1976-2000 of 173,463

# 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？



7524

Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ora\_4850.trc (incident=112633):  
ORA-03137: TTC ÐÓéÁÚ²¿ííó: [12333] [0] [0] [0] □ □ □ □  
Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb2/incident/incdir\_112633/hsudb2\_ora\_4850\_i112633.trc  
Thread 2 advanced to log sequence 143282 (LGWR switch)  
Current log# 8 seq# 143282 mem# 0: +DATA/hsudb/onlinelog/group\_8.278.907769991  
Current log# 8 seq# 143282 mem# 1: +DATA/hsudb/onlinelog/group\_8.279.907769993  
3 more samples...



3673

Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ora\_7736.trc (incident=114083):  
ORA-03137: TTC ÐÓéÁÚ²¿ííó: [3120] □ □ □ □ □ □  
Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb2/incident/incdir\_114083/hsudb2\_ora\_7736\_i114083.trc  
1 more sample...



181

Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ora\_8382.trc (incident=115233):  
ORA-03137: TTC ÐÓéÁÚ²¿ííó: [12333] [0] [0] [0] □ □ □ □



19

Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ora\_10142.trc (incident=114121):  
ORA-03137: TTC ÐÓéÁÚ²¿ííó: [12333] [96] [1] [0] □ □ □ □  
Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ora\_10326.trc (incident=114138):  
ORA-03137: TTC ÐÓéÁÚ²¿ííó: [12333] [0] [0] [1] □ □ □ □  
Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb2/incident/incdir\_114121/hsudb2\_ora\_10142\_i114121.trc  
Incident details in: /oracle/app/diag/rdbms/hsudb/hsudb2/incident/incdir\_114138/hsudb2\_ora\_10326\_i114138.trc



查询数据库启动日志，我们发现

'Log Source' = 'Database Alert Logs' and 'Starting ORACLE Instance' | timestats count by 'Log Source'

Field Summary

Visualize Fields

Histogram

Count - Log Scale

Database Alert Logs (23 records)

Time (UTC+8:00) Original Log Content

Sep 12, 2017, 11:18:56 AM

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.  
Public Interface 'lan900:801' configured from GPNP for use as a public interface.  
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/cellaaffinity.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。

'Log Source' = 'Database Alert Logs' and 'Starting ORACLE instance' | timestats count by 'Log Source'

Field Summary

Histogram

Count - Log Scale

Database Alert Logs (23 records)

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
[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):
  SCN scheme 3
  copy_file_dest is same as db_create_file_dest
  retention is turned on.
  = 0
  disabled
  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
```

ORA-00020: maximum number of processes (1500) exceeded  
ORA-20 errors will not be written to the alert log for the next minute. Please look at trace files to see all the ORA-20 errors.

3

查询数据库启动日志，我们发现

'Log Source' = 'Database Alert Logs' and 'Starting ORACLE Instance' | timestats count by 'Log Source'

Field Summary

Visualize Fields

Histogram

Count - Log Scale

Database Alert Logs (23 records)

Time (UTC+8:00) Original Log Content

Sep 12, 2017, 11:18:56 AM

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.  
Public Interface 'lan900:801' configured from GPnP for use as a public interface.  
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

3. 系统审计被关闭

查询数据库启动日志，我们发现

'Log Source' = 'Database Alert Logs' and 'Starting ORACLE Instance' | timestats count by 'Log Source'

Time (UTC+8:00)	Original Log Content
Sep 12, 2017, 11:18:56 AM	<pre> 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. Public Interface 'lan900:801' configured from GPNP for use as a public interface. 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 match-free OCN scheme 0 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 </pre>

#### 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.*



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。

77 Control file backup creation failed:  
failure to open backup target file /home/oracle/BKB\_Scripts/control\_hsudb1.ora.  
Errors in file /oracle/app/diag/rdbms/hsudb/hsudb2/trace/hsudb2\_ckpt\_4479.trc:  
ORA-27037: unable to obtain file status  
HPUX-ia64 Error: 2: No such file or directory  
Additional information: 3

74 Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1\_ora\_28746.trc:  
ORA-00245: control file backup failed; target is likely on a local file system

2 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  
1 more sample...

1 Process PZ99 died, see its trace file  
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: 2  
ORA-27301: OS failure message: No such file or directory  
ORA-27302: failure occurred at: skgpspawn5  
Process PZ99 died, see its trace file  
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: 2  
ORA-27301: OS failure message: No such file or directory  
ORA-27302: failure occurred at: skgpspawn5

内存不足，进程终止。请参考 411.1

The screenshot displays a list of Oracle ADR incidents, each with a waveform icon and a count. The incidents are as follows:

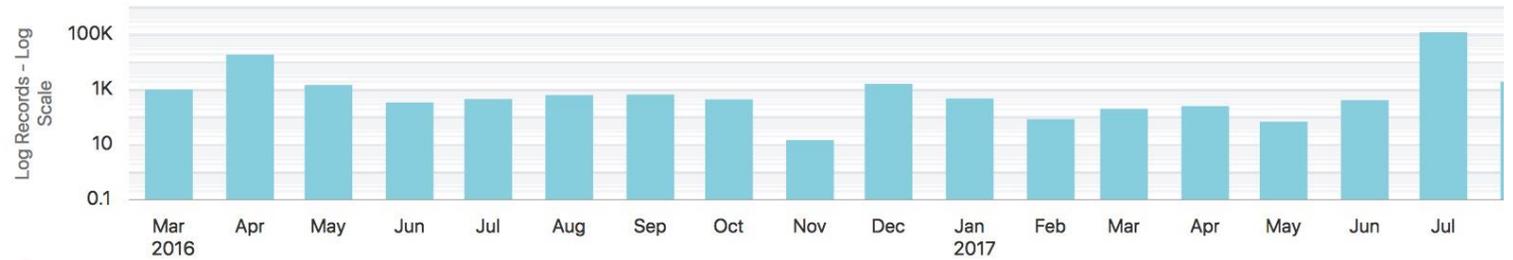
- Incident 1:** Exception [type: SIGBUS, Unknown Error] [ADDR:0x9FFFFFFFFFB66F0] [PC:0x4000000076F7E91, {empty}] [except]. Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/trace/hsudb1\_ora\_20123.trc: ORA-07445: exception encountered: core dump [PC:0x4000000076F7E91] [SIGBUS] [ADDR:0x9FFFFFFFFFB66F0]. 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.
- Incident 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,KSPX OSD memory region).
- Incident 2:** Errors in file /oracle/app/diag/rdbms/hsudb/hsudb1/incident/incdir\_135233/hsudb1\_ora\_3815\_i135233.trc: ORA-04030: 4225048 xO½Ú (pga heap,redo strand array) Ê±½ø³ÄÚ'æ²»xã. ORA-04030: 254488 xO½Ú (QERHJ hash-join,klcqas:klsltba) Ê±½ø³ÄÚ'æ²»xã.
- Incident 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...](#)
- Incident 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,KSPX 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.
- Incident 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 [kkjcre1p](#): unable to spawn jobq slave process.
- Incident 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,KSPX 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

150 Clusters

39 Potential Issues

10 Outliers



Use the Show Log Scale option to turn off the logarithmic scale

Show Similar Trends Show Records

Trend	Count	Sample Message
	120350	TCP/IP socket failure occurred while fetching statedump over HTTP from -3457121671947408993S:10.112.48.11: [8003,8003,-1,-1,-1,-1]:SBDT:s3.
	14876	User defined listener com.dareway.framework.systemmonitor.SEFSessionListener failed: java.lang.NullPointerException.
	6748	IOException occurred on socket: Socket[addr=/10.112.48.11,port=52755,localport=8004]
	6303	Server state changed to FAILED
	6169	Async web service support is not fully configured. The async response web service /AsyncResponseServiceSoap12Https for this server was not fully deployed because the JMS reliability queue was not defined/deployed: weblogic.wsee.DefaultQueue. The server will periodically retry completing the deploy for the service. This message can usually be ignored unless there are async web service applications. To completely disable async web service support, thus avoiding this message, set -Dweblogic.wsee.skip.async.response=true.
	5602	ExecuteRequest failed

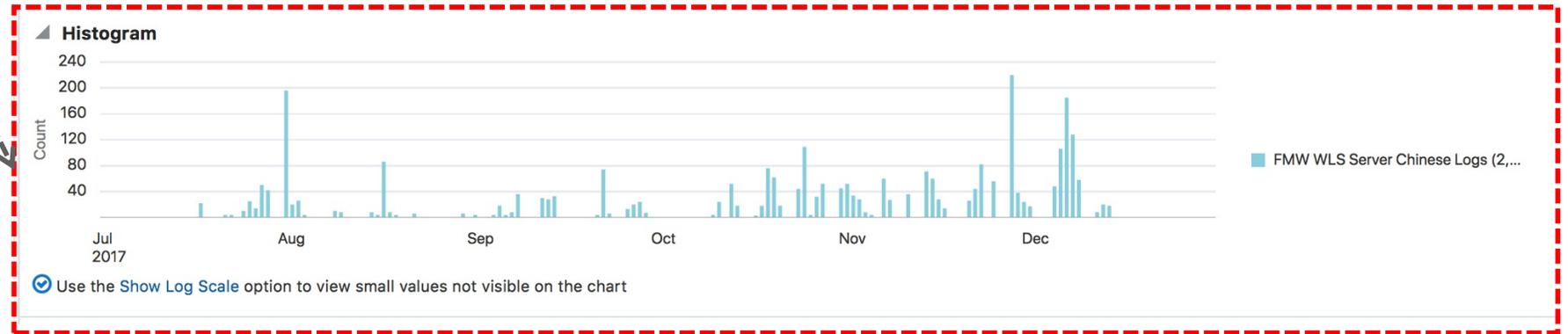
TPC/IP Socket Failures

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;Lweblogic.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

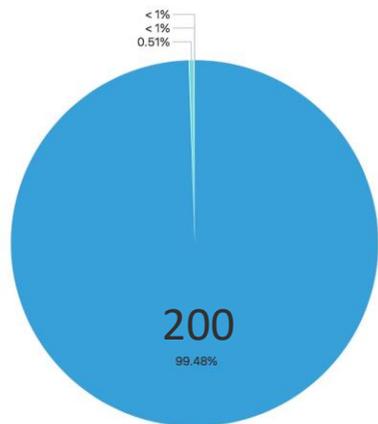


## 有做漏洞扫描? 还是被扫描?

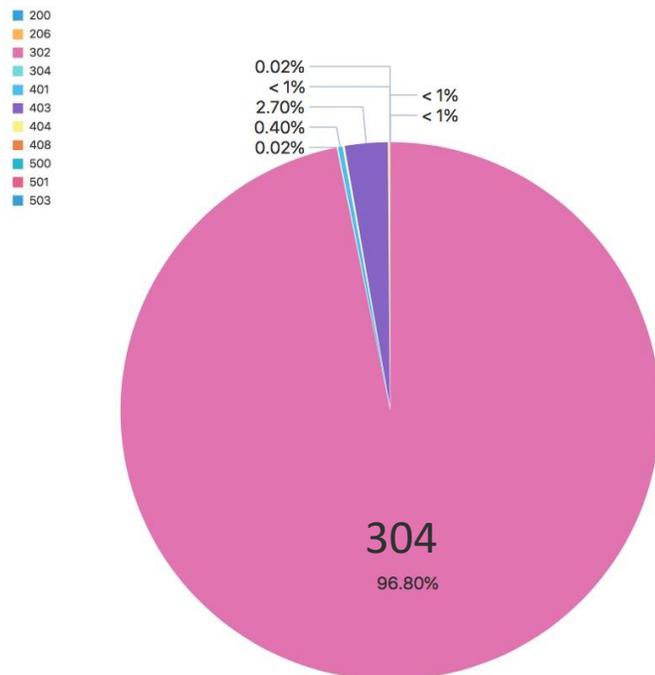
	▶		10	10.112.48.220 - - [22/九月/2017:13:44:21 +0800] "GET /Wsusadmin/Errors/BrowserSettings.aspx HTTP/1.1" 404 1164
	▶		8	The LogBroadcaster on this server failed to broadcast log messages to the admin server. The Admin server may not be running. Message broadcasts to the admin serv
	▶		8	Error looking up session with id:BlmDAhbz_EICqnuauGscNOCjZD5XpO0!140952249!NONE 1 more sample...
	▶		3	The ListenThread because of an error: java.lang.OutOfMemoryError 1 more sample...
	▶		3	Muxer received error: getNewTla

## OutOfMemoryError

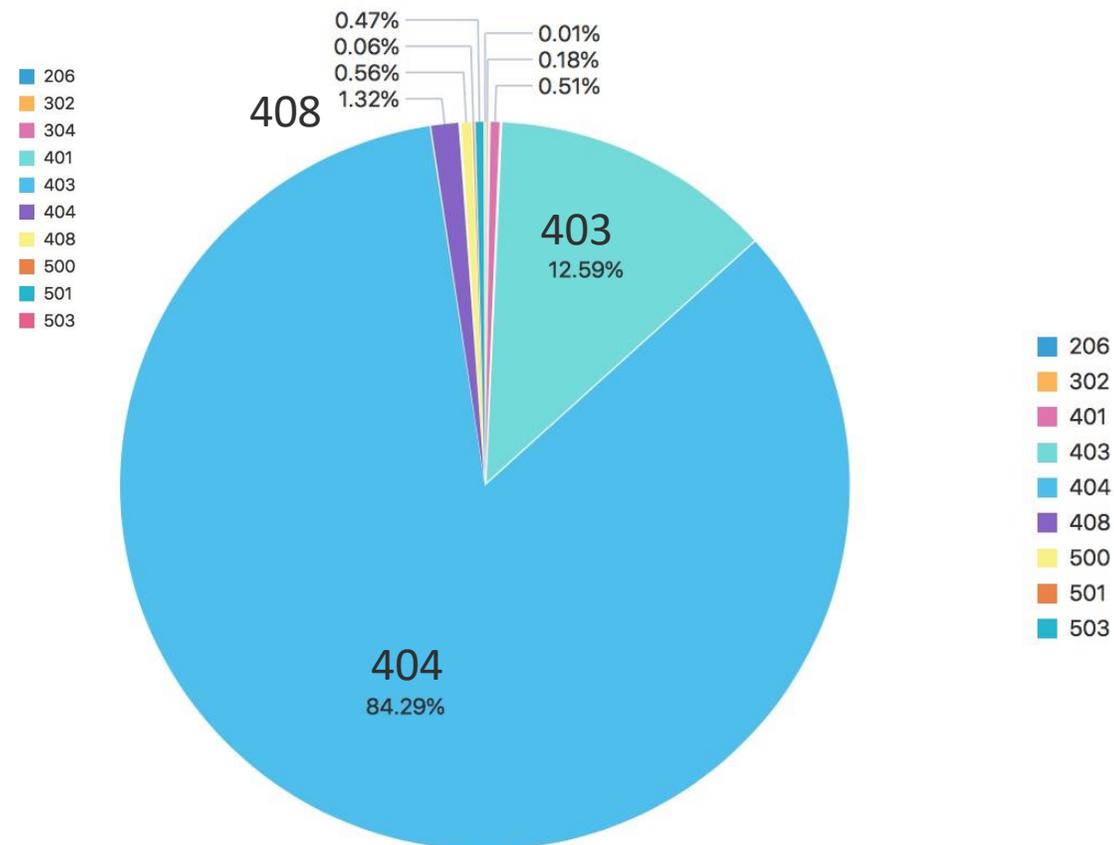
	▶		3	The ListenThread because of an error: java.lang.OutOfMemoryError 1 more sample...
	▶		3	Muxer received error: getNewTla
	▶		3	Deployment service servlet encountered an Exception while handling the deployment service message for request id "-1" from server "AdminServer". Exception is: "java.lang.OutOfMemoryError: getNewTla
	▶		3	An attempt was made to execute the 'distribute' operation on an application named 'hsu' that is not currently available. The application may have been created after non-dynamic configuration changes were activated. If so, the operation can not be performed until server is restarted so that the application will be available.
	▶		1	Unicast receive error : java.lang.OutOfMemoryError: allocLargeObjectOrArray: [B, size 8208



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

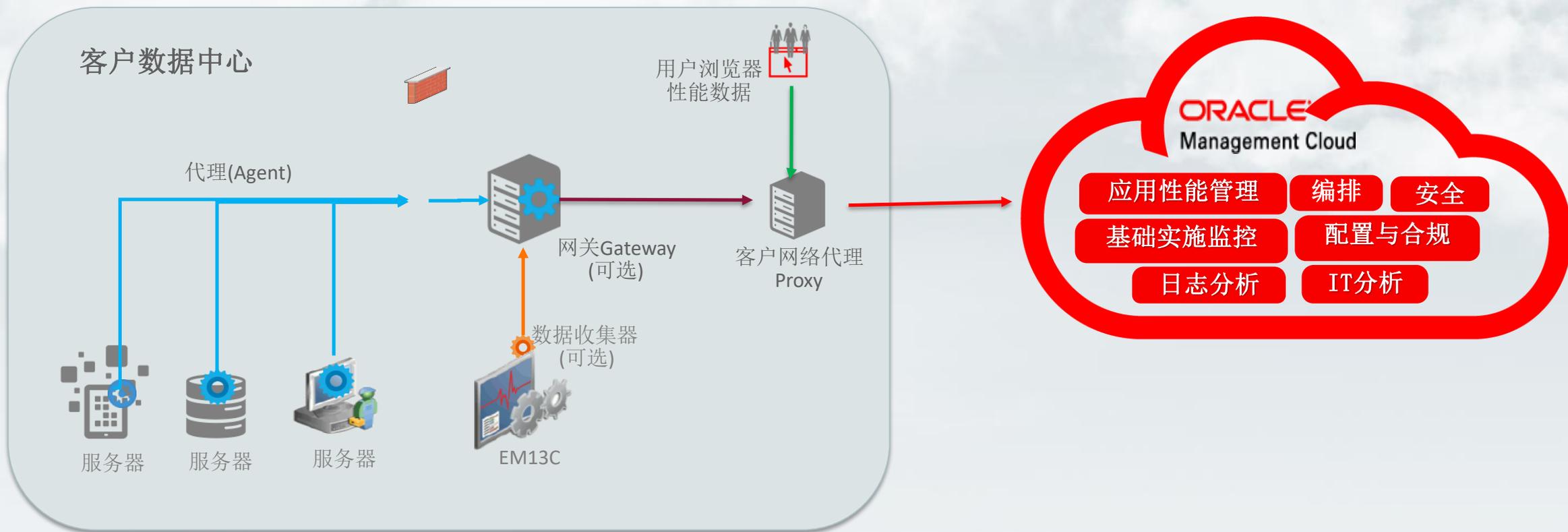
Directory Travel 攻击, 尝试获取密码。失败。

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	u).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	/awstattotals.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	/awstattotals.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	/awstattotals.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	/awstattotals/awstattotals.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	/awstattotals/awstattotals.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	/awstattotals/awstattotals.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	/awstattotals/awstattotals.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

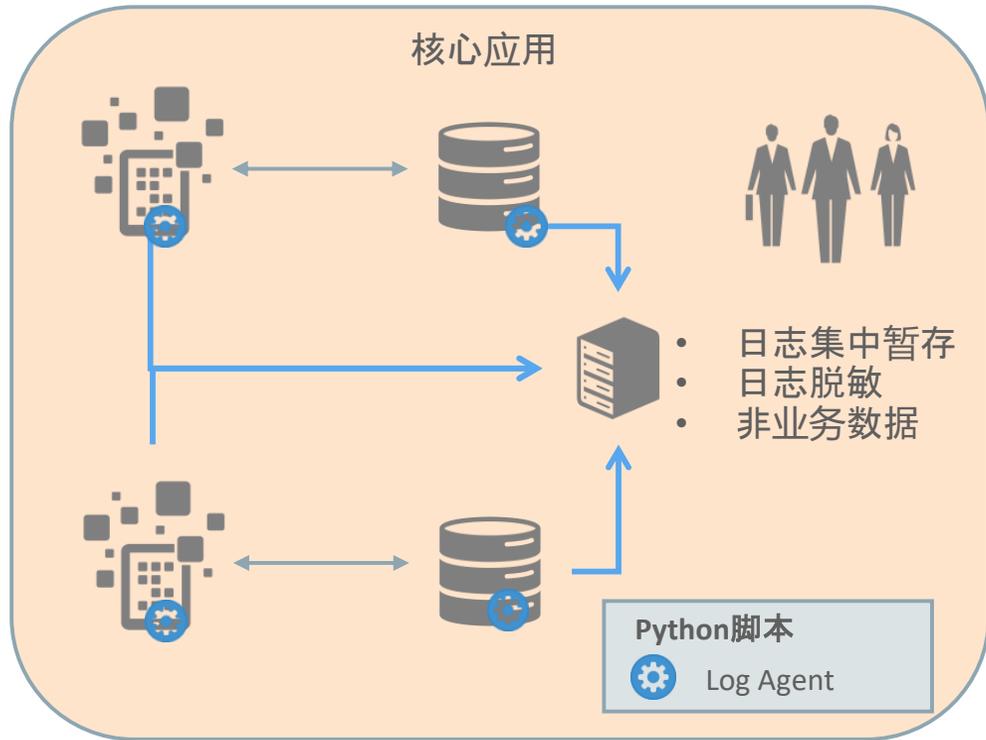


- 协议和端口：[https/443](https://443)

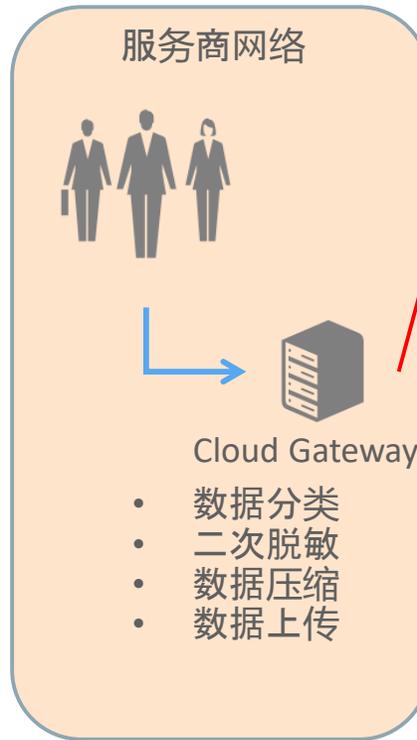
外网访问地址[https://<tenantid>.itom.management.us2.oraclecloud.com/\\*](https://<tenantid>.itom.management.us2.oraclecloud.com/*)

内网访问网关Gateway server (typically 1830)

# OMC的服务模型



Customer Firewall



Https: 443,22

