SMTP 노트

Centos5에서 dovecot 설치하기

Dovecot 설치 (centos 5.x버전)

1. Dovecot 패키지 설치

```
$> yum install -y dovecot
```

2. Dovecot 설정

```
$> vi /etc/dovecot.conf#protocols = imap imaps pop3 pop3s
에서 사용할 서비스만 기재
Ef) protocols = imap pop3
listen = * 추가
```

3. 서비스 활성화 후 포트 리슨 확인

```
[root@localhost /]# chkconfig dovecot on
[root@localhost /]# /etc/init.d/dovecot start
[root@localhost /]# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Addres State PID/Program name
tcp 0 0 0.0.0.0:110 0.0.0.0:* LISTEN 2102/dovecot
tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN 2102/dovecot
```

4. 접속테스트 (pop3)

```
$> telnet localhost 110
user test
pass 암호
list (편지함 내역 확인)
+OK 13 messages:
1 5081
retr 1 (편지 읽기)
+OK 5081 octets
```

centos6에서 dovecot 설치하기

1. 활성화 서비스 설정

```
$> vi /etc/dovecot/dovecot.conf
#protocols = imap pop3 lmtp 에서 주석 해제 후 사용할 서비스만 기재 Ef) protocols = imap pop3
#listen = *, :: 에서 listen = * 으로 변경
```

2. 각 계정 메일 데이터 저장소 수동으로 설정

```
$> vi /etc/dovecot/conf.d/10-mail.conf
mail_location = mbox:~/mail:INBOX=/var/spool/mail/%u:INDEX=MEMORY
```

3. SSL을 사용하지 않을경우 (해당 내용을 수정하지 않으면, 993/995번 자동으로 LISTEN)

```
$> vi /etc/dovecot/conf.d/10-ssl.conf
#ssl = yes 에서 ssl = no 로 변경
```

4. SSL 미사용시 암호화 설정 해제

```
$> vi /etc/dovecot/conf.d/10-auth.conf
#disable_plaintext_auth = yes 에서 주석풀고 disable_plaintext_auth = no 로 변경
```

Centos에서 POSTFIX설치하기

Centos6이후부터는 기본SMTP가 Sendmail에서 postfix로 변경되었습니다.

1. Sendmail 패키지 삭제

```
$> yum erase sendmail -y
```

2. Postfix 패키지 설치

```
$> yum install postfix -y
```

3. Postfix 설정

```
vi /etc/postfix/main.cf

mydomain = localhost (발송 호스트네임 기재)
mynetworks_style = host (로컬에서만 발송가능 설정)
mynetworks = 127.0.0.1, 192.168.0/24 (발송할 대역기재)
smtpd_sasl_auth_enable = yes (인증라이브러리 연동)
inet_interfaces = $myhostname (open relay차단, 설정 해제시 all 으로 변경)
postfix,인증라이브러리 연동
```

```
$> vi /usr/lib/sasl2/smtpd.conf
pwcheck_method: saslauthd
chkconfig postfix on
chkconfig saslauthd on
/etc/init.d/postfix start
/etc/init.d/saslauthd start
```

4. 기본 Trouble Shooting
    1. 디렉토리 구조
        1. postfix 파일 디렉토리 : /var/spool/postfix
        2. incoming : 모든 메시지
        3. active : 배달 준비 중인 메시지
        4. deferred : 재전송 시도하는 메시지
        5. corrupt : 배달할 수 없는 메시지
    2. 데이터 관리
        1. 메일 발송 로그는 sendmail 과 동일하게 /var/log/maillog에 기재됨
        2. 메일 데이터는 /var/spool/mail/계정명
    3. Queue관리

```
[root@localhost /]# mailq –> Queue에 쌓인 메일 확인
[root@localhost /]# postfix flush –> Queue 전체 지우기
[root@localhost /]# postsuper -d ALL deferred –> Queue메일 중 Deferred(지연발송메일) 만 삭제
```

        1. 가상 도메인 세팅

```
$> vi /etc/postfix/main.cf
virtual_alias_domain = test.com example.com (등록할 호스트명 기재)
```

        2. Alias 설정

```
$> vi /etc/postfix/main.cf
virtual_alias_maps = hash:/etc/postfix/virtual
```

```
$> vi /etc/postfix/virtual
postmaster@example.com postmaster
info@example.com joe
sales@example.com jane
(메일주소) (실계정명)
```

3. 적용

```
[root@localhost /]# postmap /etc/postfix/virtual
```

clamd설치 / Sendmail 연동하기

clamav 설치

1.Sendmail과 연동하기 위한 패키지 설치

```
$> yum install -y sendmail-devel
```

1. clam바이너리 다운로드 - http://sourceforge.net/projects/clamav/files/clamav/0.97.8/clamav-0.97.8.tar.gz
2. 바이너리 컴파일 & 설치

```
$> tar -zxvf clamav-0.97.8.tar.gz
$> useradd -s /bin/false clamav
$> cd clamav-0.97.8
$> ./configure --prefix=/usr/ --sysconfdir=/etc/ --enable-milter
$> make;make install
```

3. 설정파일 변경 – Freshclam (엔진 업데이트)

```
$> $ vi /etc/freshclam.conf
#Example
...
UpdateLogFile /var/log/clamav/freshclam.log
LogTime yes
DatabaseMirror database.clamav.net
NotifyClamd /etc/clamd.conf
SubmitDetectionStats /etc/clamd.conf
...
```

4. 설정파일 변경 – Clamd (Clamav데몬)

```
$> vi /etc/clamd.conf
LogFile /var/log/clamav/clamd.log
LogTime yes
LogSyslog yes
PidFile /var/run/clamav/clamd.pid
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
TCPSocket 3310
TCPAddr 127.0.0.1
StreamMaxLength 100M
User clamav
PhishingSignatures yes
PhishingScanURLs yes
MaxFileSize 30M
```

5. 설정파일 변경 – Milter(SMTP와 연동)

```
$> vi /etc/clamav-milter.conf
MilterSocket /var/run/clamav/clamav-milter.sock
MilterSocketMode 666
FixStaleSocket yes
User clamav
PidFile /var/run/clamav/clamav-milter.pid
ClamdSocket unix:/var/run/clamav/clamd.sock
OnClean Accept
OnInfected Quarantine
OnFail Defer
LogFile /var/log/clamav/clamav-milter.log
LogTime yes
```

6. 파일 생성 및 권한 변경

```
$> mkdir /usr/share/clamav
$> cd /var/log
$> mkdir clamav
```

```
$> cd clamav
$> touch clamav-milter.log
$> touch clamd.log
$> touch freshclam.log
$> cd /var/run
$> mkdir clamav
$> chown -R clamav.clamav /var/log/clamav
$> chown -R clamav.clamav /var/run/clamav
$> chown -R clamav.clamav /usr/share/clamav
```

7. 엔진 업데이트 & 프로세스 실행

```
$> freshclam
$> /usr/sbin/clamav-milter
```

8. 정상적으로 실행할 경우

```
$> ps -ef | grep clam
clamav 4242 1 0 15:37 ? 00:00:00 clamd
clamav 4251 1 0 15:37 ? 00:00:00 clamav-milter
```

Sendmail연동

1. /etc/mail/sendmail.mc 파일 열어서

```
$> vi /etc/mail/sendmail.mc
...
INPUT_MAIL_FILTER(`clamav`, `S=local:/var/run/clamav/clamav-milter.sock, F=, T=S:4m;R:4m`)
define(`confINPUT_MAIL_FILTERS`, `clamav`)
...
*따음표(‘) 와 역슬래쉬(`)와 구분해야 되요
```

2. sendmail 서비스는 freshclam 후에 구동되도록 설정이 필요.

```
$> chkconfig sendmail off
```

3. 자동으로 엔진업데이트를 하기 위해서는 freshclam 프로세스를 데몬형태로 띄우면 됨(conf파일 정책에 따라 2시간마다 한번씩 업데이트 시도함)

```
$> freshclam -d
```

4. /etc/rc.local에 아래 내용 추가

```
$> vi /etc/rc.local
/usr/sbin/clamd /usr/sbin/clamav-milter freshclam -d
$> /etc/init.d/sendmail start
```

Dovecot Trouble Shooting

1. imap, pop3 포트 변경 시

```
$> vi /etc/dovecot.conf
protocol imap {
listen = *:변경할 포트
}
protocol pop3 {
listen = *:변경할 포트
}
```

2. 홈디렉토리 없는 사용자의 메일을 받고 싶을 때

```
$> $ vi /etc/dovecot.conf
mail_location = mbox:/var/empty:INBOX=/var/spool/mail/%u:INDEX=MEMORY
$ /etc/init.d/dovecot restart
$ useradd -M -s /bin/false 계정명
```

3. imap 로그인 시 로그인 되지 않고, Plaintext 메시지 출력시 (주석 해제한 다음에 dovecot 서비스 재시작)

```
$> vi /etc/dovecot.conf
#disable_plaintext_auth = no
```

4. Centos 6.x 이상버전에서는 config파일 분리
    1. 설정파일 위치 : /etc/dovecot/dovecot.conf
    2. 해당 버전에서의 dovecot은 /etc/dovecot/conf.d/ 폴더에 추가 설정파일이 분산 저장됨
        1. 포트 변경 참조파일 : 10-master.conf
        2. Pop3 미 사용 참조파일 : 10-ssl.conf
        3. disable_plaintext 참조파일 : 10-auth.conf
        4. 메일경로 변경 참조파일 : 10-mail.conf

procmailrc를 이용한 스팸메일 차단

1. 패키지 설치

```
$> yum install procmail -y
```

2. 스팸메일 수신시 관리하는 계정생성

```
$> useradd spam-admin
```

3. 스팸차단 로그 생성

```
$> touch /var/log/procmail
```

4. /etc/procmailrc 파일 생성하기 (샘플)

```
$> vi /etc/procmailrc
##############################################
# 수신 메일 제목을 기준으로 메일 차단하기

#Log file path
LOGFILE=/var/log/procmail

VERBOSE=no

# System Path
PATH=/usr/bin:/usr/local/bin:/bin
SHELL=/bin/sh



# Spam mail Blocking & Forward
:0
* ? formail -x"From" -x"From:" -x"Sender:" \
  -x"Reply-To:" -x"Return-Path:" -x"To:"
/var/spool/mail/spam-admin


# Based on spam lists

:0
* ^Subject: .*[sS][eE][xX]|.*[Pp][Oo][rR][Nn]|.*[Vv][Ii][aA][gG][rR][aA]|.*[Dd][rR][uU][gG]|.*[pP][eE][nN][Ii][sS]|.*[mM][oO][rR][tT][aA][gG][eE].my new photo
/var/spool/mail/spam-admin

:0
* ^Subject: .*포.*르.*노|.*색.*골|.*야.*시|.*목.*록|.*리.*스.*트|.*성.*인|.*몰.*카|.*대.*출|.*보.*험|.*무.*료|.*부업|.*경품|.*만화|.*다이어트
/var/spool/mail/spam-admin


:0
* ^Subject: .*(\{광|\[광|\(광|<광|廣-告|廣告|廣\ 告|廣\.告|=B1=A4=B0=ED|saSw7Q==?=|W7GksO1d|=BC=BA=C0=CE=B1=A4=B0=ED)
/var/spool/mail/spam-admin


:0
* ^Subject: .*(성인|성인정보|성인\ 광고|포르노|색골|야시시|몰카|포X노|투시|야동|페니스|경마|뽀르노|섹스|비아\.그라|카드연체|카드값대출|카드대출|카드빚|카드대납|스카이라이프|skylife)
/var/spool/mail/spam-admin


:0
* ^Subject:.(Re:.)*(Thank you!|Your details|Details|My details|Approved|Your application|Wicked screensaver|That movie)
/var/spool/mail/spam-admin
```

sendmail 로그 분석하기

메일로그 기본구조

로그항목	내 용
From	발신자 주소
Size	메시지의 바이트 크기
Class	메시지의 등급(낮을수록 우선순위 높음)
Pri	시작 메시지의 우선순위 등급
Nrcpts	수신 메시지의 개수
Msgid	메시지 식별자(메시지 헤더)
Proto	수신시 사용된 프로토콜(ESMTP / UUCP)
Relay	메시지를 전달한 장치이름
to	수신자 리스트
Delay	발신에서 수신까지 걸린 시간
Xdelay	전송시도에 걸리는 시간(접속시간)
Mailer	메시지를 전달하는 이름
Stat	전달상태
Ctladdr	메시지를 보낼 수 있는 사용자
Dsn	배달상태 통지

예제로그 설명

Feb 6 14:16:43 mail sendmail[15064]:k165Gg315062: to=**1)test@test.co.kr**,ctladdr=**2)test@test123.co.kr**(570/100), **3)Delay=00:00:00**, **4)xdelay=00:00:00**,**5)mailer=esmtp** **accepted for delivery)**

- 메일을 받는 사용자는 test@test.co.kr
- 메일을 보낸 사용자는 test@test123.co.kr
- 메시지를 발송하는데 걸린시간은 0초,
- 전송시도에 걸린 시간은 0초
- Mailier는 esmtp이고
- 메시지를 전달하는 장치는 test.co.kr
- 메시지는 전송이 정상적으로 완료됨

sendmail Trouble Shooting

Hosts 수정 (부팅 시 sendmail에서 진행이 지연되고 있을 때 진행)

```
$> vi /etc/hosts
서버IP 호스트명 지정
Ef) 1.2.3.4 test.co.kr test.co.kr
```