BiMAP 維運大數據分析

iT 系統效能暨資安維運管理

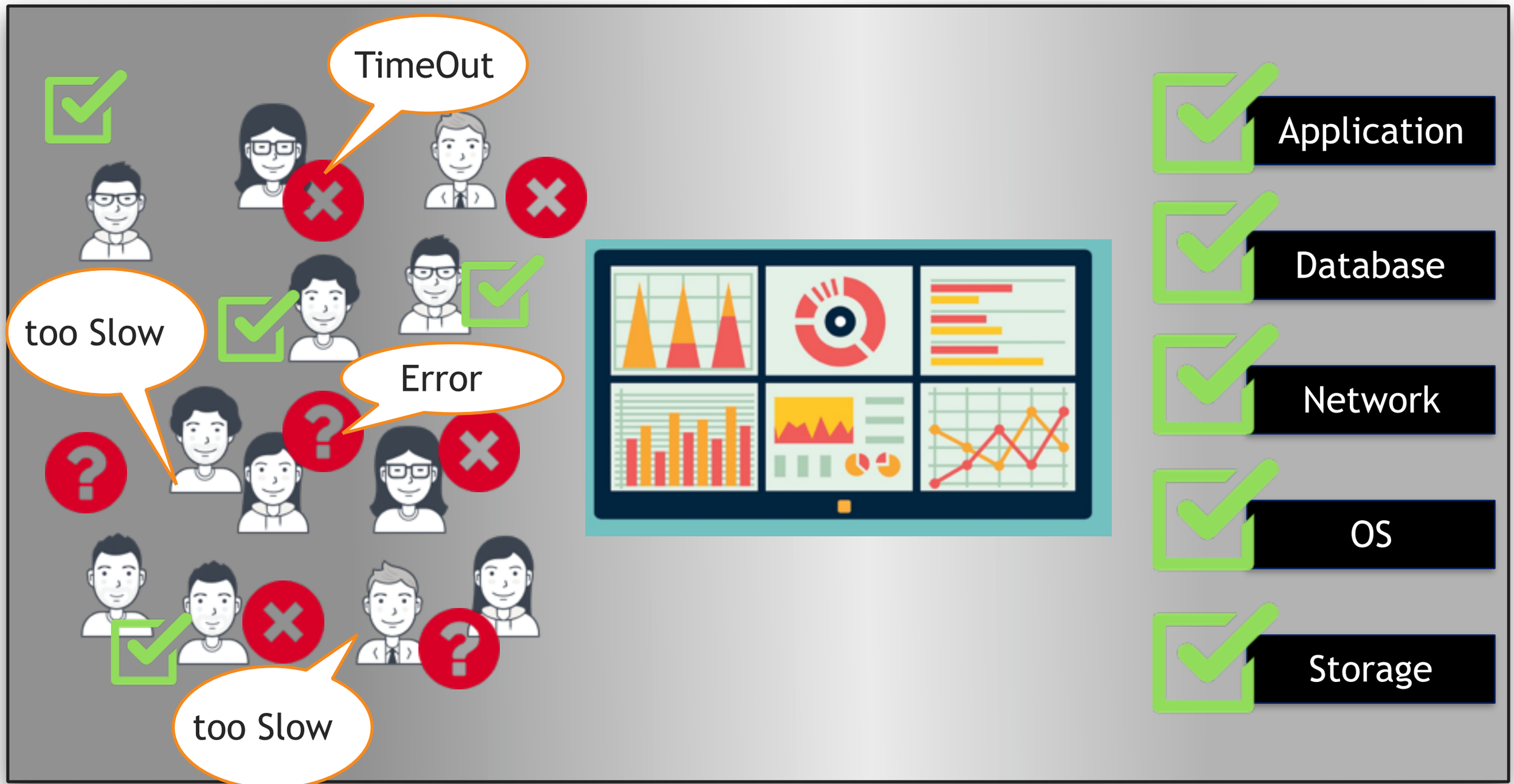
訊達電腦 陳柏霖

2017-06-23

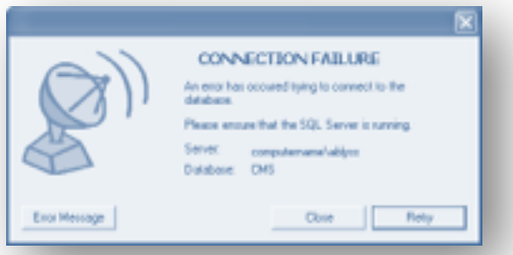
系統效能維運

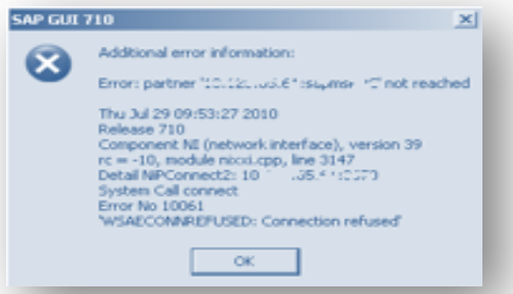
Slowwww

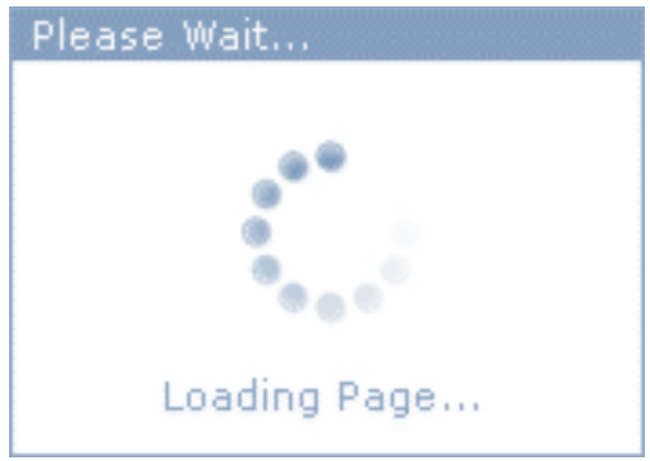
報錯&&緩慢 是用戶最經常抱怨的問題



被動告知&&頭痛醫頭&&難以預防







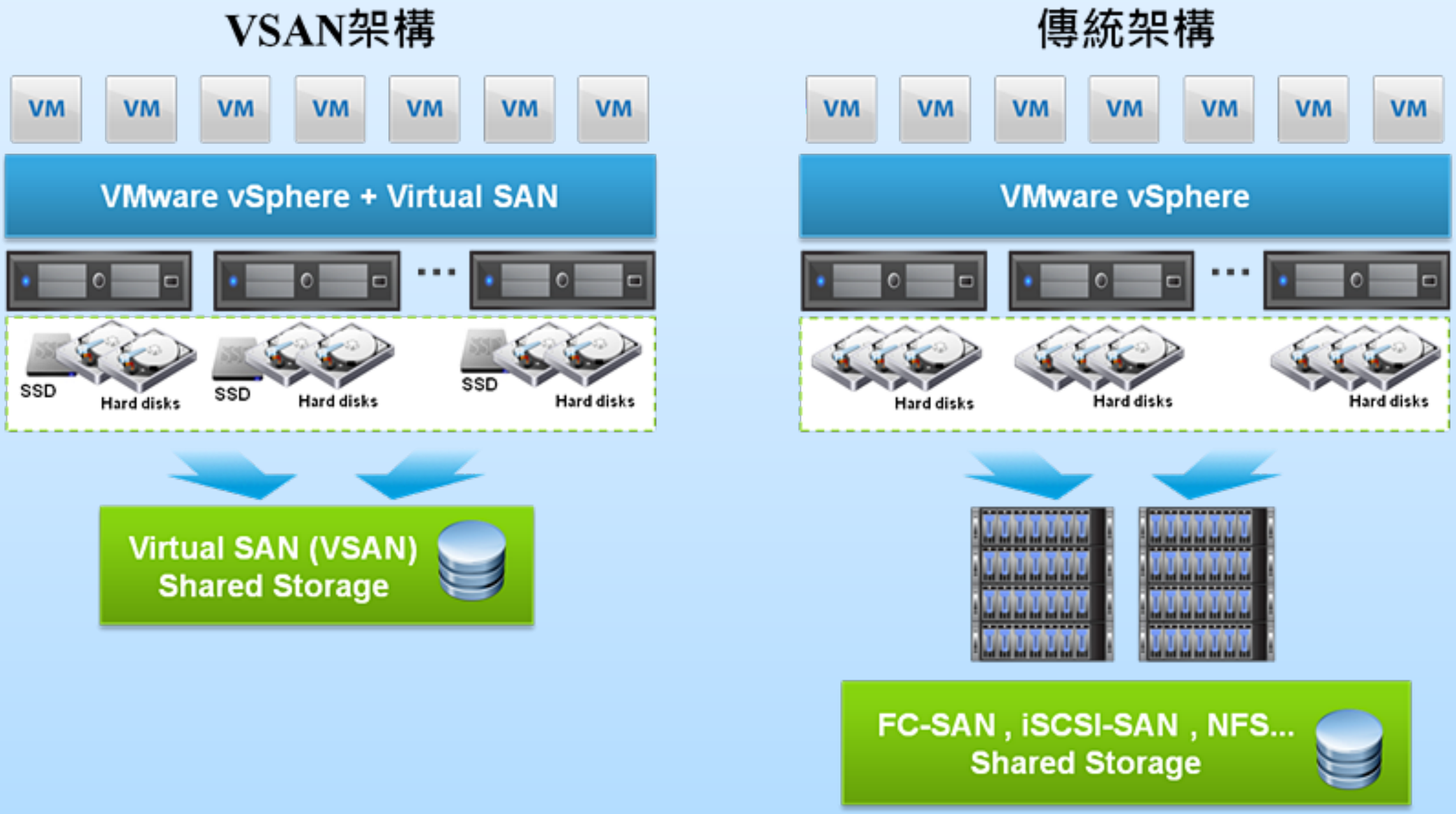
負載過大、用戶等待

運行緩慢、無法登入

應用當機、系統重啟

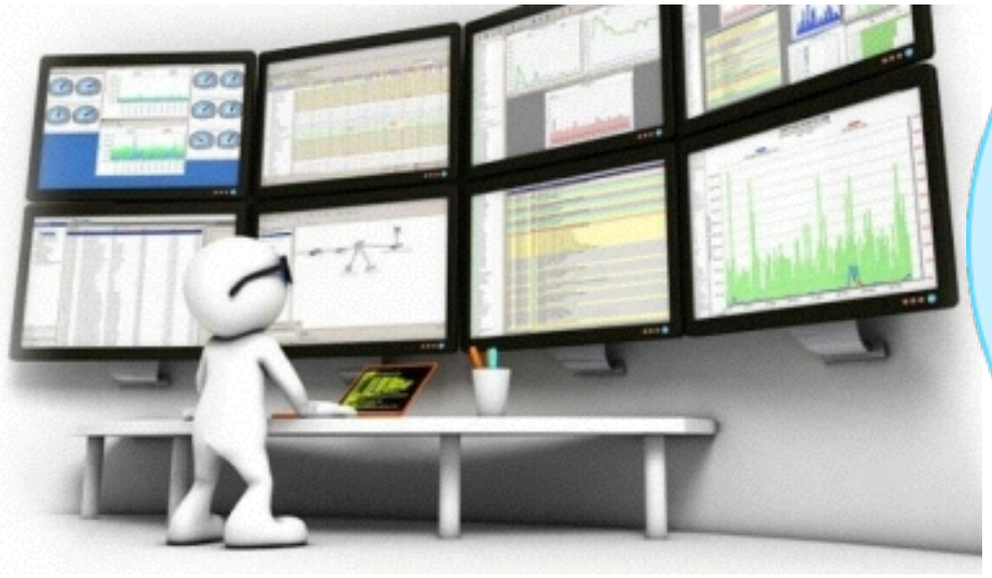
系統複雜 AND 關聯性高

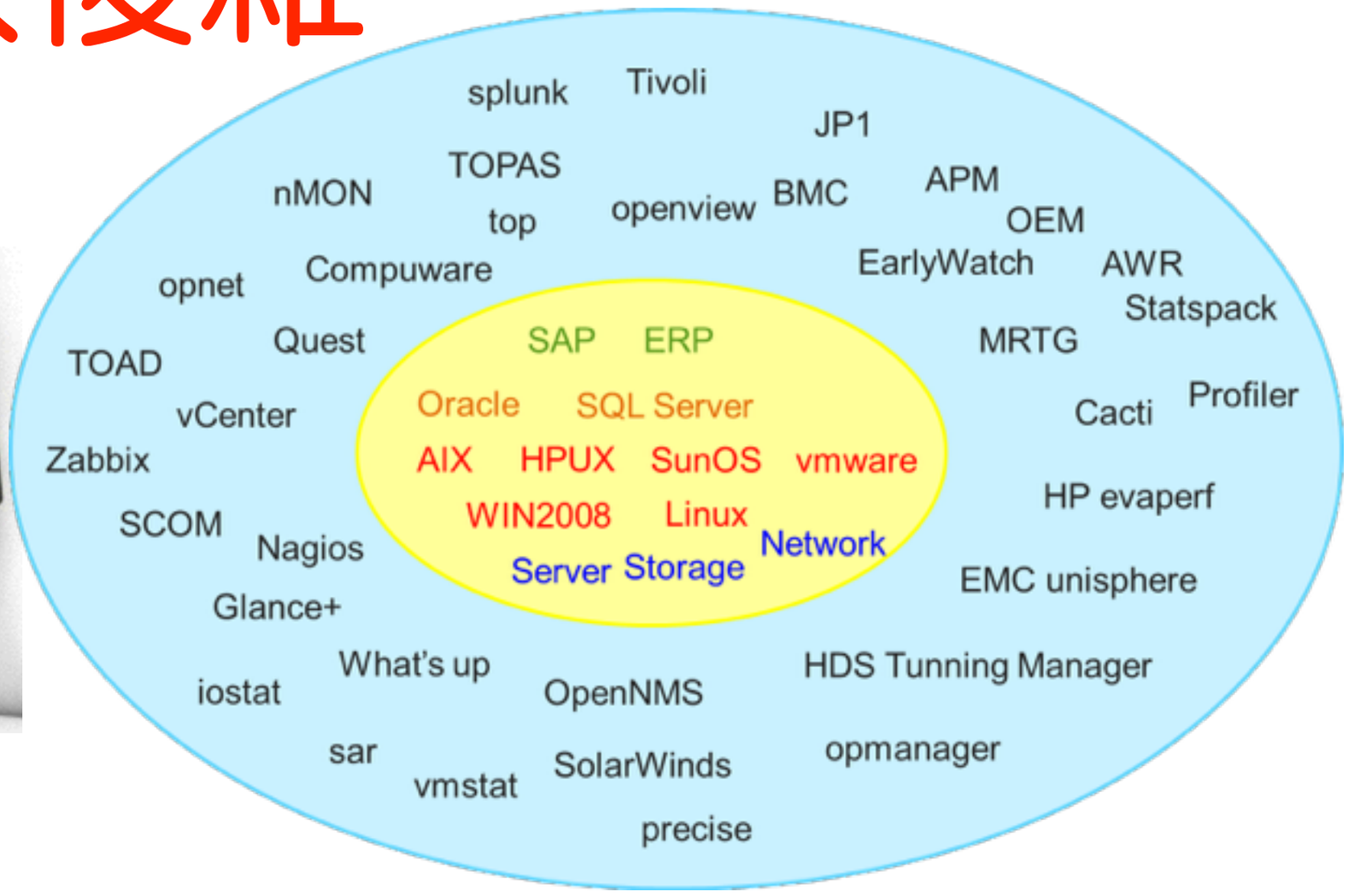
效能問題處理週期.....長



監控工具很多

太貴 or 太複雜





網路
維運&監控

主機
維運&監控

存儲
維運&監控

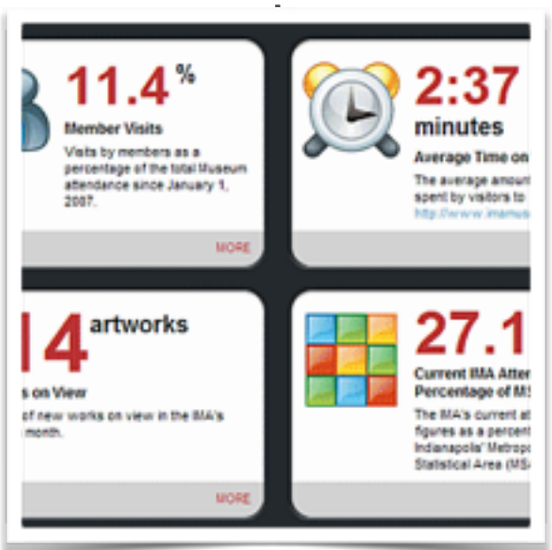
Database
維運&監控

Application
維運&監控

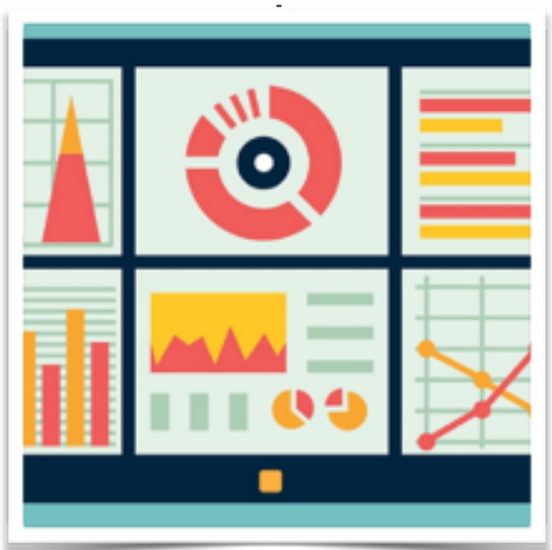
事前預防：提前發現問題 、 降低救火頻率

事中控制：縮短處理週期 、 提升服務品質

事後稽核：管理決策依據 、 提升投資效益



數據化管理



可視化管理

自動化管理

現代IT管理的進化

出問題

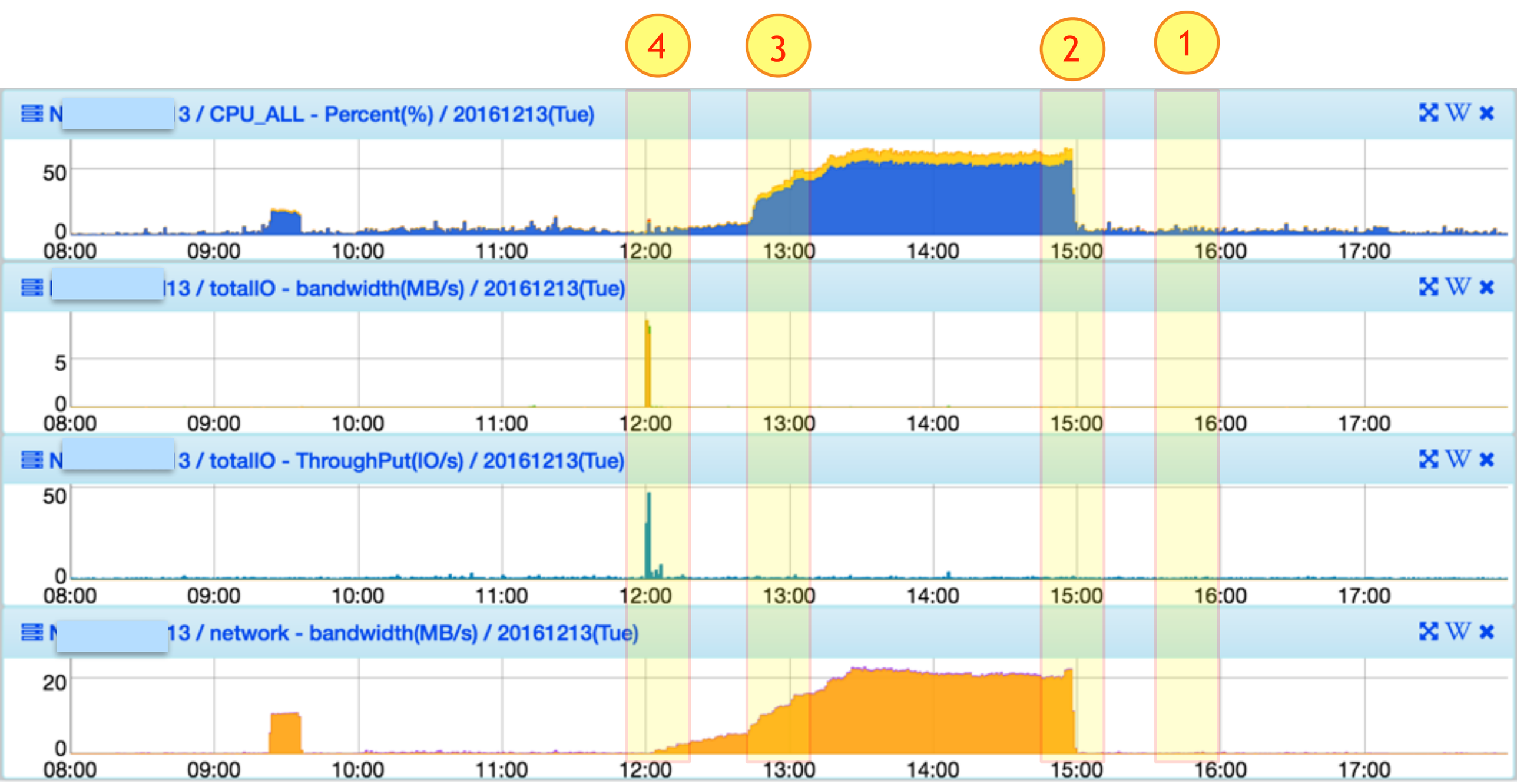
~~問題~~

解決問題

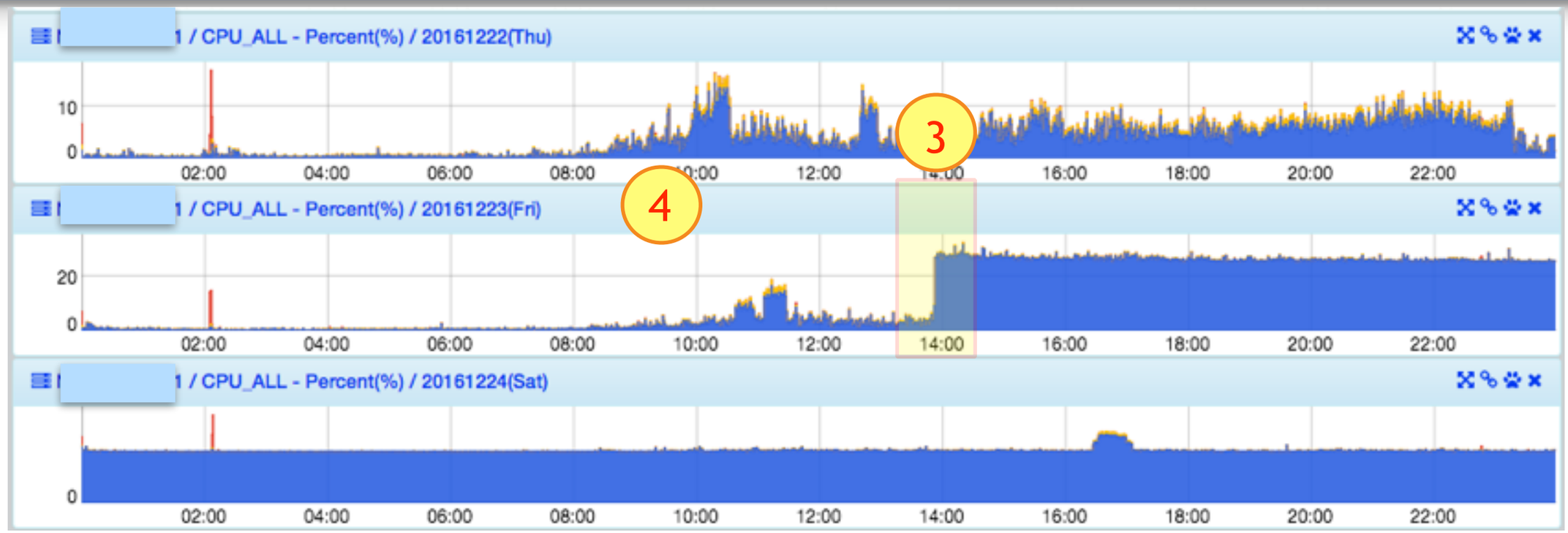
用BiMAP 定位問題
Event Tracking

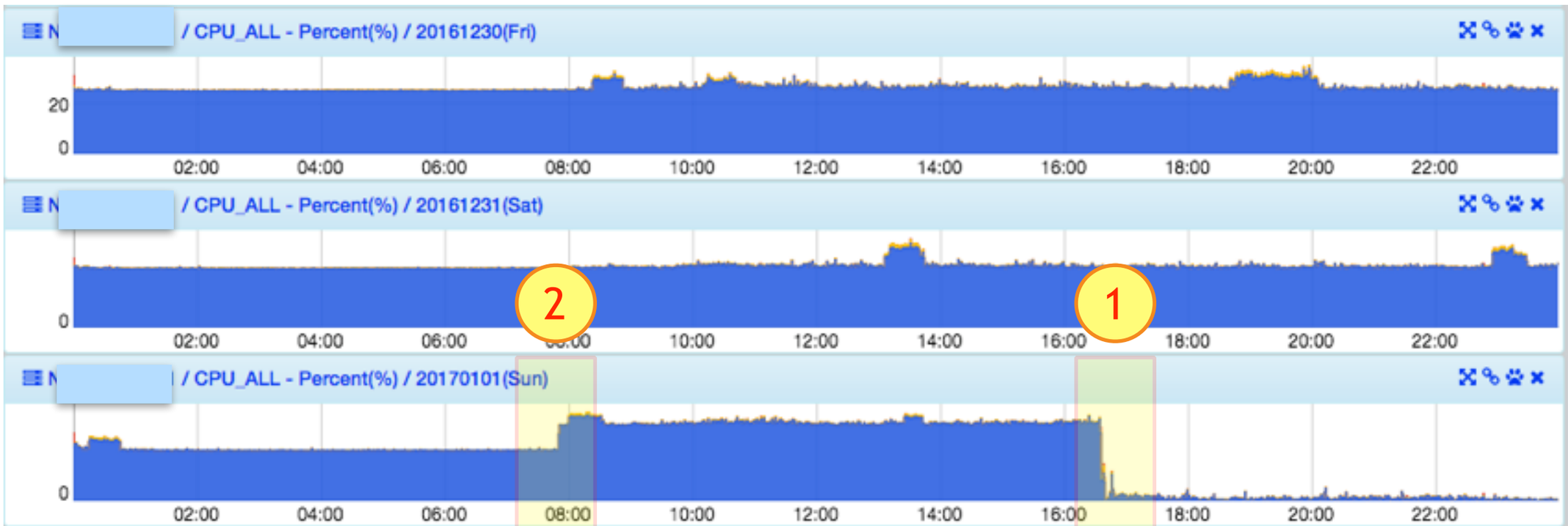
Step1: 發生問題的時間定位

場景一： 幾小時前產生異常

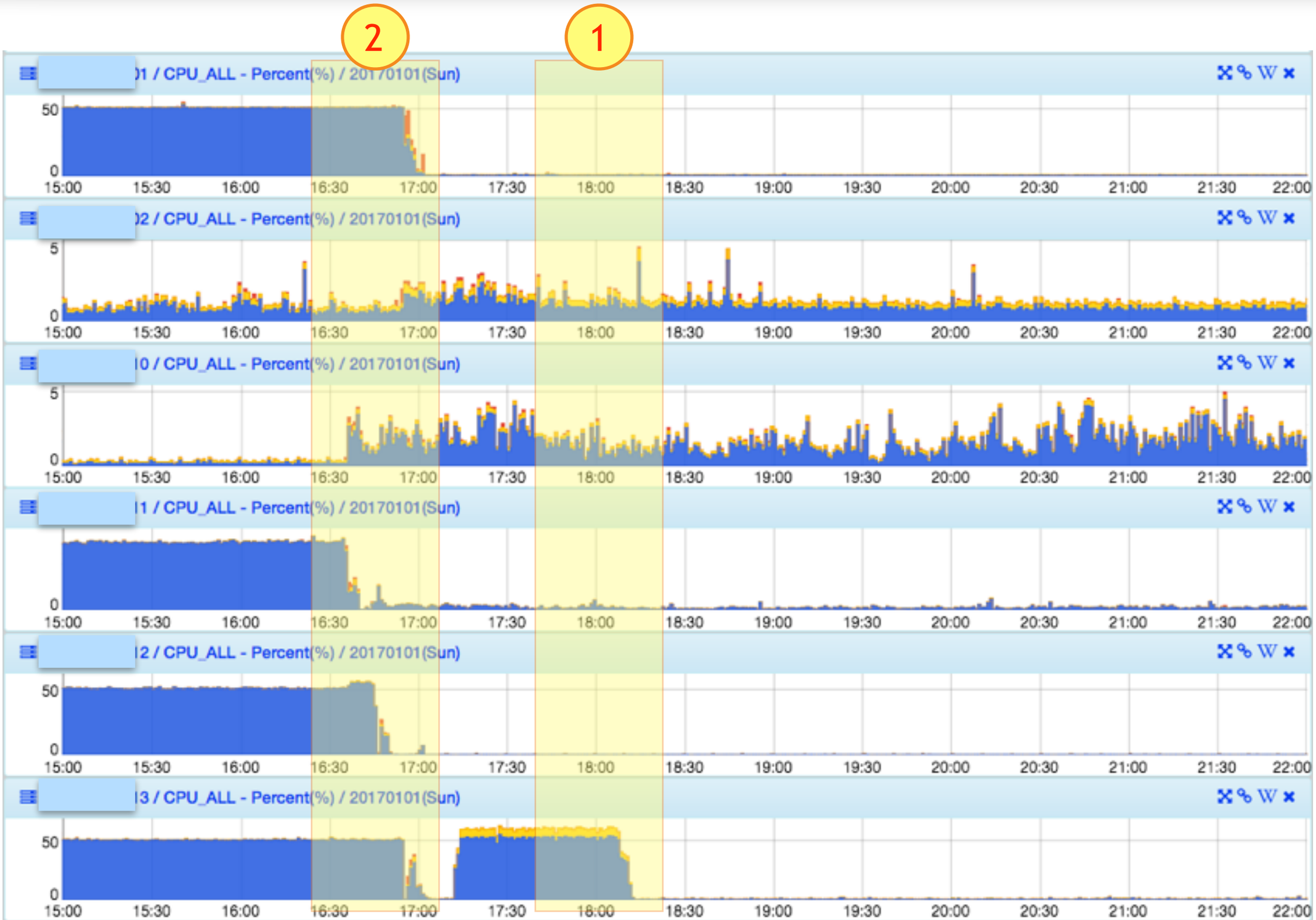


場景二： 多天前產生異常


/ CPU_ALL - Percent(%) / 20161222(Thu)
10
0
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
3
4
/ CPU_ALL - Percent(%) / 20161223(Fri)
20
0
/ CPU_ALL - Percent(%) / 20161224(Sat)


/ CPU_ALL - Percent(%) / 20161230(Fri)
20
0
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
/ CPU_ALL - Percent(%) / 20161231(Sat)
2
1
/ CPU_ALL - Percent(%) / 20170101(Sun)

場景三： 多台同時產生異常



利用大數據分析

1. 創建系統預測模型，有效預防故障產生
2. 準確判斷異常原因，提高問題處理效率

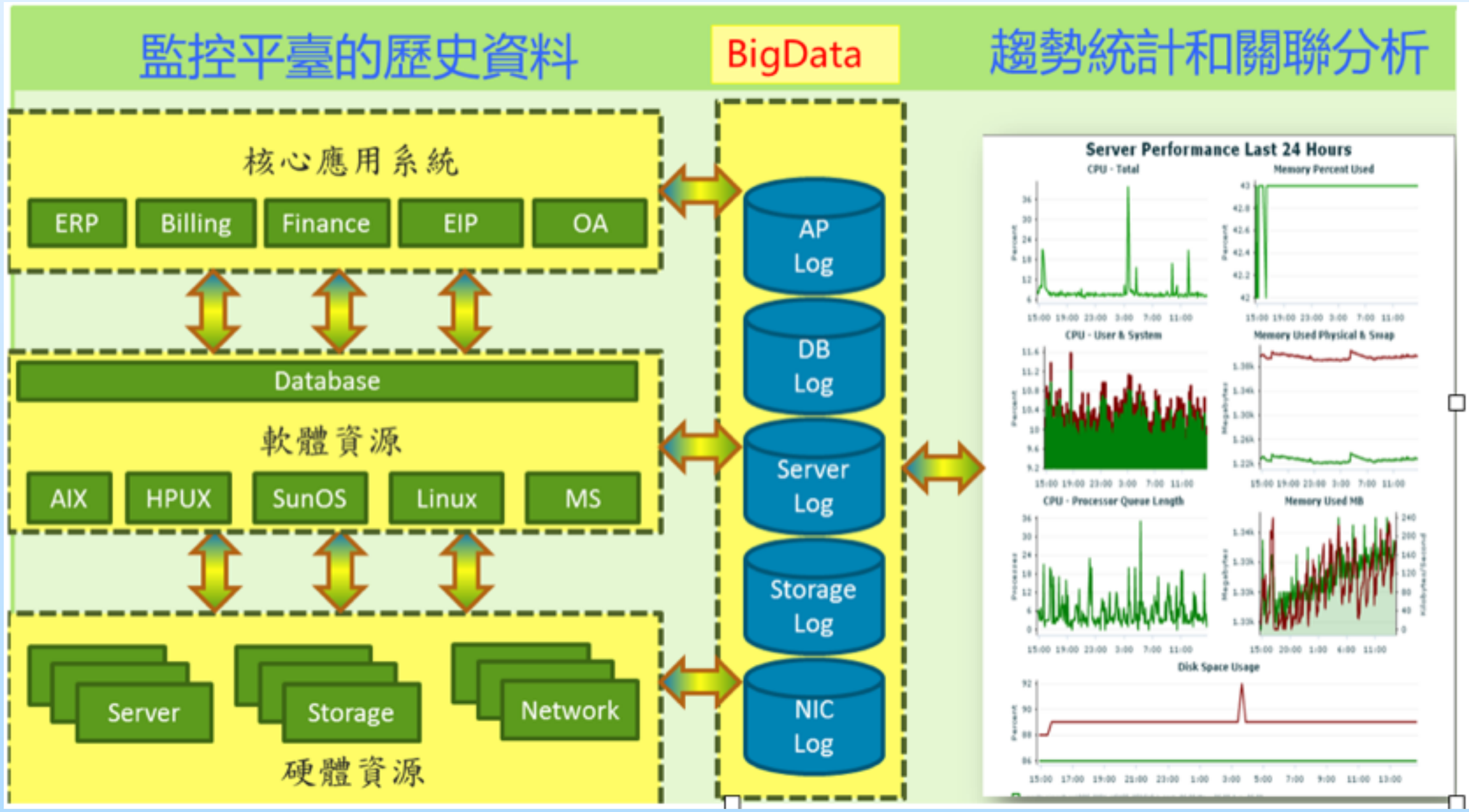
BiMAP

事前預防

利用BiMAP 大數據分析
提前排查系統隱憂

利用大數據分析，落實預防管理模式

- 通過統一收集IT系統的主機、存儲、網絡、OS、DB、AP等相關LOG，利用BIG DATA 的挖掘分析技術，建立關鍵指標的趨勢統計和關聯分析，創建異常前兆的識別模型。

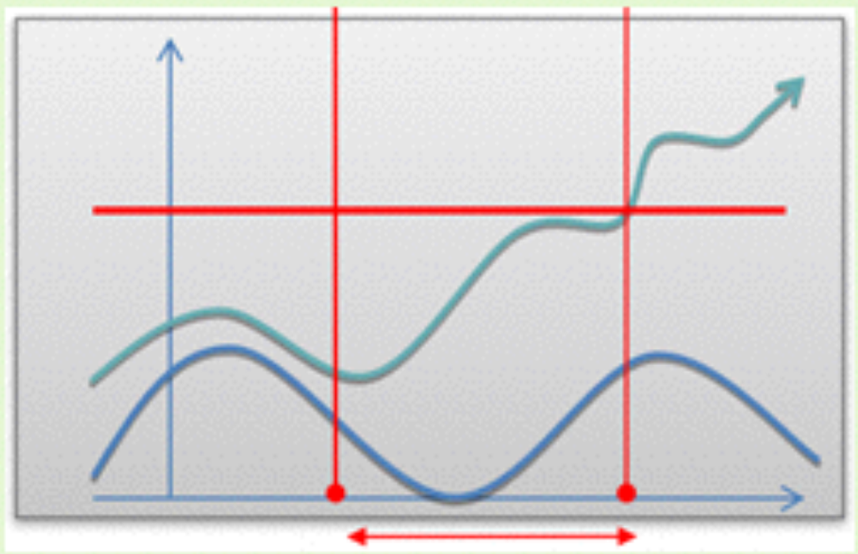


及時判別異常的前兆現象

- 有效的預警機制，來自異常發生前的前兆識別

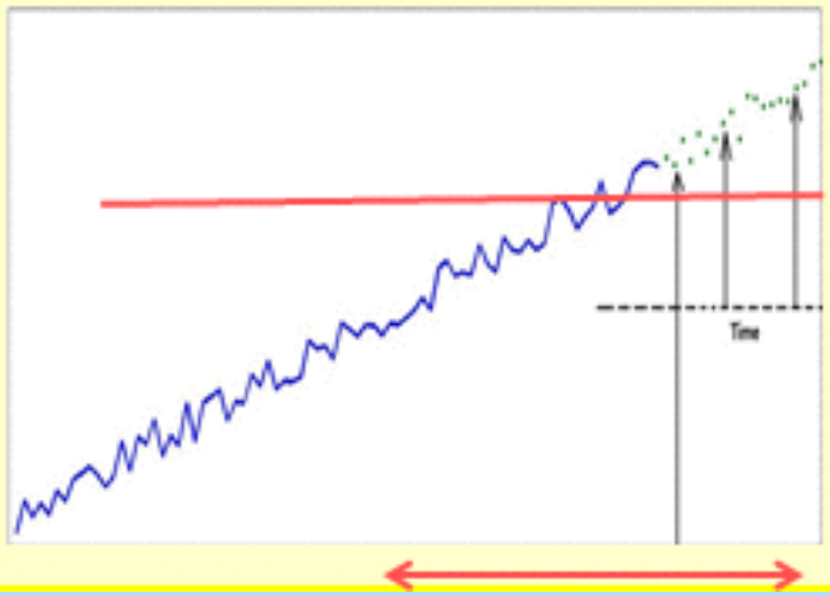
關鍵指標的偏離關係分析 提出預警

經由多個不同KPI的偏離關係分析，在實際業務受到影響之前，發佈預警通報，及時處理問題。



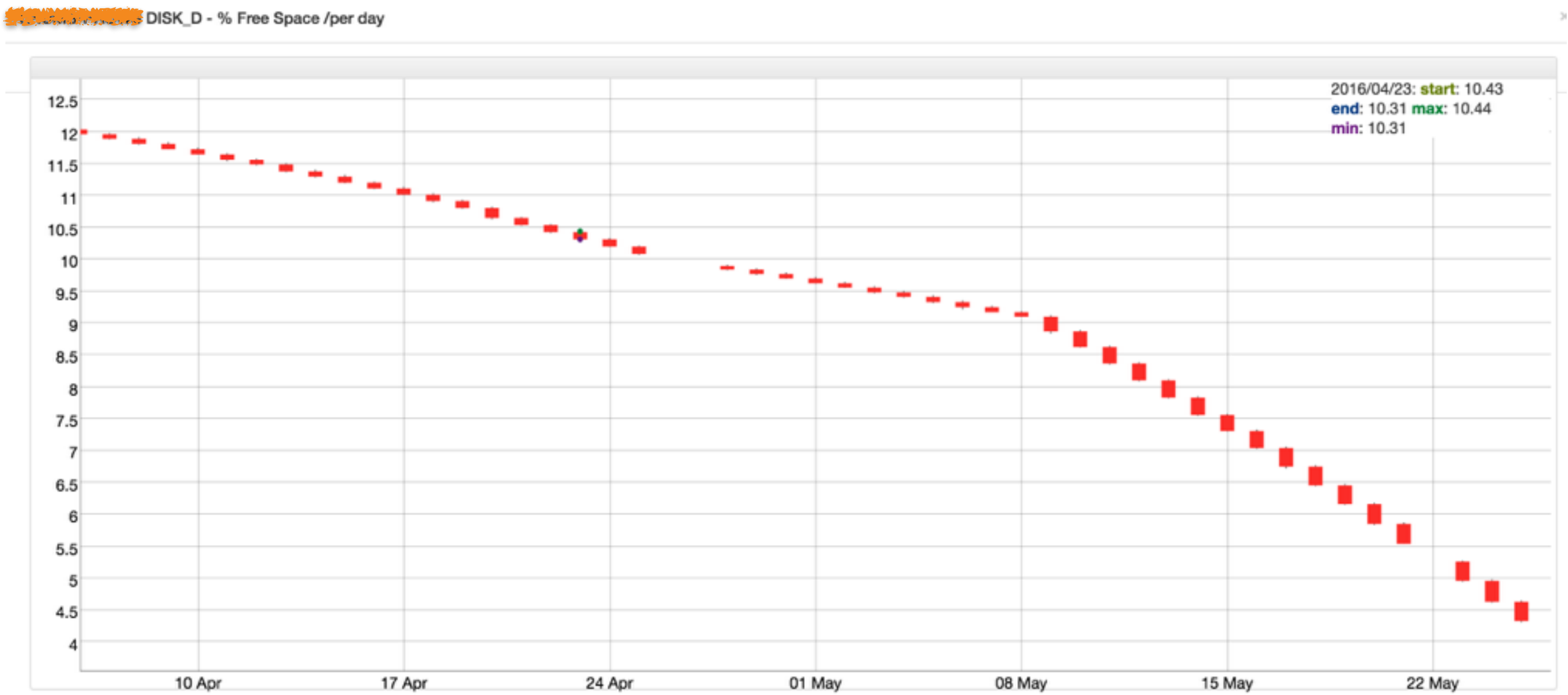
關鍵指標的變動趨勢分析 發佈預警

通過關鍵指標KPI的變動趨勢分析，建立預警模型，辨識出即將達到告警閥值的前兆現象。



利用BiMAP K線圖 提前發現問題

Storage Capacity Plan Trend Analysis

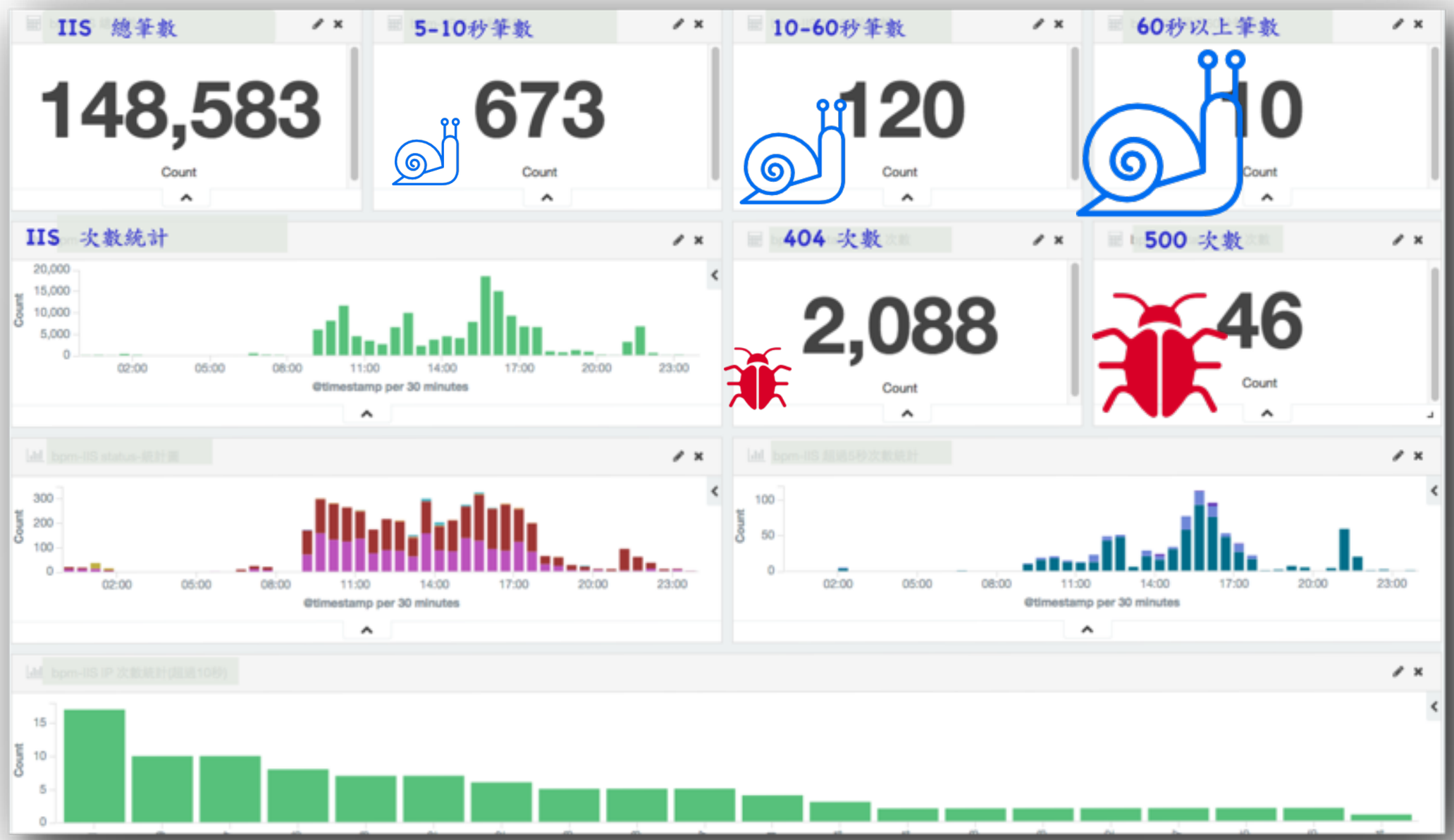


利用BiMAP 預測系統支撐力

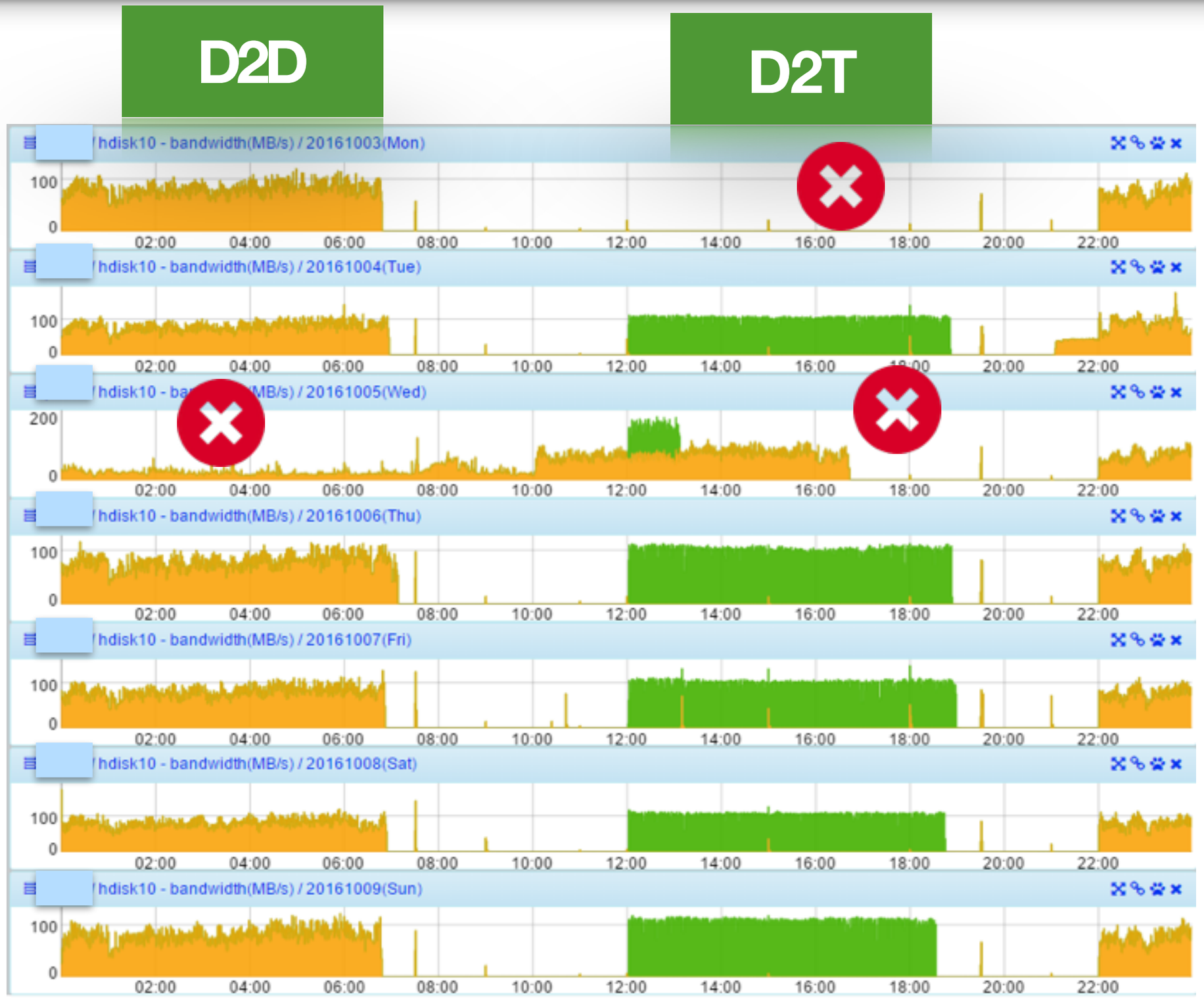
從歷史Log 取得趨勢分析

利用BiMAP 量化軟體品質指標

量化 報錯&&緩慢 指標



利用BiMAP 構建系統模型



利用BiMAP 實施效能規劃

提升系統改造的成功率
規避改善不如預期的風險

- 設備採購後，是否一定可以解決原來的問題？
- 如何規避改善不如預期效果的風險？
- 如何有效評估升級方案的投資效益？

需要多少預算？

需要更高規格的設備？

採購最好設備？

如何保證升級後的改善效果？

如何評估廠商提供產品的技術指標?

是否對症下藥？

系統效能維運

高峰期運行緩慢

準確定位造成系統緩慢的根源，提昇效能問題的處理效率，並提高應用高峰期設備資源的最大利用率。

軟體品質驗收

提供系統上線前軟體品質的驗收方案，提昇應用系統的穩定性，降低系統上線後才發現產生報錯和緩慢的風險。

異常服務中斷

提前挖掘系統隱患並持續追蹤，落實主動維運，提前排除可能造成服務中斷的異常，降低被動救火的次數。

最大支撐力預測

通過歷史日誌的統計分析，建立關鍵指標的趨勢統計預測，避免因業務和資料增長後，產生的系統當機風險。

壓力測試效能評估

評估測試環境下的各種壓測場景的效能瓶頸分析，並預測生產環境的資源最大的應用支撐力。

升級改造採購依據

量化系統實際的應用需求，提供軟、硬體的採購依據，提供iT 投資效益，避免設備升級後改善不如預期的風險。

大數據分析的關鍵三因素

訊達 分析能力

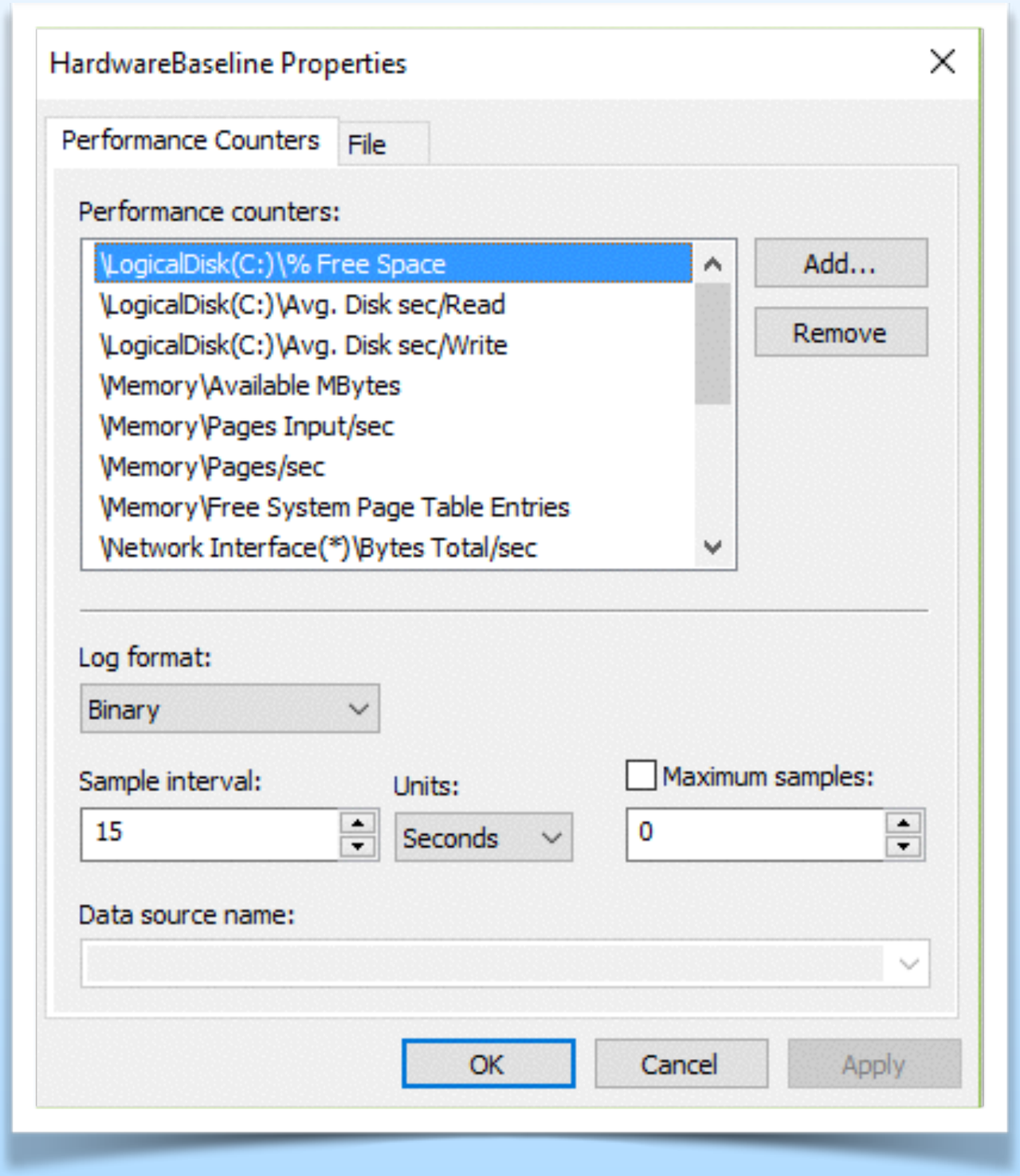
分析工具 BiMAP

用戶 日誌＋資料

Window 效能log - logman

Win 效能監控工具

1. CPU 負載
2. 多核CPU負載
3. 內存負載
4. 虛擬內存
5. Disk 負載
6. MPIO 負載
7. Network 負載
8. Disk 容量
9. process 負載



Linux 效能log - Sysstat

Linux 效能監控工具

1. CPU 負載
2. 多核CPU負載
3. 內存負載
4. 虛擬內存
5. Disk 負載
6. MPIO 負載
7. Network 負載
8. Disk 容量
9. process 負載

```
File  Edit  View  Terminal  Help
top - 03:28:25 up  5:08,  4 users,  load average: 0.03, 0.05, 0.01
Tasks: 218 total,   2 running, 216 sleeping,   0 stopped,   0 zombie
Cpu0  :  0.7%us,  1.3%sy,  0.0%ni, 98.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu1  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu2  :  0.0%us,  0.0%sy,  0.0%ni,100.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Cpu3  :  0.7%us,  0.0%sy,  0.0%ni, 99.3%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   8193284k total,  2054268k used,  6139016k free,   184712k buffers
Swap:        0k total,        0k used,        0k free,  1099976k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 7287 vivek     20   0  715m 175m  28m S    1  2.2   1:55.96 firefox
 7485 vivek     20   0  212m  16m  10m S    1  0.2   0:02.33 gnome-terminal
   75 root      15  -5     0    0    0 S    0  0.0   0:02.66 scsi_eh_4
 1520 root      20   0 22180 1240 1040 S    0  0.0   0:05.19 hald-addon-stor
 1554 root      20   0  387m  47m  15m S    0  0.6   9:44.74 Xorg
 7352 vivek     20   0  146m  31m  11m S    0  0.4   0:16.51 npviewer.bin
    1 root      20   0 19456 1880 1204 S    0  0.0   0:01.01 init
    2 root      15  -5     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      RT  -5     0    0    0 S    0  0.0   0:00.01 migration/0
    4 root      15  -5     0    0    0 S    0  0.0   0:00.09 ksoftirqd/0
    5 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/0
    6 root      RT  -5     0    0    0 S    0  0.0   0:00.00 migration/1
    7 root      15  -5     0    0    0 S    0  0.0   0:00.03 ksoftirqd/1
    8 root      RT  -5     0    0    0 S    0  0.0   0:00.00 watchdog/1
```

Unix 效能log - nMON

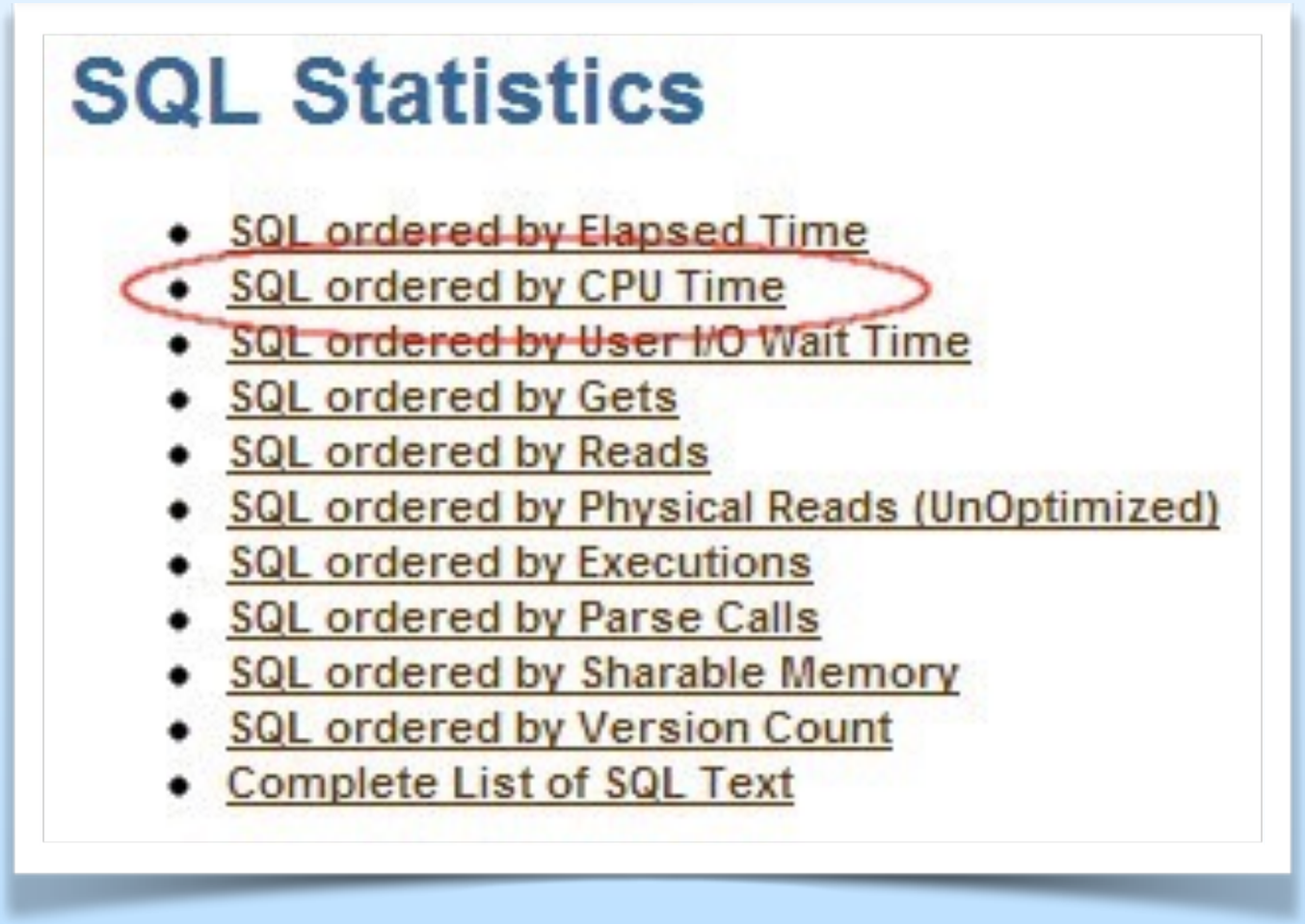
Unix 效能監控工具

1. 系統配置
2. CPU 負載
3. 多核CPU負載
4. 內存負載
5. 虛擬內存
6. Disk 負載
7. MPIO 負載
8. Network 負載
9. mount point 容量
10. process 負載

```
nmon-13g———[H for help]——Hostname=nas02———Refresh= 2secs ——01:37.29——
CPU Utilisation
                          +-------------------------------------------------+
CPU  User%  Sys% Wait% Idle|0          |25         |50         |75        100|
 1   0.0    0.0   0.0  100.0| >                                              |
                          +-------------------------------------------------+
Memory Stats
              RAM      High       Low      Swap
 Total MB    2989.8     -0.0      -0.0     684.0
 Free  MB    2666.9     -0.0      -0.0     684.0
 Free Percent  89.2%   100.0%    100.0%    100.0%
            MB                      MB                      MB
                        Cached=    91.5     Active=    236.7
 Buffers=    18.6 Swapcached=     0.0  Inactive =     43.3
 Dirty  =     0.0 Writeback =     0.0  Mapped   =     13.0
 Slab   =    13.9 Commit_AS =   294.0 PageTables=      2.9
Virtual-Memory
nr_dirty    =       -1 pgpgin      =       0                 High Normal     DMA
nr_writeback=       -1 pgpgout     =       0 alloc             0      0       0
nr_unstable =       -1 pgpswpin    =       0 refill            0      0       0
nr_table_pgs=       68 pgpswpout   =       0 steal             0      0       1
nr_mapped   =       -1 pgfree      =       0 scan_kswapd       0      0       0
nr_slab     =       -1 pgactivate  =       0 scan_direct       0      0       0
                       pgdeactivate=       0
allocstall  =        0 pgfault     =       0 kswapd_steal      =      0
pageoutrun  =        0 pgmajfault  =       0 kswapd_inodesteal=       0
slabs scanned=       0 pgrotated   =       0 pginodesteal      =      0
Kernel Stats
 RunQueue              1   Load Average    CPU use since boot time
 ContextSwitch      17.0    1 mins  0.00    Uptime Days=  0 Hours=11 Mins=16
 Forks               0.0    5 mins  0.00    Idle   Days=  0 Hours=11 Mins=15
 Interrupts         26.5   15 mins  0.00    Average CPU use=  0.21%
Network I/O
I/F Name Recv=KB/s Trans=KB/s packin packout insize outsize Peak->Recv Trans
      lo      0.0      0.0       0.0      0.0     0.0     0.0        0.3     0.3
    eth0      0.0      0.0       0.0      0.0     0.0     0.0        0.0     0.0
    eth1      0.0      0.2       0.5      0.5    70.0   354.0        4.9   487.0
    ppp0      0.0      0.0       0.0      0.0     0.0     0.0        0.0     0.0
Disk I/O ——/proc/diskstats——mostly in KB/s——Warning:contains duplicates——
DiskName Busy  Read WriteKB|0          |25         |50         |75        100|
sda        0%    0.0    0.0|>                                               |
```

Oracle 效能log -AWR

1.TOP 10 SQL 語法
2.表空間I/O 使用量
3.File I/O 使用量
4.Oracle 系統參數



VMware 效能log - esxtop

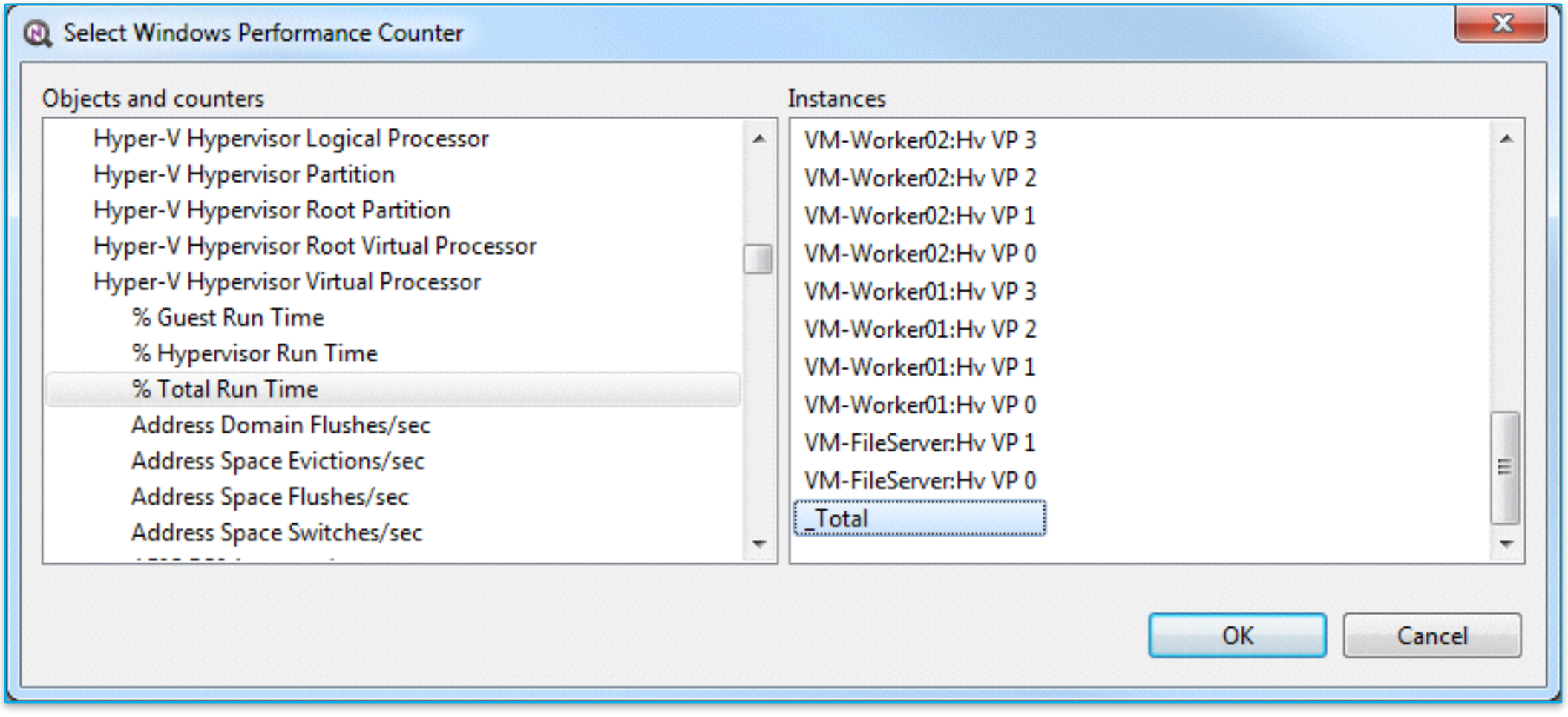
- CPU
- Memory
- Network
- Disk Adapter
- Disk Device
- Disk VM

```
10:25:57pm up 49 days  1:25, 432 worlds, 12 VMs, 23 vCPUs; MEM overcommit avg: 0.00, 0.00, 0.00
PMEM  /MB: 196562   total:  2152     vmk, 41759 other, 152650 free
VMKMEM/MB: 196178 managed:  2576 minfree,  6909 rsvd, 189268 ursvd,  high state
NUMA  /MB: 98258 (78164), 98304 (74093)
PSHARE/MB:    82  shared,    19  common:    63 saving
SWAP  /MB:     0    curr,     0 rclmtgt:                0.00 r/s,   0.00 w/s
ZIP   /MB:     0  zipped,     0   saved
MEMCTL/MB:     0    curr,     0  target, 28631 max

    GID NAME             MEMSZ    GRANT     SZTGT     TCHD    TCHD_W    SWCUR    SWTGT    SWR/s    SWW/s  LLSWR/s  LLSWW/s   OVHDUW     OVHD  OVHDMAX
4849766 papaya         4096.00  2084.00   2325.98   163.84    163.84     0.00     0.00     0.00     0.00     0.00     0.00     6.64    32.34    47.37
4849768 vm-vmx.2773816 4096.00  2084.00   2325.98   163.84    163.84     0.00     0.00     0.00     0.00     0.00     0.00     6.64    32.34    47.37
4849769 vm-vmm.2773816 4096.00  2084.00   2325.98   163.84    163.84     0.00     0.00     0.00     0.00     0.00     0.00     6.64    32.34    47.37
4629546 snarf          4096.00  4096.00   4128.28   286.72    204.80     0.00     0.00     0.00     0.00     0.00     0.00     6.64    37.04    47.37
4629548 vm-vmx.2647453 4096.00  4096.00   4128.28   286.72    204.80     0.00     0.00     0.00     0.00     0.00     0.00     6.64    37.04    47.37
4629549 vm-vmm.2647453 4096.00  4096.00   4128.28   286.72    204.80     0.00     0.00     0.00     0.00     0.00     0.00     6.64    37.04    47.37
4630108 liono          4096.00  1710.00   1913.65   286.72    286.72     0.00     0.00     0.00     0.00     0.00     0.00     6.64    31.42    47.37
4630110 vm-vmx.2647818 4096.00  1710.00   1913.65   286.72    286.72     0.00     0.00     0.00     0.00     0.00     0.00     6.64    31.42    47.37
4630111 vm-vmm.2647818 4096.00  1710.00   1913.65   286.72    286.72     0.00     0.00     0.00     0.00     0.00     0.00     6.64    31.42    47.37
4794112 slee-bos-v30-vm 4096.00 4096.00   4137.51   368.64    368.64     0.00     0.00     0.00     0.00     0.00     0.00     6.64    40.27    47.37
4794114 vm-vmx.2741981 4096.00  4096.00   4137.51   368.64    368.64     0.00     0.00     0.00     0.00     0.00     0.00     6.64    40.27    47.37
4794115 vm-vmm.2741981 4096.00  4096.00   4137.51   368.64    368.64     0.00     0.00     0.00     0.00     0.00     0.00     6.64    40.27    47.37
4737414 larrivee       4096.00  1362.00   1529.87    81.92     40.96     0.00     0.00     0.00     0.00     0.00     0.00     6.58    30.43    47.30
```

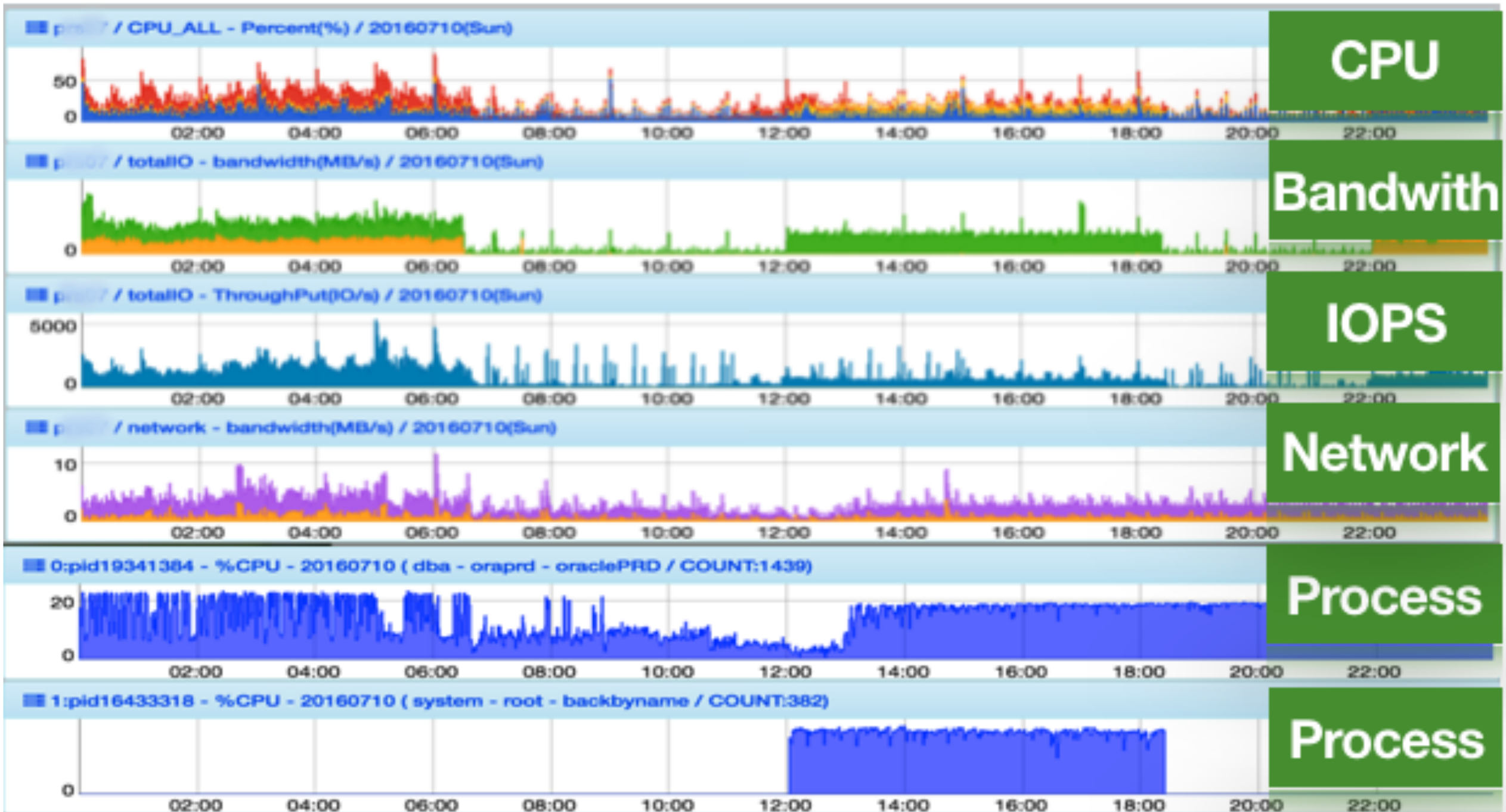
hyper-V 效能計數器

- CPU
- Memory
- Network
- Disk Adapter
- Disk Device
- Disk VM

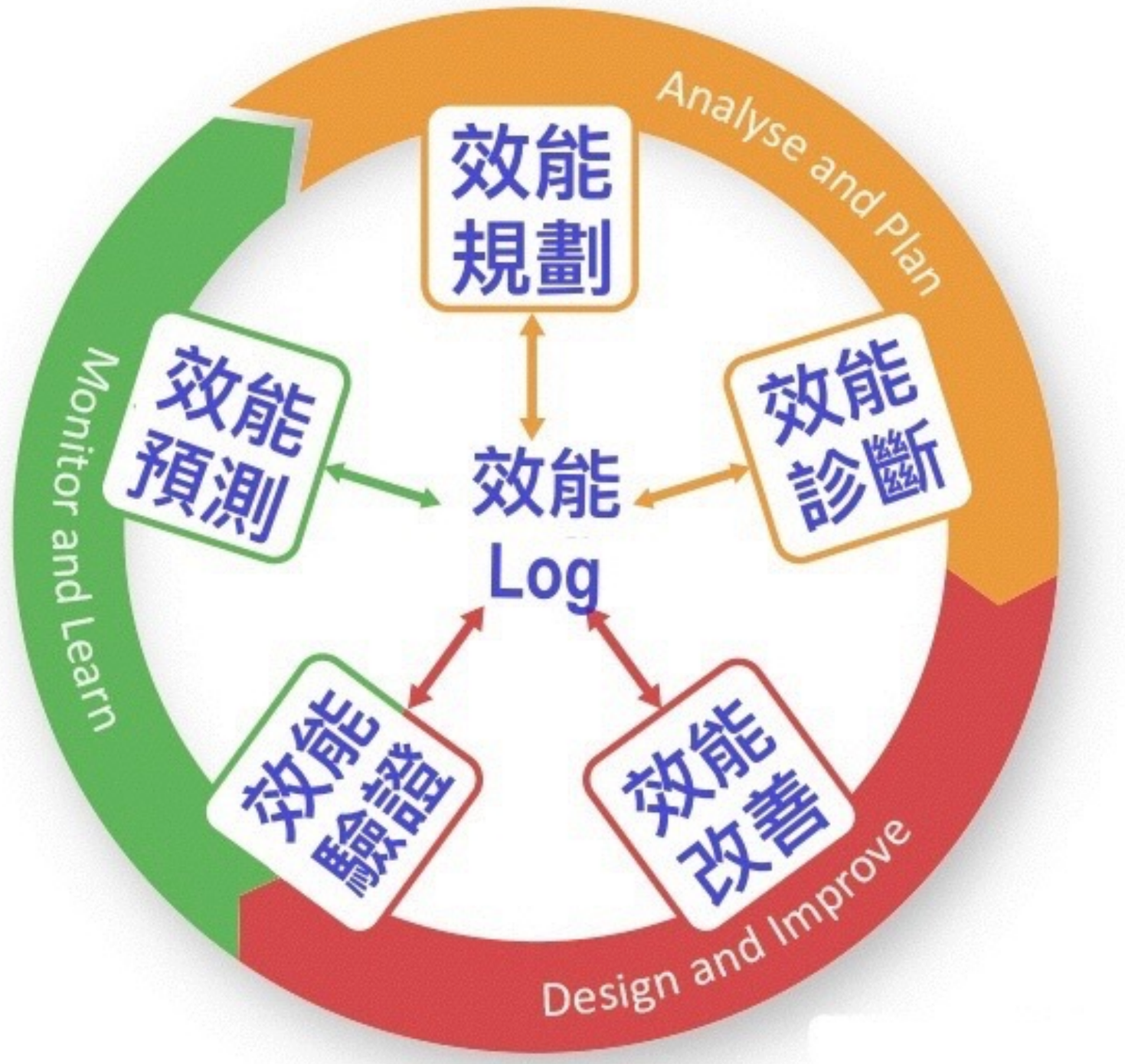


應用軟體效能關聯分析

Software Process PID關聯分析



系統效能管控範圍



效能log

- NMON
- glance
- OSWatcher
- LOGMAN
- AWR
- NAR/NAZ
- 3PAR

資安日誌分析

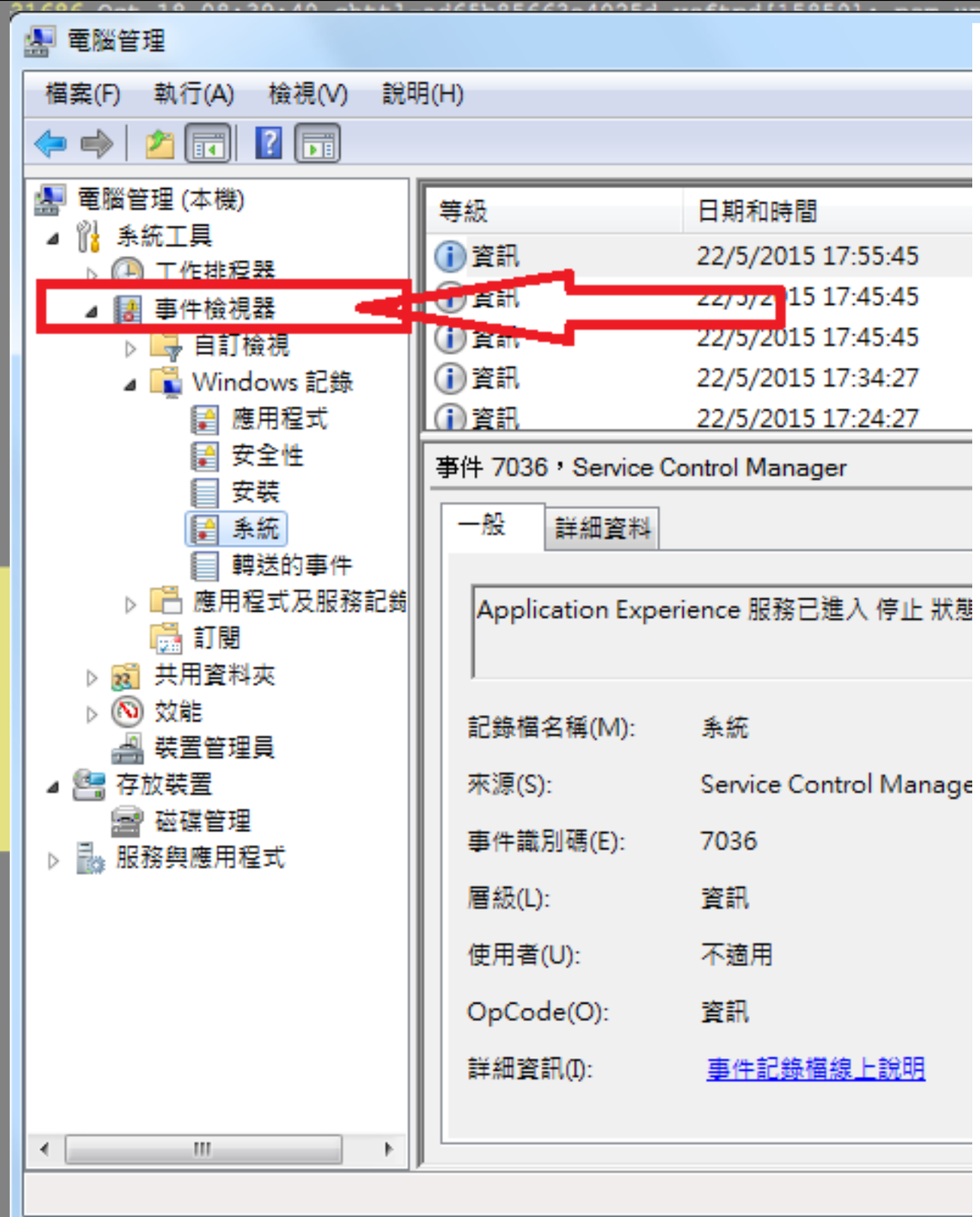
凡走過必留下痕跡 – 登錄Log


```
31686 Oct 18 08:39:40 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): check pass; user unknown
31687 Oct 18 08:39:40 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31688 Oct 18 08:39:40 chttl-ad65b85663e4025d vsftpd[15859]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31689 Oct 18 08:39:43 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): check pass; user unknown
31690 Oct 18 08:39:43 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31691 Oct 18 08:39:43 chttl-ad65b85663e4025d vsftpd[15859]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31692 Oct 18 08:39:46 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): check pass; user unknown
31693 Oct 18 08:39:46 chttl-ad65b85663e4025d vsftpd[15859]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31694 Oct 18 08:39:46 chttl-ad65b85663e4025d vsftpd[15859]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31695 Oct 18 08:39:49 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): check pass; user unknown
31696 Oct 18 08:39:49 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31697 Oct 18 08:39:49 chttl-ad65b85663e4025d vsftpd[15865]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31698 Oct 18 08:39:49 chttl-ad65b85663e4025d sshd[15863]: Accepted password for root from 114.25.34.29 port 50473 ssh2
31699 Oct 18 08:39:49 chttl-ad65b85663e4025d sshd[15863]: pam_unix(sshd:session): session opened for user root by (uid=0)
31700 Oct 18 08:39:53 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): check pass; user unknown
31701 Oct 18 08:39:53 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31702 Oct 18 08:39:53 chttl-ad65b85663e4025d vsftpd[15865]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31703 Oct 18 08:39:56 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): check pass; user unknown
31704 Oct 18 08:39:56 chttl-ad65b85663e4025d vsftpd[15865]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31705 Oct 18 08:39:56 chttl-ad65b85663e4025d vsftpd[15865]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31706 Oct 18 08:39:59 chttl-ad65b85663e4025d vsftpd[15891]: pam_unix(vsftpd:auth): check pass; user unknown
31707 Oct 18 08:39:59 chttl-ad65b85663e4025d vsftpd[15891]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31708 Oct 18 08:39:59 chttl-ad65b85663e4025d vsftpd[15891]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31709 Oct 18 08:40:01 chttl-ad65b85663e4025d vsftpd[15891]: pam_unix(vsftpd:auth): check pass; user unknown
31710 Oct 18 08:40:01 chttl-ad65b85663e4025d vsftpd[15891]: pam_unix(vsftpd:auth): authentication failure; logname= uid=0 euid=0 tty=ftp r
      user=Administrateur rhost=116.77.34.131
31711 Oct 18 08:40:01 chttl-ad65b85663e4025d vsftpd[15891]: pam_succeed_if(vsftpd:auth): error retrieving information about user Administr
      ateur
31712 Oct 18 08:40:05 chttl-ad65b85663e4025d vsftpd[15891]: pam_unix(vsftpd:auth): check pass; user unknown
```

系統的資安log (Linux)

/var/log/message: General message and system related stuff
/var/log/auth.log: Authenication logs
/var/log/kern.log: Kernel logs
/var/log/cron.log: Crond logs (cron job)
/var/log/maillog: Mail server logs
/var/log/qmail/ : Qmail log directory (more files inside this directory)
/var/log/httpd/: Apache access and error logs directory
/var/log/php-fpm/error.log: PHP-FPM error logs
/var/log/nginx/error.log: NGINX access error logs
/var/log/nginx/access.log: NGINX access logs
/var/log/lighttpd: Lighttpd access and error logs directory
/var/log/boot.log : System boot log
/var/log/mysqld.log: MySQL database server log file
/var/log/secure: Authentication log
/var/log/utmp or /var/log/wtmp : Login records file
/var/log/yum.log: Yum log files

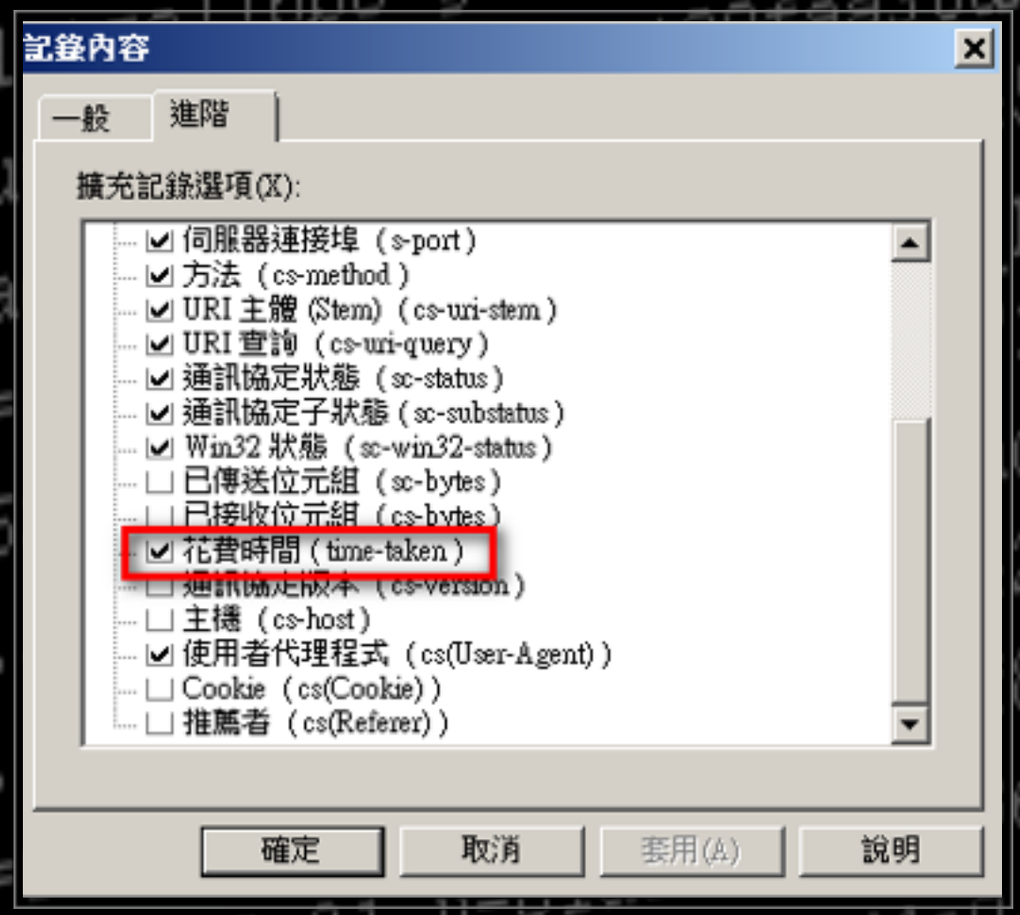
系統的資安log (Window Events Log)



- Type 2 : Console logon from local computer.
- Type 3 : Network logon or network mapping (net use/net view)
- Type 4 : Batch logon, running of scheduler
- Type 5 : Service logon a service that uses an account
- Type 7 : Unlock Workstation
- **Event ID 529 : Unknown user name or bad password**
- **Event ID 530 : Logon time restriction violation**
- **Event ID 531 : Account disabled**
- **Event ID 532 : Account expired**
- **Event ID 533 : Workstation restriction, the user is not allowed to logon at this co**
- **Event ID 534 : Inadequate rights for console login.**
- **Event ID 535 : Password expired**
- **Event ID 536 : Net Logon service down**
- **Event ID 537 : unexpected error**
- **Event ID 539 : Logon Failure: Account locked out**
- **Event ID 627 : NT AUTHORITY\ANONYMOUS is trying to change a password**
- **Event ID 644 : User account Locked out**
- Event ID 541 : IPSec security association established
- Event ID 542 : IPSec security association ended (mode data protection)
- Event ID 543 : IPSec security association ended (key exchange)
- Event ID 544 : IPSec security association establishment failed because peer coul
- Event ID 545 : IPSec peer authentication failed
- Event ID 546 : IPSec security association establishment failed because peer sent
- Event ID 547 : IPSec security association negotiation failed
- Event ID 672 : Authentication Ticket Granted
- Event ID 673 : Service Ticket Granted
- Event ID 674 : Ticket Granted Renewed

iis 網頁log

1. 訪問量最大的Top10 URL
2. 訪問失敗量前10名網頁
3. 無法訪問前10名網頁
4. 發生錯誤最多的信息
5. 訪問時間超過5秒的網頁
6. 訪問量最多的時間段(熱點時段)
7. 前10名下載流量最大的zip 文件
8. 指定的IP做了那些訪問那些網頁
9. 在線人數的統計分析
10. 訪問量前10名的IP 地址

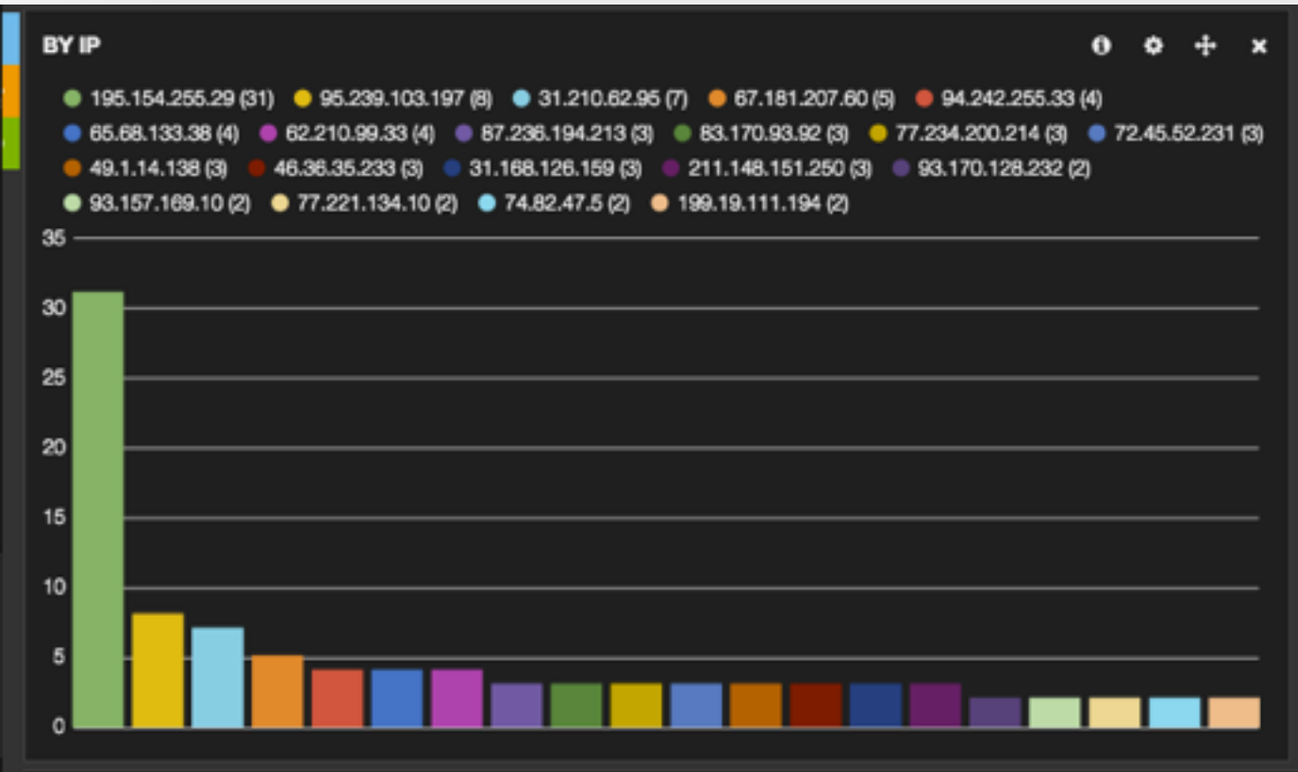


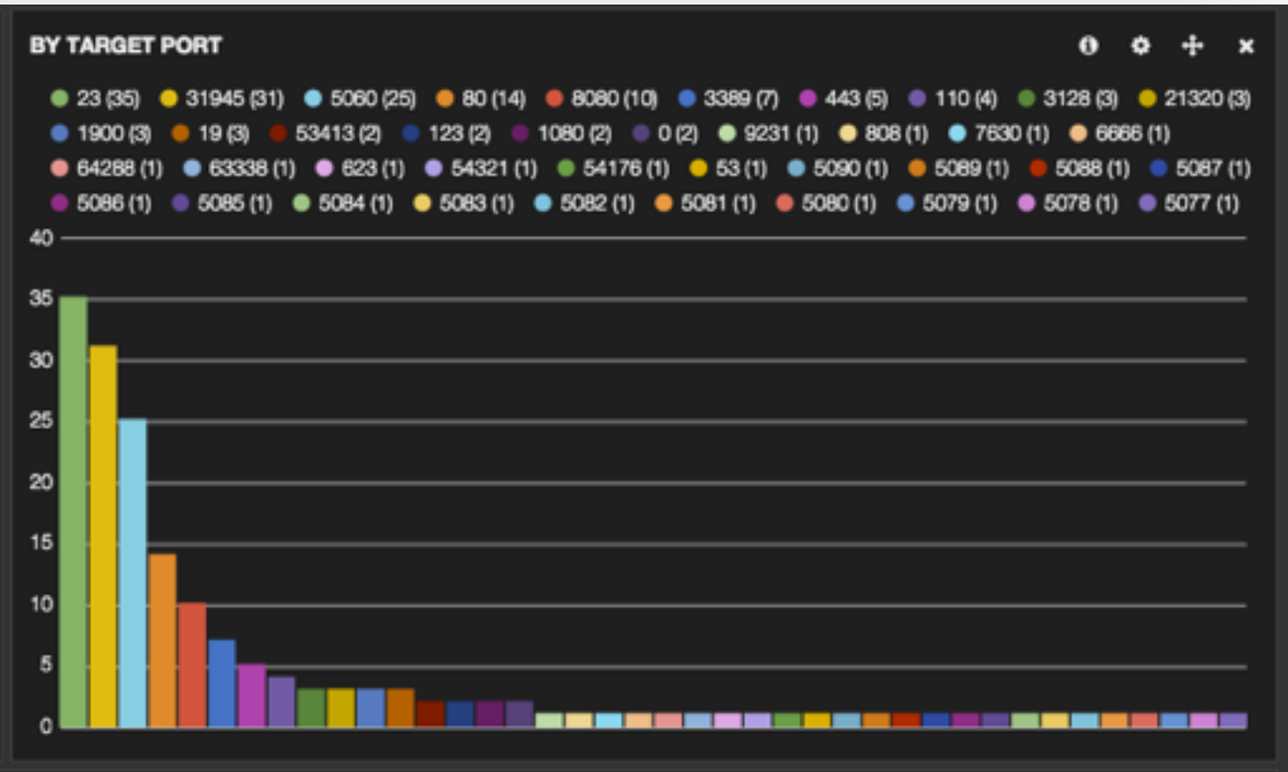
apache access log

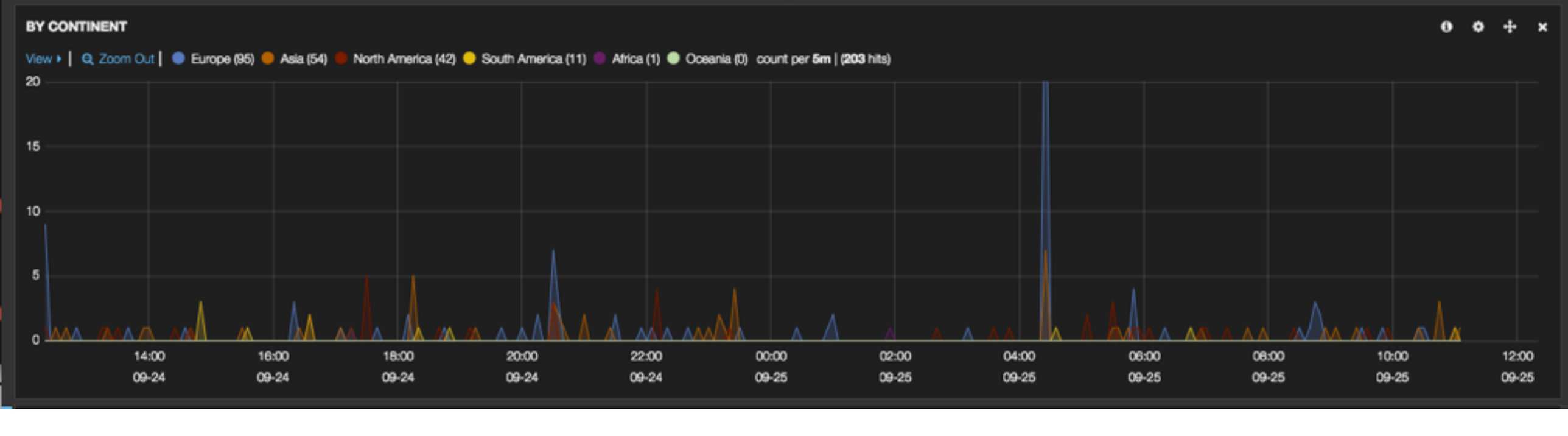
- 訪問訊息：IP/URL/訪問狀態/消耗時間
- 錯誤訊息：錯誤級別/錯誤信息

```
  1699039 2016-09-25 08:06 access_log
1388465171 2016-09-25 02:07 access_log-20160828
1149946713 2016-09-25 08:06 access_log-20160904
 591284484 2016-09-25 08:06 access_log-20160911
 373018985 2016-09-25 08:07 access_log-20160918
 402748493 2016-09-25 08:07 access_log-20160925
       420 2016-09-25 08:07 error_log
     11267 2016-09-25 02:08 error_log-20160828
     12648 2016-09-25 08:07 error_log-20160904
     16057 2016-09-25 08:07 error_log-20160911
     15244 2016-09-25 08:07 error_log-20160918
     14408 2016-09-25 08:07 error_log-20160925
```

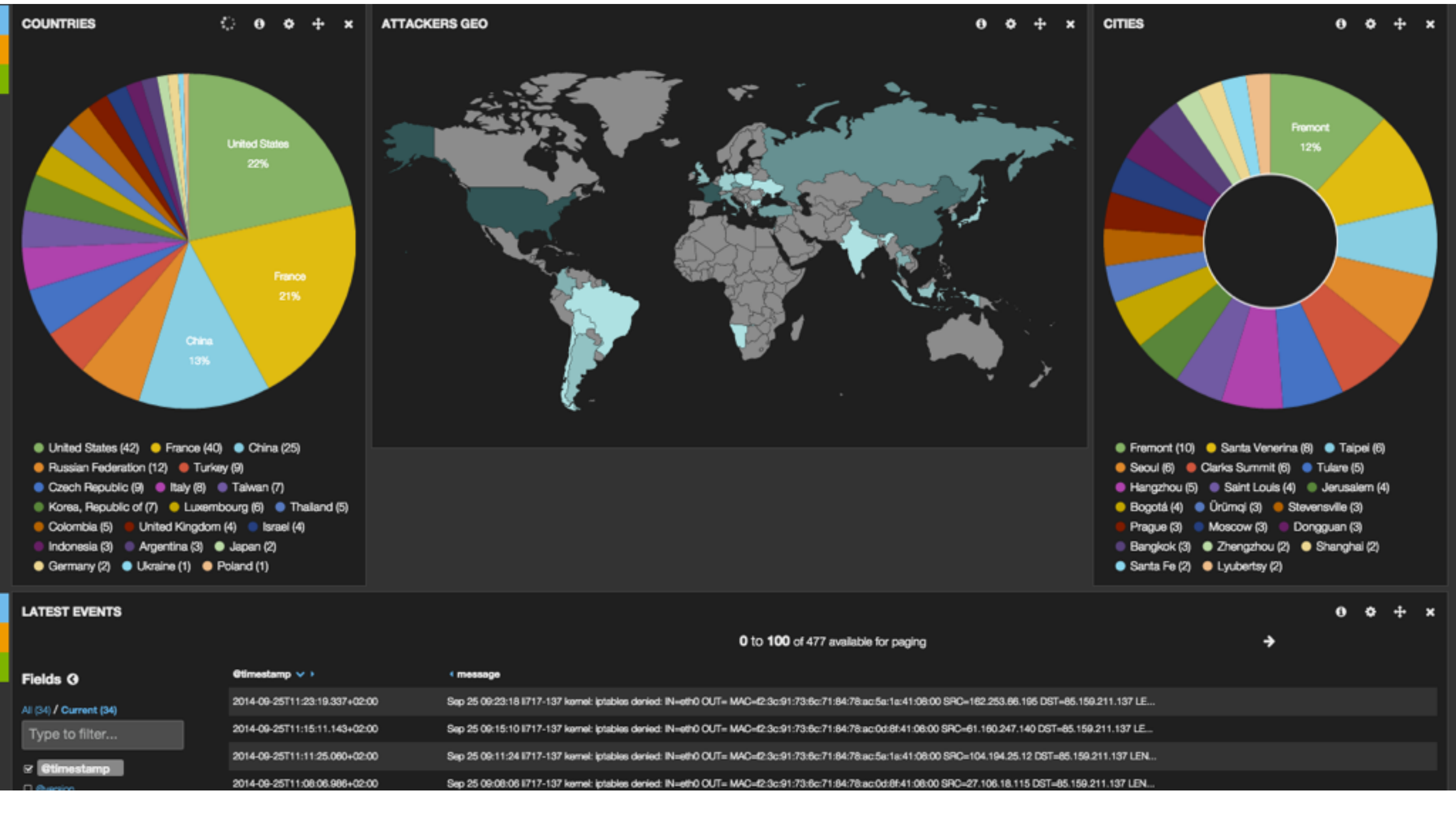
誰來了，什麼時候來的？


BY IP
195.154.255.29 (31) 95.239.103.197 (8) 31.210.62.95 (7) 67.181.207.60 (5) 94.242.255.33 (4)
65.68.133.38 (4) 62.210.99.33 (4) 87.236.194.213 (3) 83.170.93.92 (3) 77.234.200.214 (3) 72.45.52.231 (3)
49.1.14.138 (3) 46.36.35.233 (3) 31.168.126.159 (3) 211.148.151.250 (3) 93.170.128.232 (2)
93.157.169.10 (2) 77.221.134.10 (2) 74.82.47.5 (2) 199.19.111.194 (2)
35
30
25
20
15
10
5
0

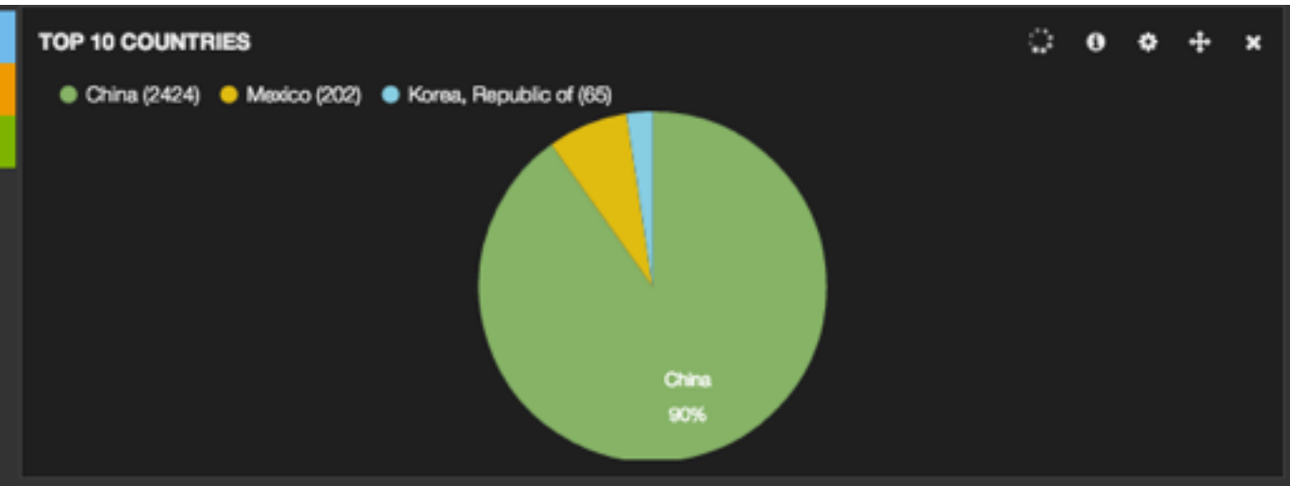

BY TARGET PORT
23 (35) 31945 (31) 5060 (25) 80 (14) 8080 (10) 3389 (7) 443 (5) 110 (4) 3128 (3) 21320 (3)
1900 (3) 19 (3) 53413 (2) 123 (2) 1080 (2) 0 (2) 9231 (1) 808 (1) 7630 (1) 6666 (1)
64288 (1) 63338 (1) 623 (1) 54321 (1) 54176 (1) 53 (1) 5090 (1) 5089 (1) 5088 (1) 5087 (1)
5086 (1) 5085 (1) 5084 (1) 5083 (1) 5082 (1) 5081 (1) 5080 (1) 5079 (1) 5078 (1) 5077 (1)
40
35
30
25
20
15
10
5
0

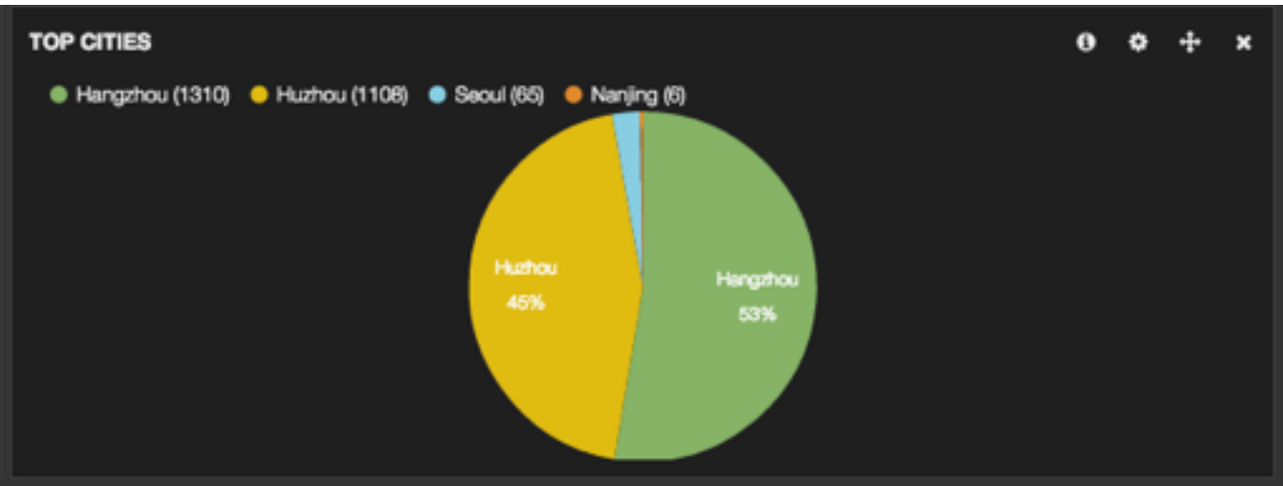

BY CONTINENT
View ▸ | Zoom Out | Europe (95) Asia (54) North America (42) South America (11) Africa (1) Oceania (0) count per 5m | (203 hits)
20
15
10
5
0
14:00 09-24
16:00 09-24
18:00 09-24
20:00 09-24
22:00 09-24
00:00 09-25
02:00 09-25
04:00 09-25
06:00 09-25
08:00 09-25
10:00 09-25
12:00 09-25

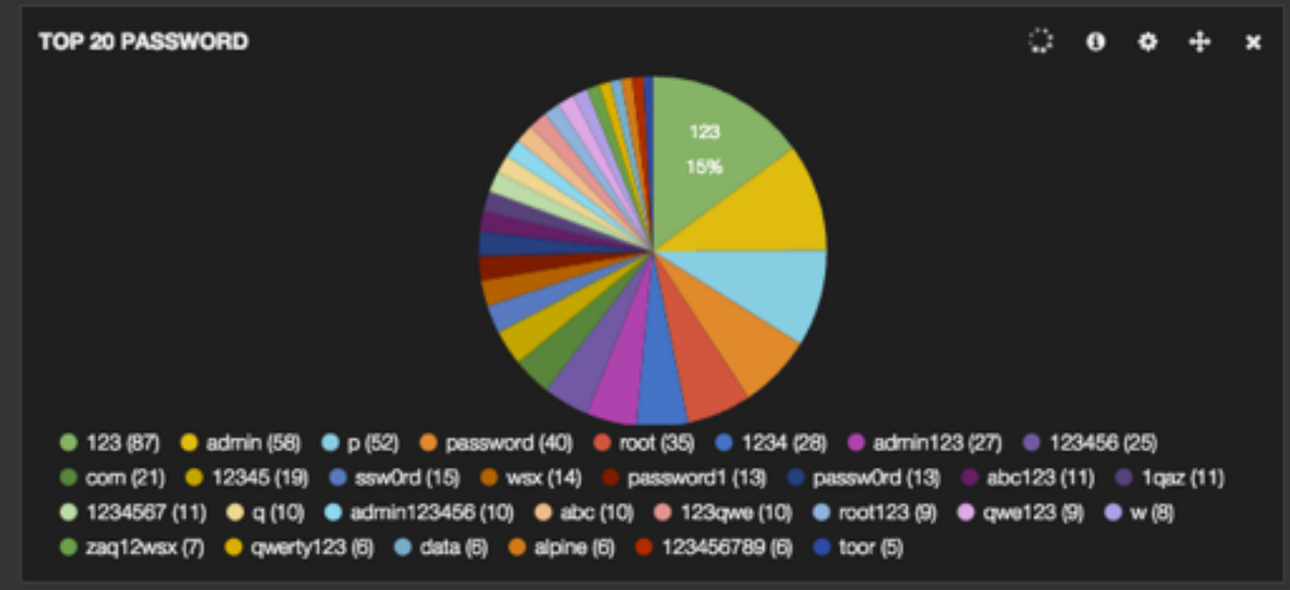
從哪裡來的？

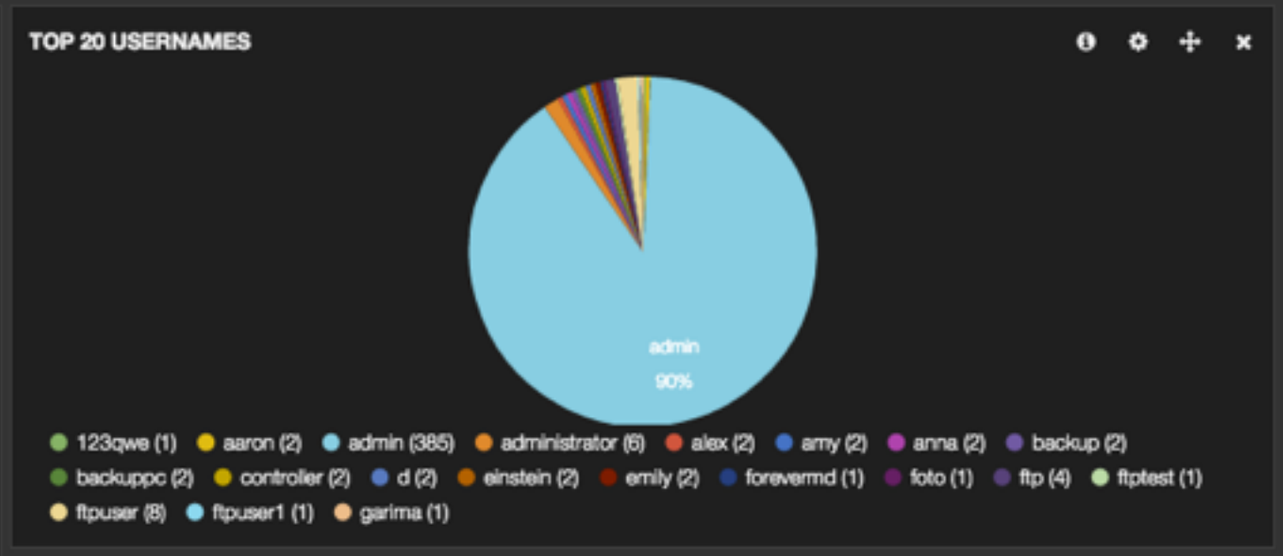

COUNTRIES
United States
22%
France
21%
China
13%
United States (42) France (40) China (25)
Russian Federation (12) Turkey (9)
Czech Republic (9) Italy (8) Taiwan (7)
Korea, Republic of (7) Luxembourg (6) Thailand (5)
Colombia (5) United Kingdom (4) Israel (4)
Indonesia (3) Argentina (3) Japan (2)
Germany (2) Ukraine (1) Poland (1)
ATTACKERS GEO
CITIES
Fremont
12%
Fremont (10) Santa Venerina (8) Taipei (6)
Seoul (6) Clarks Summit (6) Tulare (5)
Hangzhou (5) Saint Louis (4) Jerusalem (4)
Bogotá (4) Ürümqi (3) Stevensville (3)
Prague (3) Moscow (3) Dongguan (3)
Bangkok (3) Zhengzhou (2) Shanghai (2)
Santa Fe (2) Lyubertsy (2)
LATEST EVENTS
0 to 100 of 477 available for paging
Fields
All (34) / Current (34)
Type to filter...
@timestamp
@timestamp
message
2014-09-25T11:23:19.337+02:00
Sep 25 09:23:18 l717-137 kernel: iptables denied: IN=eth0 OUT= MAC=f2:3c:91:73:6c:71:84:78:ac:5a:1a:41:08:00 SRC=162.253.66.106 DST=85.159.211.137 LE...
2014-09-25T11:15:11.143+02:00
Sep 25 09:15:10 l717-137 kernel: iptables denied: IN=eth0 OUT= MAC=f2:3c:91:73:6c:71:84:78:ac:0d:8f:41:08:00 SRC=61.160.247.140 DST=85.159.211.137 LE...
2014-09-25T11:11:25.060+02:00
Sep 25 09:11:24 l717-137 kernel: iptables denied: IN=eth0 OUT= MAC=f2:3c:91:73:6c:71:84:78:ac:5a:1a:41:08:00 SRC=104.194.25.12 DST=85.159.211.137 LEN...
2014-09-25T11:06:06.986+02:00
Sep 25 09:06:06 l717-137 kernel: iptables denied: IN=eth0 OUT= MAC=f2:3c:91:73:6c:71:84:78:ac:0d:8f:41:08:00 SRC=27.106.18.115 DST=85.159.211.137 LEN...

怎麼進來的？


TOP 10 COUNTRIES
China (2424)
Mexico (202)
Korea, Republic of (65)
China
90%


TOP CITIES
Hangzhou (1310)
Huzhou (1108)
Seoul (65)
Nanjing (6)
Huzhou
45%
Hangzhou
53%


TOP 20 PASSWORD
123
15%
123 (87)
admin (58)
p (52)
password (40)
root (35)
1234 (28)
admin123 (27)
123456 (25)
com (21)
12345 (19)
ssw0rd (15)
wsx (14)
password1 (13)
passw0rd (13)
abc123 (11)
1qaz (11)
1234567 (11)
q (10)
admin123456 (10)
abc (10)
123qwe (10)
root123 (9)
qwe123 (9)
w (8)
zaq12wsx (7)
qwerty123 (6)
data (6)
alpine (6)
123456789 (6)
toor (5)


TOP 20 USERNAMES
admin
90%
123qwe (1)
aaron (2)
admin (385)
administrator (6)
alex (2)
amy (2)
anna (2)
backup (2)
backuppc (2)
controller (2)
d (2)
einstein (2)
emily (2)
forevermd (1)
foto (1)
ftp (4)
ftptest (1)
ftpuser (8)
ftpuser1 (1)
garima (1)

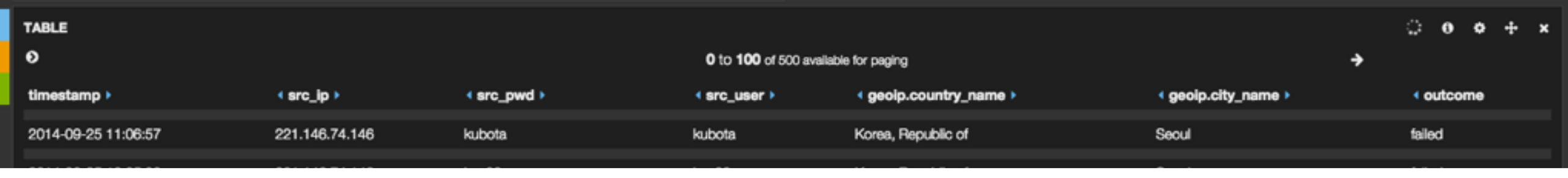


TABLE
0 to 100 of 500 available for paging
timestamp
src_ip
src_pwd
src_user
geoip.country_name
geoip.city_name
outcome
2014-09-25 11:06:57
221.146.74.146
kubota
kubota
Korea, Republic of
Seoul
failed

IT 系統日誌類別

日誌種類

1. 應用AP日誌
2. 效能日誌
3. 訪問日誌
4. 數據庫日誌
5. 用戶登錄日誌
6. 系統event 日誌
7. 防火牆日誌
8. 網路流量日誌
9. ....

日誌集中

日誌分析需求

1. 故障信息查詢
2. 應用異常追蹤
3. 性能瓶頸定位
4. 性能優化
5. 非法登錄查詢
6. 系統報錯查詢
7. 資安問題排查
8. 日誌稽核審計
9. ....

應用案例