UNIX/Linux for Enterprise Envir. 2/52

1. แสดงและอธิบายถึงขนาดของ swap partition

```
swapinfo -h
pstat -sh
```

Swap parition ใช้เป็นเหมือน Virtual Memory ใน Windows เป็นที่เก็บ page file และใช้เป็นหน่วยความจำสำรองในกรณีที่ Main memory เต็ม

ในเครื่องรุ่นเก่าๆเช่น RAM 128MB แนะนำให้ Swap มีขนาด 1.5-2 เท่าของขนาด Main memory หรือใหญ่กว่า 1GB ส่วนเครื่องรุ่นใหม่ปรับแล้วแต่การใช้งานเช่น เครื่อง Desktop ปรับขนาด 2 เท่าของ RAM เพื่อรองรับ Application ได้เยอะๆ แต่เครื่อง Server ใช้ประมาณ 0.5 เท่าของ RAM

2. อธิบายว่าทำไมจึงต้องแบ่ง Disk เป็น partition

```
df -h
```

ในแต่ละ partition จะมีลักษณะการทำงานที่แตกต่างกัน บาง partition เป็นแบบ read-mostly ในขณะที่บาง partition มีลักษณะเป็น write-mostly ดังนั้นการแบ่ง partition จะช่วยให้ File System สามารถปรับแต่งตัวเองให้เหมาะสมกับแต่ละลักษณะการทำงานได้ และจะช่วยให้ system fragmentation ซึ่งมักจะทำบน partition ที่มีการเขียนเป็นส่วนใหญ่ ไม่ไปกระทบกับ partition ที่มีการอ่านเป็นส่วนใหญ่ นอกจากนี้ การจัดให้ partition ที่ write-mostly อยู่ใกล้กับขอบของ disk จะเป็นการเพิ่มประสิทธิภาพการทำงานในส่วนของ I/O ได้อีกด้วย

3. แสดงถึง System specific และ Site-wide configuration

System configuration information ต่างๆจะถูกเก็บไว้ที่ `/etc/rc.conf` มักจะถูกใช้เมื่อ Boot OS ใหม่ ผู้ดูแลระบบควรสร้าง `/etc/rc.conf` ขึ้นมาเพื่อ override `/etc/defaults/rc.conf` ไฟล์ `/etc/rc.conf` นี้จะเก็บ System specific information ซึ่งเป็นข้อมูลเฉพาะของเครื่องนั้นๆ

Site-wide configuration เป็นการ config เครื่องต่างๆในระบบให้เหมือนๆกัน เช่นการชี้ตำแหน่ง Gateway หรือ Router ตัวอย่างการใช้งานคือ สร้างไฟล์ `/etc/rc.conf.site` ขึ้นมาเพื่อแยกเก็บ config กลาง แล้ว include ไฟล์ดังกล่าวใน `/etc/rc.conf` เพื่อให้ถูกรันตอนเปิดเครื่อง จากนั้นก็ sync ไฟล์นี้ไปสู่เครื่องอื่นๆในระบบ โดยใช้โปรแกรมเช่น `rsync`

ประโยชน์ของการทำแบบนี้คือลด Overhead ในการ Maintenace ระบบได้

อ่านเพิ่มเติมที่ http://www.freebsd.org/doc/en/books/handbook/configtuning-core-configuration.html

4. แสดงข้อแตกต่างหรือความสัมพันธ์ระหว่าง /usr/local/etc/* กับ /usr/local/etc/rc.d/* และ /etc/rc.d/*

- `/etc/rc.d/*`
  Start/stop scripts for basic services and daemons
- `/usr/local/etc/rc.d/*`
  Start/stop scripts for installed applications.
- `/usr/local/etc/*`
  Configuration files for installed applications. May contain per-application subdirectories.

ความแตกต่างคือ `/usr/local/etc/*` เป็น Configuration file ส่วนอันอื่นๆเป็น Start/stop script

ความสัมพันธ์ของ `/etc/rc.d/*` และ `/usr/local/etc/rc.d/*` คือ คำสั่ง init จะเข้าไปรัน `/etc/rc` ซึ่งจะเรียกไฟล์ `/etc/rc.d/*` ก่อนแล้วจึงเรียกไฟล์ `/usr/local/etc/rc.d/*` ขึ้นมารัน

อ่านเพิ่มเติม http://www.freebsd.org/doc/en/books/handbook/configtuning-configfiles.html

5. แสดงและอธิบายความหมายของแต่ละ Field ใน /etc/crontab file

ด้านบนของไฟล์จะให้กำหนด Environment variable มี 3 ตัวดังนี้

1. `SHELL` – ถ้าไม่กำหนดจำใช้ sh
2. `PATH` – ถ้าไม่กำหนด command ต่างๆที่จะรันต้องอ้างด้วย Absolute path
3. `HOME` – ถ้าไม่กำหนดจะใช้ Home directory ของแต่ละ user

การกำหนดเวลาและคำสั่งที่ต้องการจะรัน โดยค่าเวลามีค่าดังนี้

min (0-59) hour (0-23) day of month (1-31) month (1-12) day of week (0-6)

ยกตัวอย่างค่าที่กำหนดไว้ เช่น

```
30    5    1    *    *    root  periodic monthly
```

หมายถึงรันคำสั่ง 'periodic monthly' ในวันที่ 1 ตอน 5.30 ของทุกเดือนทุกปี ห้ามจำผิด ไม่ใช่รันทุก 30 นาทีไรงี้

```
0     */5   *    *    *    root  /home/komsitr/myCommand
```

หมายถึงการรันคำสั่ง '/home/komsitr/myCommand' ทุกๆ 5 ชั่วโมงตอนนาทีที่ 0

Cron มีการทำงาน 2 mode คือ system crontab และ user crontab ซึ่งจะมีข้อแตกต่างที่ field 'who' ถ้าเป็น system crontab จะ Run as any users แต่ถ้าเป็น user crontab จะไม่มี field นี้

6. แสดงการ install NDIS (Network Driver Interface Specification) โดยผ่าน NDISulator

อ่านเพิ่มเติมได้ที่ http://www.freebsd.org/doc/en/books/handbook/config-network-setup.html

7. แสดงการทำ Multiple IP Address (Virtual host)

การทำให้ Server เครื่องเดียวสามารถมองเห็นเป็นหลายเครื่องได้ ทำโดยการแก้ /etc/rc.conf โดยเพิ่ม Alias Address ลงไป ดังนี้

```
ifconfig_fxp0="inet 10.1.1.1 netmask 255.255.255.0"          ตั้ง IP จริง ๆ
ifconfig_fxp0_alias0="inet 10.1.1.2 netmask 255.255.255.255"  ตั้ง IP เสมือน
ifconfig_fxp0_alias1="inet 10.1.1.3 netmask 255.255.255.255"  ตั้ง IP เสมือน
```

สังเกตว่า fxp0 เป็นชื่อ Network interface ของเราซึ่งอาจจะไม่ตรงกันในแต่ละเครื่อง ให้เช็คด้วยคำสั่ง `ifconfig -a` ก่อน และส่วน netmask ของ alias ต้องเป็น 255.255.255.255 เท่านั้น

ใน FreeBSD การตั้ง IP Address จะมี Address จริงๆ ได้เพียงแค่ Address เดียวเท่านั้น ส่วนถ้าต้องการตั้ง IP เสมือนด้วย Virtual Host สามารถตั้งได้หลายๆ IP โดยต้องเริ่มตั้งแต่ alias0, alias1 ไปเรื่อยๆ และตัวเลขต้องต่อเนื่องกัน

8. /etc/hosts ใช้ทำอะไร เมื่อมี /etc/resolv.conf แล้วทำไมยังต้องใช้อีก

- `/etc/hosts` - a simple text database reminiscent of the old Internet
  ทำงานเชื่อมระหว่าง DNS กับ NIS เพื่อ mapping ชื่อ Domain กับ IP Address
  สามารถเอาไว้ตั้งชื่อเครื่องอื่นๆในวงแลนแทนการเข้าผ่าน IP Address
  หรือการกำหนด Local record เพื่อประหยัดเวลาการไป query หา IP Address ผ่าน DNS แบบวิธีทั่วไป
- `/etc/resolv.conf` - dictates how FreeBSD's resolver accesses the Internet Domain Name System (DNS) ชี้ตำแหน่ง DNS Server อยากมาก 3 แห่ง เพื่อเอาไว้แปลง domain เป็น IP Address

9. แสดงการ tune จำนวน process ให้เป็น 10,000 โดยใช้ sysctl(8)

```
sysctl kern.maxprocperuid=10000
```

10. อธิบายถึง Soft update ในการ tune ระบบแฟ้ม โดยใช้คำสั่ง tunefs(8)

```
tunefs -n enable|disable /filesystem
```

Soft updates are an approach to **maintaining disk integrity after a crash or power outage.** Instead of duplicating metadata writes in a journal, **soft updates work by properly ordering the metadata writes to**

guarantee consistency after a crash. Like journaling, soft updates do not guarantee that no data will be lost, but do make sure the filesystem is consistent.

An advantage is that it can be mounted immediately after a crash since there is no log replay.

อ่านเพิ่มเติม http://en.wikipedia.org/wiki/Soft_updates

11. แสดงการใช้ netstat(1) และอธิบาย field ต่าง ๆ

```
netstat [-a]
```

1. Active Internet Connection
    a. Proto – Protocol ที่ใช้
    b. Recv-Q – จำนวน byte ที่โปรแกรมยังไม่ดึงไปใช้
    c. Send-Q – จำนวน byte ที่ Remote host ยังไม่ ack
    d. Local Address
    e. Foreign Address
    f. State
2. Active UNIX Domain sockets
    a. Address - ??
    b. Type – ประเภทของ socket
    c. Inode - ??
    d. Conn - ??
    e. Refs - ??
    f. Nextref - ??
    g. Path

12. Bootstrap คืออะไร เกี่ยวข้องกับ BIOS และ MBR อย่างไร

Bootstrap คือ the process of loading an operating system โดย FreeBSD แบ่งออกเป็น 3 ขั้นตอนดังนี้

1. โหลด BIOS เพื่อ Initialize H/W
2. โหลด First track of disk0 หรือ Master Boot Record (MBR) เพื่อรันโปรแกรมเล็ก ชี้ตำแหน่ง OS
3. โหลดตัว OS

13. Boot flag –s ใช้ทำอะไร หมายถึงอะไร

Boot เข้า single-user mode ทำให้สามารถมีผู้ใช้งานระบบได้เพียงคนเดียว คือ super user เพื่อ Maintenance ระบบที่ใช้งานหลายคน เช่น

1. การต้องการ Exclusive access ส่วน shared resource เพื่อทำการ `fsck` (scan disk) ซึ่งต้อง un-mount ก่อน
2. การ Reset root's password
3. Security purpose – Service ต่างๆที่เกี่ยวกับ network จะไม่ถูกรัน ทำให้ปลอดภัยจากการรบกวนจากภายนอก

14. shutdown ต่างจาก halt command อย่างไร

```
shutdown -h now
```

`shutdown` สามารถสั่งงานได้หลากหลายกว่า รวมถึงการ `reboot` และ `halt` ด้วย นอกจากนี้ `shutdown` สามารถตั้งเวลาของคำสั่งได้ มีการแจ้ง User ล่วงหน้า และมีการ Cleanly closing service

15. แสดงการใช้ chpass(1)

```
chpass [_username_]
```

เป็นคำสั่งเพื่อแก้ไข User profile โดยถ้าไม่กรอก username จะเป็นการแก้ไขข้อมูลของ current user คำสั่งนี้สามารถใช้งานได้ 2 กรณี

1. Normal-user mode
   แก้ไขได้เฉพาะ User profile ได้แก่ ชื่อ-สกุล, Office location, Office/Home phone และ Other Information (พวก Gecos field และ site specific user information)
2. Super-user mode
   สามารถแก้ข้อมูลได้ทุกอย่างนอกเหนือจากใน Normal-user mode ได้แก่ Login, Password, UID, GID, Home Directory, Shell, Account Expiration time และ Password Change time

16. แสดงการใช้ md5(1) ในการทำ file integrity check

```
md5 _filepath_
```

17. อธิบายถึงความสัมพันธ์ระหว่าง DOS attack (Denial of Service) กับการจำกัด Server fork

- `inetd -c _maximum_`
  กำหนดจำนวน child-per-service ค่า default เป็น unlimited

- `inetd -C _rate_`
  กำหนด max-connections-per-ip-per-minute
- `inetd -R _rate_`
  กำหนดจำนวน maximum number ที่ server สามารถถูก invoke ได้ใน 1 นาที (0 คือ unlimited)

การทำ DOS Attack คือการส่ง Connection มาเยอะๆ ทำให้ Server ต้อง fork child process ออกมาเป็นจำนวนมาจน Memory หมด และในที่สุดก็จะ halt ไป ซึ่งการจำกัดจำนวน fork จะช่วยป้องกันปัญหานี้ได้

อ่านเพิ่มเติมที่ http://www.freebsd.org/doc/en/books/handbook/securing-freebsd.html

18. อธิบายและแสดงถึงวิธีหาว่าระบบใช้วิธีการใด (DES/MD5/Blowfish) ในการ Encrypt password

มี 2 วิธี ดังนี้

1. ดูว่าตอนนี้ระบบใช้วิธีการใดอยู่

```
cat /etc/login.conf | more
```

กดเลื่อนลงไปเรื่อยๆ ในส่วนของ default:\ หาคำว่า :passwd_format จะมี value ที่เป็นไปได้ 3 แบบคือ md5, des และ blf

2. ดูว่า Password ของ User คนนี้เข้ารหัสแบบไหนอยู่

```
chpass [_username_]
vi /etc/master.passwd
```

ดูที่ field password ถ้าเป็น *MD5* ขึ้นต้นด้วย 1 ถ้าเป็น *Blowfish* ขึ้นต้นด้วย $2a$ นอกนั้นเป็น *DES*

19. แสดงการใช้และสถานะของ USB device

```
camcontrol devlist
cat dmesg | more
```

ใครรู้รายละเอียดเติมให้หน่อย

20. แสดงการใช้ file system snapshots – mksnap_ffs(8)

```
mksnap_ffs _snapshot_name_
```

เป็นการทำ Snapshot ของ File system โดยเก็บไว้ที่ *_snaphost_name_*

ตัวอย่างการใช้งาน

```
mksnap_ffs /usr/home/snapshot
```

จะได้ไฟล์ Snapshot ของทั้ง System เป็นเหมือน Image file ไว้

ทดลอง mount มาดูข้อมูลข้างใน

```
mdconfig -a -t vnode - o readonly -f /usr/home/snapshot
mount -o ro /dev/md0 /mnt/
```

เมื่อใช้เสร็จแล้ว unmount ออก

```
umount  /dev/md0
mdconfig -d -u 0
```