ขั้นตอนการติดตั้ง Mail Server (Postfix + Openwebmail)

สรุปโดย อดิศร ขาวสังข์

จัดทำเมื่อ 1 มีนาคม 2552

ทดสอบบน ubuntu 8.10

<u>มีขั้นตอนดังนี้</u>

1. ติดตั้ง Ubuntu 8.10 Server 64 Bits
2. ติดตั้ง ClamAV Antivirus
   - apt-get install clamav
   - apt-get install clamav-daemon
3. ติดตั้ง OpenSSH
   - apt-get install openssh-client
   - apt-get install openssh-server
   - คอนฟิกไฟล์ /etc/ssh/sshd_config ให้ PermitRootLogin no
4. ติดตั้งโปรแกรม Webmin เพื่ออำนวยความสะดวกในการบริหารจัดการ
   - ดาว Webmin ด้วยคำสั่ง

     wget http://prdownloads.sourceforge.net/webadmin/webmin_1.450_all.deb
   - ติดตั้งด้วยคำสั่ง dpkg -i webmin_1.450_all.deb
   - ถ้าเจอปัญหาให้ใช้คำสั่ง apt-get –f install
   - สามารถเรียกใช้งาน webmin ผ่าน Browser ที่ https://host_name_or_ip:10000
5. ติดตั้ง Usermin เพื่อบริการจัดการ Webmail
   - ดาว usermin ด้วยคำสั่ง

     wget http://prdownloads.sourceforge.net/webadmin/usermin_1.380_all.deb
   - ติดตั้งด้วยคำสั่ง dpkg -i usermin_1.380_all.deb
   - สามารถเรียกใช้งาน usermin ผ่าน Browser ที่ https://host_name_or_ip:20000
6. การตั้งตั้ง Vitualmin ซึ่งใช้ทำหน้าที่ Manage your virtual domains, mailboxes, databases, applications, and the entire server, from one comprehensive interface.
   - ดาวน์โหลด Installer ได้ด้วยคำสั่ง

     wget http://software.virtualmin.com/gpl/scripts/install.sh
   - กำหนดสิทธิ์ด้วยคำสั่ง chmod +x install.sh
   - ติดตั้งด้วยคำสั่ง ./install.sh แต่ติดตั้งไม่ได้บน Ubuntu 8.10 ระบบที่ติดตั้งได้ดังนี้

     The systems currently supported by install.sh are:

     CentOS 4 and 5 on i386 and x86_64

Debian 4.0 on i386 and amd64

Ubuntu 8.04 LTS on i386 and amd64

7. ติดตั้ง Postfix Mail
   - ติดตั้ง Postfix ด้วยคำสั่ง apt-get install postfix
     - General type of mail configuration : Internet Site
     - System mail name : south.cattelecom.com (ให้ระบุโดเมนหรือ subdomain)
   - สามารถ Reconfigure Postfix ด้วยคำสั่ง dpkg-reconfigure postfix
     - Root and postmaster mail recipient :
     - Other destinations to accept mail for (blank for none):

       south.cattelecom.com, mail.south.cattelecom.com, localhost.south.cattelecom.com, localhost
     - Force synchronous updates on mail queue? : No
     - Local networks 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
     - Mailbox size limit (bytes): 0 (no limit)
     - Local address extension character: +
     - Internet protocols to use: ipv4
   - เราสามารถคอนฟิกค่าเพิ่มเติมได้ที่ไฟล์ /etc/postfix/main.cf
   - เราสามารถ Restart Postfix ด้วยคำสั่ง /etc/init.d/postfix restart
   - เราสามารถทดสอบการทำงานของ Postfix ด้วยคำสั่ง telnet localhost smtp

     Trying 127.0.0.1...

     Connected to localhost.

     Escape character is '^]'.

     220 mail.south.cattelecom.com ESMTP Postfix (Ubuntu)
   - ออกจากการทดสอบข้างบนด้วยการกดปุ่ม ctrl +] แล้วพิมพ์ quit
8. ติดตั้ง POP & IMAP Server with Dovecot Server
   - ติดตั้งด้วยคำสั่ง apt-get install dovecot-common dovecot-imapd dovecot-pop3d
   - เราสามารถคอนฟิก dovecot ที่ไฟล์ /etc/dovecot/dovecot.conf
   - ในไฟล์คอนฟิกเราสามารถกำหนด
     - โปรโตคอลเป็น protocols = pop3 pop3s imap imaps หรือเลือกเอาเฉพาะบางโปรโตคอลที่จำเป็น
     - disable_plaintext_auth = no
   - เราสามารถ Restart dovecot ด้วยคำสั่ง /etc/init.d/dovecot restart

- เราสามารถทดสอบการทำงานของ pop3 ด้วยคำสั่ง telnet localhost pop3

  Trying 127.0.0.1...

  Connected to localhost.

  Escape character is '^]'.

  +OK Dovecot ready.

- ออกจากการทดสอบข้างบนด้วยการกดปุ่ม ctrl +] แล้วพิมพ์ quit

9. ติดตั้ง apache2
   - ติดตั้งด้วยคำสั่ง apt-get install apache2
10. ติดตั้ง SpamAssassin
    - ติดตั้งด้วยคำสั่ง apt-get install spamassassin
11. ติดตั้ง Openwebmail
    - ดาวน์โหลด Openwebmail สำหรับ Debian ด้วยคำสั่ง

      wget http://www.openwebmail.org/openwebmail/download/debian/owm2.53-2.deb
    - ติดตั้งด้วยคำสั่ง dpkg -i owm2.53-2.deb
    - ถ้าติดตั้งไม่ได้ให้ใช้คำสั่ง apt-get –f install
    - ทดสอบเรียกใช้งาน Openwebmail ที่

      http://host_name_or_ip/cgi-bin/openwebmail/openwebmail.pl
    - โดยจะมีการติดตั้งไฟล์ของ Openwebmail ที่เป็นหน้า webpage ไว้ที่

      /usr/lib/cgi-bin/openwebmail
    - และมีการสร้าง Link (shortcut) ชื่อว่า /usr/lib/cgi-bin/openwebmail/etc ไปยังตำแหน่งไฟล์สำหรับการจัดการคอนฟิกที่ตำแหน่งแท้จริงเป็น /etc/openwebmail
    - ทำการคอนฟิก Openwebmail ที่สองไฟล์ดังนี้
      - /etc/openwebmail/openwebmail.conf (First Priority)
      - /etc/openwebmail/defaults/openwebmail.conf (Next Priority)
    - ค่าที่ควรเปลี่ยนแปลงในไฟล์ /etc/openwebmail/openwebmail.conf (First Priority)
      - domainnames south.cattelecom.com
      - enable_viruscheck yes
      - enable_spamcheck yes
      - enable_learnspam yes
      - default_style LushGreen
    - ค่าที่ควรเปลี่ยนแปลงในไฟล์ /etc/openwebmail/default/openwebmail.conf (Next Priority)
      - viruscheck_pipe /usr/bin/clamdscan --disable-summary --stdout –

- spamcheck_pipe /usr/bin/spamc -c -x -t 60 -u @@@USERNAME@@@

  (Spamc is the client half of the spamc/spamd pair. It should be used in place of spamassassin in scripts to process mail)

- learnspam_pipe /usr/bin/sa-learn --spam
- learnham_pipe /usr/bin/sa-learn –ham
- default_locale th_TH.TIS-620 หรือ th_TH.UTF-8
- default_msgsperpage 20 (จำนวนจดหมายต่อหน้า)
- default_filter_badaddrformat yes (ไม่รับจดหมายที่ชื่อผู้ส่งมีรูปแบบไม่ถูกต้อง)
- default_filter_fakedsmtp yes (ไม่รับจดหมายจาก SMTP เซิร์ฟเวอร์ปลอม)
- default_filter_fakedfrom yes (ไม่รับจดหมายที่ใช้ชื่อผู้ส่งปลอม)
- default_filter_fakedexecontenttype yes (ไม่รับจดหมายที่มีการปลอมชนิดของข้อมูล)

- ในกรณีที่เจอปัญหาตอนส่งเมล์ที่เป็นข้อความภาษาไทย แล้วมีฟ้องว่า

  "Wide character" (Wide character in subroutine entry at /usr/lib/cgi-bin/openwebmail/modules/tool.pl line 160.)

  ให้ดูวิธีการแก้ปัญหาได้ที่ http://openwebmail.acatysmoof.com/archive/html/owm-devel/owm-devel.200708/msg00006.html

  ซึ่งหมายถึง UTF 8 มีปัญหาในการสนับสนุนเวอร์ชันในปัจจุบันของ perl's CGI.pm module โดยให้รันคำสั่ง

  perl -e 'use CGI; print "$CGI::VERSION\n";'

  เพื่อหาเวอร์ชันของ CGI.pm ถ้าเวอรัชันเป็น 3.21 หรือสูงกว่า คุณจำเป็นต้องค้นหาไฟล์ CGI.pm ในระบบของคุณโดยใช้คำสั่ง find / -name CGI.pm จากนั้นให้แทนที่บรรทัดที่มีข้อความว่า

  my $utf8 = $charset eq 'utf-8';

  ด้วยข้อความ

  my $utf8 = 0;

12. ติดตั้ง MainScanner

- ติดตั้งด้วยคำสั่ง apt-get install mailscanner
- เมื่อติดตั้งเสร็จจะมีคำแนะนำดังนี้

  Please edit the file /etc/MailScanner/MailScanner.conf according to your needs. Then configure sendmail or exim for use with mailscanner.

  After you are done you will have to edit /etc/default/mailscanner as well. There you will have to

set the variable run_mailscanner to 1, and then type "/etc/init.d/mailscanner start" to start the mailscanner daemon.

- เริ่มคอนฟิกด้วยการสั่งให้ Postfix หยุดการทำงานด้วยคำสั่ง

  /etc/init.d/postfix stop

- สร้างไดเร็คทอรี่สำหรับ SpamAssassin และเซ็ต Permission ด้วยคำสั่ง

  mkdir /var/spool/MailScanner/spamassassin

  chown postfix /var/spool/MailScanner/spamassassin

- สำรองและแก้ไขคอนฟิกของ MailScanner ด้วยคำสั่ง

  cp /etc/MailScanner/MailScanner.conf /etc/MailScanner/MailScanner.conf.bak

  vi /etc/MailScanner/MailScanner.conf

- เซ็ตค่าของ /etc/MailScanner/MailScanner.conf เป็นดังนี้

  %org-name% = ORGNAME

  %org-long-name% = ORGFULLNAME

  %web-site% = ORGWEBSITE

  Run As User = postfix

  Run As Group = postfix

  Incoming Queue Dir = /var/spool/postfix/hold

  Outgoing Queue Dir = /var/spool/postfix/incoming

  MTA = postfix

  Virus Scanners = clamav

  Spam List = SBL+XBL

  SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin

- เซ็ต postfix ด้วยคำสั่ง

  postconf -e "header_checks = regexp:/etc/postfix/header_checks"

- แก้ไข header_checks ด้วยคำสั่ง

  vim /etc/postfix/header_checks

  แล้วเพิ่มบรรทัดต่อไปนี้เข้าไปในไฟล์

  /^Received:/ HOLD

- ทำการ disable permission check ของไดเร็คทอรี่ MailScanner ด้วยการ comment out (เอาเครื่องหมาย # ออก) หน้าบรรทัดที่เป็น check directory (check_dir) และตามด้วย /var/* จำนวน 4 บรรทัด ในไฟล์ /etc/rc2.d/S20mailscanner

- เซ็ต MailScanner มีการ start ตอน boot เครื่องด้วยการกำหนดค่าในไฟล์ /etc/default/mailscanner ให้ค่า run_mailscanner=1

- ทำการ Start MailScanner และ Postfix ดังนี้

  /etc/init.d/mailscanner start

  /etc/init.d/postfix start

- เมื่อเจอปัญหาว่า

  Could not read directory /var/spool/MailScanner/incoming at

  /usr/share/MailScanner//MailScanner/Config.pm line 2488

  Error in configuration file line 166, directory /var/spool/MailScanner/incoming for

  incomingworkdir does not exist (or is not readable) at

  /usr/share/MailScanner//MailScanner/Config.pm line 2812

  Could not read directory /var/spool/MailScanner/quarantine at

  /usr/share/MailScanner//MailScanner/Config.pm line 2488

  Error in configuration file line 170, directory /var/spool/MailScanner/quarantine for

  quarantinedir does not exist (or is not readable) at

  /usr/share/MailScanner//MailScanner/Config.pm line 2812

  ให้ทำการเปลี่ยนเจ้าของของไดเร็คทอรี่ /var/spool/MailScanner ด้วยคำสั่ง

  chown -R postfix:postfix /var/spool/MailScanner

13. ปรับแต่งเพิ่มเติม

- กำหนดขนาดของไฟล์ในการ Attachment ทำได้ด้วยการป้อนข้อความต่อไปนี้เข้าไปในไฟล์

  /etc/postfix/main.cf

  message_size_limit = 40960000

- ในกรณีที่อ่านเมล์แล้วถูกย้ายเมล์ไปยังส่วน “บันทึก” ให้แก้ไขไฟล์

  /usr/lib/cgi-bin/openwebmail/etc/openwebmail.pl และ

  /usr/lib/cgi-bin/openwebmail/etc/default/openwebmail.pl ให้ค่าเป็นดังนี้

  forced_moveoldmsgfrominbox no

  default_moveoldmsgfrominbox no

14. การป้องกันการบุกรุกบน Postfix

เพิ่มค่าพารามิเตอร์ต่อไปนี้ ต่อท้ายไฟล์ mail.cf

smtpd_error_sleep_time = 2s

smtpd_soft_error_limit = 10

smtpd_hard_error_limit = 20

<u>อธิบายเพิ่มเติม</u> บรรทัดแรกเป็น sleep or delay time นั่นคือหลังจากระบบรับรู้ถึงการบุกรุกจำนวน 10 ครั้ง จากแหล่งกำเนิดอันเดียวกัน การบุกรุกในครั้งที่ 11 จะถูกหน่วงไป 12 วินาที และการบุกรุกในครั้งที่ 12

จะถูกหน่วงไป 14 วินาที และครั้งต่อไปจะถูกหน่วงไปทำนองนี้ และเมื่อไปถึงค่า hard limit (20) จะส่งผลให้ client ที่ มีพฤติกรรมไม่เหมาะสม (misbehaving client) ถูกตัดออกจากระบบ

15. **ในกรณีที่มีปัญหาไม่สามารถส่งเมล์ไปยัง Hotmail หรือ Yahoo ได้** ขอแนะนำให้มีการปรับแต่งเพื่อให้มี SPF (Sender Policy Framework) ซึ่งสามารถดูข้อมูลได้ที่ URL ข้างล่างนี้
http://www.itmanage.info/technology/linux/ubuntu/spf/install_spf_on_postfix_ubuntu_dns.pdf

จบครับ