การติดตั้ง Log Server ด้วย Linux

เตรียมค่า IP Address ก่อนการติดตั้ง

IP Address : ……. Primary DNS : 203.146.15.9

Subnet Mask : ……..…… Secondary DNS : 203.146.237.237

Gateway : ……..……..

1. ติดตั้ง Log Server 1.0

1. บูตเครื่องจากแผ่นติดตั้ง Log Server 1.0 จากนั้นจะแสดงหน้าจอ Welcome to Log Server 1.0 ให้เลือก Install or Upgrade แล้วกด Enter

2. จากนั้นจะแสดงหน้าจอการตรวจสอบแผ่น ให้เลือก SKIP เพื่อข้ามขั้นตอนนี้ไป

3. ในหน้าจอ Welcome to Log Server ให้กด Enter ผ่านไป

4. หน้าต่างภาษาให้เลือกภาษา English และหน้าต่างแป้นพิมพ์ เลือก us

5. จากนั้นจะแสดงหน้าจอ เตือนการติดตั้ง Linux ให้ตอบ YES

6. จากนั้นจะแสดงหน้าจอเลือกการแบ่งพาร์ทิชั่นของ Harddisk ในที่นี้ให้เลือกแบบที่ 1 คือ Remove all partitions on selected drives and create default layout แล้วตอบ OK

7. จากนั้นให้ตอบ YES เพื่อยืนยันการแบ่งพาร์ทิชั่น และตอบ YES เพื่อดูพาร์ทิชั่นที่ระบบแบ่งพาร์ทิชั่นให้อัตโนมัติ แล้วตอบ OK และ YES ตามลำดับ

8. จากนั้นจะแสดงหน้าจอ Boot Loader Configuration ให้ตั้งเป็นค่า Default โดยเลือก OK ทุกหน้าจอ

9. หน้าจอ Network Configuration for eth0 เลือก [*] Enable IPV4 support และ [*] Activate on boot จากนั้นใสค่า IP Address และ Subnet Mask ที่เตรียมไว้ แล้วตอบ OK

10. จากนั้นใสค่า Gateway และ DNS ที่เตรียมไว้ แล้วตอบ OK

11. จากนั้นจะแสดงหน้าจอให้ระบุชื่อโดเมนเนม ให้เลือก [*] manually แล้วระบุชื่อโฮสเนม และ โดเมนเนมตามที่ต้องการ เช่น log.sakate.com จากนั้นตอบ OK

12. จากนั้นจะแสดงหน้าจอเลือกโซนเวลา ให้เลือก Asia/Bangkok แล้วตอบ OK

13. จากนั้นให้ใส่รหัสผ่านของ root โดยใส่ 2 ครั้งเหมือนกัน แล้วตอบ OK

14. จากนั้นเลือกการติดตั้ง Server โดยเลือก [*] NTP Server และ [*] Syslog-ng Server แล้วตอบ OK

15. จากนั้นจะแสดงหน้าจอ เริ่มการติดตั้ง Linux ให้ตอบ OK แล้วรอขั้นตอนการติดตั้งจนแล้วเสร็จ เมื่อติดตั้งเสร็จแล้วจะแสดงหน้าต่าง Complete ให้นำแผ่นซีดีรอมสำหรับติดตั้ง Linux ออก แล้วกด Enter จากนั้นระบบจะบูตเครื่องใหม่

16. เมื่อเครื่องบูตขึ้นใหม่จะแสดงหน้าต่าง Setup Agent ให้เลือก Run Tool และเลือก Next แล้วออกจากหน้าต่างโดยเลือก Exit จากนั้นจะแสดงหน้าต่าง Login เข้าสู่ระบบ

2. การเข้าสู่ระบบ Linux

1. เมื่อแสดงหน้าต่าง Login เข้าสู่ระบบ

   Log login : ให้ใส่ชื่อ root

   Password : ให้ใส่รหัสผ่านที่ตั้งไว้ในขั้นตอนที่ 13

2. ถ้าใส่รหัสถูกต้องจะเข้าสู่ระบบ และแสดงหน้าจอ [root@log ~]#

3. ติดตั้ง LOG SERVER

1. สั่งให้ seedit-init ทำงาน

   # seedit-init ===> สั่งให้ seedit ทำงาน

   # reboot ===> จากนั้นเครื่องจะบูตตัวเองประมาณ 2 ครั้ง

2. ปรับค่า Firewall

   # lokkit เลือก customize

   จากนั้นเลือก [*] eth+ ในช่อง Trusted Interface และ Masquerading

   ส่วนในช่อง Trusted Service ให้เอาออกให้หมด

   ในช่อง Other Port เพื่อค่า 514:tcp 514:udp จากนั้นตอบ OK

3. แก้ไขค่าไฟล์ hosts.deny

   # vi /etc/ hosts.deny

   จากนั้นเพิ่มบรรทัดนี้ในบรรทัดสุดท้าย ALL:ALL

4. แก้ไขค่าไฟล์ hosts.allow

   # vi /etc/ hosts.allow

   จากนั้นเพิ่มเพิ่มบรรทัดนี้ในบรรทัดสุดท้าย

   syslog-ng : ค่า IP ที่อนุญาตให้ส่งไฟล์มาเก็บไว้ใน Log Server ได้ วงที่ 1,2,.....

   เช่น syslog-ng:192.168. 203.146.

5. ติดตั้งโปรแกรม Portsentry (ไฟล์ติดตั้งอยู่ในแผ่น Linux Server 3.0)

   # mkdir -p /mnt/cdrom ===> สร้างไดเรคทรอรี่

   # mount /dev/cdrom /mnt/cdrom ===> เชื่อมต่อกับซีดีรอม

   # rpm -ivh /mnt/cdrom/MyBooks/portsentry กด Tab

   # eject ===> นำแผ่นซีดีรอมออก

   # service portsentry restart ===> สั่งให้ service portsentry ทำงาน

   # chkconfig portsentry on ===> ให้ service portsentry ทำงานทุกครั้งที่เปิดเครื่อง

6. ตรวจสอบการทำงานของ NTP Server

   เมื่อติดตั้ง Log Server 1.0 แล้ว NTP จะทำงานโดยอัตโนมัติ ให้ตรวจสอบค่าต่างๆ ดังนี้

   # date ===> ดูเวลา

   # ntpstat ===> ดูค่า Stratum เวลา

   # ntptrace clock.nectec.or.th ===> ตรวจดู Server ที่ใช้อ้างอิงฐานเวลา

ntptrace clock2.nectec.or.th ===> ตรวจดู Server ที่ใช้อ้างอิงฐานเวลา

หมายเหตุ ในการตรวจสอบถ้ามีข้อความ *** Request time out *** แสดงว่า Server ไม่ทำงาน

และจะต้องตั้งเวลาในเครื่องในระบบเครือข่ายทุกตัวให้อ้างอิง NTP Server ด้วย

7. แก้ไขค่าไฟล์ syslog-ng.conf

vi /etc/syslog-ng/syslog-ng.conf

บรรทัดที่ 219 : ให้ใส่เครื่องหมาย # หน้าบรรทัดนี้ เป็น

#filter f_www1 {program("apache");};

บรรทัดที่ 227 : ให้ลบข้อความ filter(f_www1); ออก เป็น

log{ source(s_client); filter(f_www); destination(d_www);};

8. สั่งให้ Service ของ syslog-ng ปรับปรุงค่าและทำงานอีกครั้ง

service syslog-ng restart ===> สั่งให้ service syslog-ng ปรับปรุงค่า

chkconfig syslog-ng on ===> ให้ service syslog-ng ทำงานทุกครั้งที่เปิดเครื่อง

9. การตรวจสอบการเก็บ Log Server

ข้อมูลจะถูกเก็บไว้ที่ /var/log โดยแยกเป็น ชื่อ $Host , $Year , $Month

และ ชื่อไฟล์ เช่น www.2008-08-28 , squid.2008-08-28 , ftp.2008-08-28 เป็นต้น

#ls /var/log

#tail /var/log/….ชื่อเครื่อง…./….ปี ค.ศ…../….เดือน…./….ชื่อไฟล์แยกเป็นวันที่…...

4. คำสั่ง Linux ที่ควรรู้

# ls	===> ขอดูไฟล์
# ls -l	===> ขอดูไฟล์ และสิทธิของไฟล์
# pwd	===> ดูตำแหน่งปัจจุบัน
# netconfig หรือ netconf	===> ติดตั้งค่า IP ของการ์ดแลน
# cd ชื่อโฟลเดอร์	===> เข้าโฟลเดอร์
# cd	===> ออกจากโฟลเดอร์
# useradd ชื่อผู้ใช้	===> สร้างผู้ใช้
# passwd ชื่อผู้ใช้	===> กำหนดรหัสผ่านให้ผู้ใช้
# userdel -r ชื่อผู้ใช้	===> ลบชื่อผู้ใช้ (-r ให้ลบโฟลเดอร์ออกด้วย)
# poweroff	===> ปิดเครื่อง
# date	===> ดูเวลา
# date ตัวเลขเดือน วัน เวลาชั่วโมง เวลานาที ปี ค.ศ.	===> ตั้งเวลา (ให้พิมพ์ตัวเลขติดกัน)
# mkdir ชื่อโฟลเดอร์	===> สร้างโฟลเดอร์
# rmdir ชื่อโฟลเดอร์	===> ลบโฟลเดอร์
# groupadd -g หมายเลขกลุ่ม ชื่อกลุ่ม	===> สร้างกลุ่มผู้ใช้งาน

group ===> ดูว่าอยู่กลุ่มไหน

ping ค่า IP Address ===> ทดสอบการเชื่อมต่อระบบ

lynx ชื่อเว็บไซต์ ===> ทดสอบการใช้งานเว็บไซต์

rm –r ชื่อไดเรคทรอรี่ ===> ลบทุกอย่างในไดเรคทรอรี่ โดยถามก่อน

rm –rf ชื่อไดเรคทรอรี่ ===> ลบทุกอย่างในไดเรคทรอรี่ โดยไม่ถาม

chmod ค่าของสิทธิ ชื่อไดเรคทรอรี่หรือไฟล์ ==> กำหนดสิทธิ์ให้กับไดเรคทรอรี่หรือไฟล์

chmod ค่าของสิทธิ * -Rf ===> กำหนดสิทธิ์ทุกไดเรคทรอรี่หรือไฟล์ที่อยู่ในนี้

tail ชื่อไฟล์ ===> แสดงข้อมูลในไฟล์

poweroff ===> ปิดเครื่อง

reboot ===> บูตระบบใหม่

5. การใช้โปรแกรม VI

กดปุ่ม	ความหมาย
dd	ลบทั้งบรรทัด
yy	คัดลอกข้อความ
p	วางข้อความที่คัดลอก
i	เข้าสถานะแก้ไขค่า
กด ESC	ยกเลิกสถานะแก้ไข (Insert)

กดปุ่ม	ความหมาย
:help	ดูคำสั่งต่างๆ
:set number	แสดงหมายเลขเลขบรรทัด
:wq หรือ :x	บันทึกค่าและออก
:q!	ออกโดยไม่บันทึกค่า
:r ชื่อไฟล์	นำเข้าข้อความจากไฟล์อื่น
/ ข้อความ	ค้นหาข้อความที่พิมพ์