[365 TIP 27호]

Postfix

작 성 일 자 : 2011-11-14

작 성 자 : slowlygo@net-farm.com

(주) 넷 팜

http://www. 365managed.com

목 차

1. 시 작 하 며

안녕하세요.

날씨가 점점 쌀쌀해 지고 있습니다.

감기 조심하셔야 할 듯 합니다.

이번호에서는 Postfix에 대해 알아보도록 하겠습니다.

Postfix는 CentOS 6.0 에서 기본 메일 전송 에이전트입니다.

http://www.postfix.org/ 를 방문해 보시거나, 혹은 README_FILES 을 대충 보시면 아시겠지만,

설명이 예제위주로 잘 되어있어 쉽게 따라하실수 있습니다.

그냥 한번 읽어보시면 도움이 될만한 간단한 내용으로 구성하였습니다.

진행 환경은 OS는 CentOS 6.0 이며 postfix-2.6.6-2.1.el6_0.x86_64 입니다.

해당 내용에 문의가 있으신 경우, slowlygo@net-farm.com 으로 메일주시면 됩니다.

그럼 시작해 보도록 하겠습니다.

2. 간단 설치 및 설정

CentOS 6.0에서는 기본 메일 전송 에이전트이기 때문에 설치가 되어있습니다.

1) 설치

설치는 간단하게 Yum을 이용해서 설치하시면 됩니다.

```
[root@localhost ~]# yum -y install postfix
[root@localhost ~]# rpm -ql postfix
/etc/pam.d/smtp.postfix
/etc/postfix
/etc/postfix/access
/etc/postfix/canonical
/etc/postfix/generic
/etc/postfix/header_checks
/etc/postfix/main.cf
.....
root@localhost ~]# /etc/init.d/postfix restart
root@localhost ~]# ps aux |grep postfix
root      1928  0.0  0.2  61972  2712 ?        Ss   13:44   0:00 /usr/libexec/postfix/master
postfix   1930  0.0  0.2  62052  2672 ?        S    13:44   0:00 pickup -l -t fifo -u
postfix   1931  0.0  0.2  62120  2716 ?        S    13:44   0:00 qmgr -l -t fifo -u
[root@ocalhost  ~]# netstat -anlp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1051/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      1928/master
tcp        0      0 :::22                       :::*                        LISTEN      1051/sshd
tcp        0      0 ::1:25                      :::*                        LISTEN      1928/master
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
unix  2      [ ACC ]     STREAM     LISTENING     10310  1928/master         private/tlsmgr
unix  2      [ ACC ]     STREAM     LISTENING     10314  1928/master         private/rewrite
.....
```

2) 기본 설정

Postfix 메인 설정파일은 /etc/postfix/main.cf 입니다.

```
[root@localhost ~]# grep "^[^#]" /etc/postfix/main.cf
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
inet_interfaces = localhost
inet_protocols = all
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
debug_peer_level = 2
debugger_command =
        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
        ddd $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
```

간단히 외부 메일 전송 및 수신을 위해서는 3가지만 처리하면 됩니다.

ㄱ. 도메인 설정

ㄴ. 포트외부 오픈

ㄷ. 인증설정

(1) 도메인 설정

설정 유틸로 postconf가 있습니다. 이 명령을 자주 사용합니다.

가장 간단하게는 hostname 설정을 하면 됩니다.
* 추가로 같은 네트웍대 다른 호스트들을 신뢰할수 없는 경우에는 mynetworks_style=host로 설정합니다.
* mydestination 로컬 전송되는 도메인을 의미합니다.
* myorigin 이서버에서 발송시 메일에 나타나는 도메인을 의미합니다.

```
[root@tip ~]# postconf | grep ^my
mydestination = $myhostname, localhost.$mydomain, localhost
mydomain = localdomain
myhostname = localhost.localdomain
mynetworks = 127.0.0.0/8 xxx.xxx.xxx.xxx/24 [::1]/128 [fe80::%eth0]/64
mynetworks_style = subnet
myorigin = $myhostname
[root@tip ~]# hostname tip.365managed.com
[root@tip ~]# postconf | grep ^my
mydestination = $myhostname, localhost.$mydomain, localhost
mydomain = 365managed.com
myhostname = tip.365managed.com
mynetworks = 127.0.0.0/8 xxx.xxx.xxx.xxx/27 [::1]/128 [fe80::%eth0]/64
mynetworks_style = subnet
myorigin = $myhostname
[root@tip ~]# postconf -e mynetworks_style=host
[root@tip ~]# postconf | grep ^my
mydestination = $myhostname, localhost.$mydomain, localhost
mydomain = 365managed.com
myhostname = tip.365managed.com
mynetworks = 127.0.0.1/32 xxx.xxx.xxx.xxx/32 [::1]/128 [fe80::20c:29ff:fe7d:157b%eth0]/128
mynetworks_style = host
myorigin = $myhostname
```

(2) 포트 외부 오픈

```
[root@tip ~]# netstat -antp |grep master
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      3806/master
[root@tip ~]# postconf -e inet_interfaces=all
[root@tip ~]# /etc/init.d/postfix restart
postfix 종료 중:                                           [  OK  ]
postfix를 시작 중:                                         [  OK  ]
[root@tip ~]# netstat -antp |grep master
tcp        0      0 0.0.0.0:25                  0.0.0.0:*                   LISTEN      3896/master
tcp        0      0 :::25                       :::*                        LISTEN      3896/master
```

(3) 인증 설정

외부오픈후 인증설정을 하지 않을 경우, 릴레이서버로 이용당하므로 필히 하셔야 합니다.
아래 README 문서는 보면 자세히 나옵니다.
/usr/share/doc/postfix-2.6.6/README-Postfix-SASL-RedHat.txt
/usr/share/doc/postfix-2.6.6/README_FILES/SASL_README

우선 어떤 인증설정이 가능한지 확인해 보겠습니다.

```
[root@tip ~]# postconf -a
cyrus
dovecot
[root@tip ~]# postconf |grep smtpd_sasl
smtpd_sasl_auth_enable = no
smtpd_sasl_authenticated_header = no
smtpd_sasl_exceptions_networks =
smtpd_sasl_local_domain =
smtpd_sasl_path = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options
smtpd_sasl_type = cyrus
```

ㄱ. 아래 내용을 main.cf 파일에 추가 합니다.

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions =
  permit_sasl_authenticated,
  permit_mynetworks,
  reject_unauth_destination
```

```
[root@tip ~]# /etc/init.d/postfix restart
postfix 종료 중:                                           [  OK  ]
postfix를 시작 중:                                         [  OK  ]
[root@tip ~]# postconf |egrep 'smtpd_sasl|smtpd_recipient_restrictions'
smtpd_recipient_restrictions = permit_sasl_authenticated,  permit_mynetworks,
reject_unauth_destination
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = no
smtpd_sasl_exceptions_networks =
smtpd_sasl_local_domain =
smtpd_sasl_path = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options
smtpd_sasl_type = cyrus
```

smtpd_sasl_local_domain = $myhostname 으로 설정하겠습니다.

```
[root@tip ~]# postconf -e smtpd_sasl_local_domain=₩$myhostname
[root@tip ~]# postconf |grep smtpd_sasl
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = no
smtpd_sasl_exceptions_networks =
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_path = smtpd
smtpd_sasl_security_options = noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options
smtpd_sasl_type = cyrus
```

ㄴ. smtpd_sasl_path = smtpd 설정은 인증 경로를 나타내고 있습니다.

```
[root@tip ~]# cat /etc/sasl2/smtpd.conf
pwcheck_method: saslauthd
mech_list: plain login

# 참고로 pam 파일을 보면
[root@tip ~]# cat /etc/pam.d/smtp.postfix
#%PAM-1.0
auth       include      password-auth
account    include      password-auth
[root@tip ~]# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

ㄷ. pwcheck_method: saslauthd 가 기본설정이므로 cyrus-sasl 설정을 확인하고 서비스를 시작합니다.

```
[root@tip ~]# rpm -qa |grep sasl
cyrus-sasl-lib-2.1.23-8.el6.x86_64
cyrus-sasl-2.1.23-8.el6.x86_64
[root@tip ~]# yum install cyrus-sasl-plain
.....
[root@tip ~]# saslauthd -v
saslauthd 2.1.23
authentication mechanisms: getpwent kerberos5 pam rimap shadow ldap

[root@tip ~]# cat /etc/sysconfig/saslauthd
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/var/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Options sent to the saslauthd. If the MECH is other than "pam" uncomment the next line.
# DAEMONOPTS=--user saslauth

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=
[root@tip ~]# /etc/init.d/saslauthd start
saslauthd (을)를 시작 중:                                  [  OK  ]
```

ㄹ. 최종 간단 테스트

```
[root@localhost ~]# telnet tip.365managed.com 25
Trying xxx.xxx.xxx.xxx..
Connected to tip.365managed.com.
Escape character is '^]'.
220 tip.365managed.com ESMTP Postfix
helo localhost
250 tip.365managed.com
ehlo localhost
250-tip.365managed.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

* mydestination 도메인 수신 체크

```
mail from:test@test.com
250 2.1.0 Ok
rcpt to:slowlygo@tip.365managed.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject:test
test
.
250 2.0.0 Ok: queued as DE4926053B
```

* 릴레이 체크

```
rset
250 2.0.0 Ok
mail from:test@test.com
250 2.1.0 Ok
rcpt to:slowlygo@net-farm.com
554 5.7.1 <slowlygo@net-farm.com>: Relay access denied
```

* 인증 체크

```
rset
250 2.0.0 Ok
auth plain AHNsb3dseWdvAHRlc3Q=
235 2.7.0 Authentication successful
mail from:test.com
250 2.1.0 Ok
rcpt to:slowlygo@net-farm.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject:test
test
.
250 2.0.0 Ok: queued as AF1486053B
```

3. Postfix 관리

1) Postfix 구조

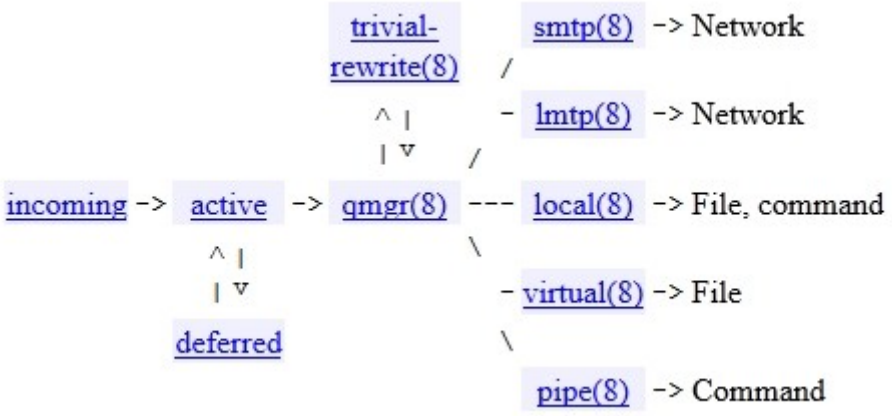
대략적인 윤곽만 잡아 보겠습니다.

자세한 사항은 http://www.postfix.org/OVERVIEW.html 를 참고하시면 됩니다.

이미지만 첨부하였습니다.

(1) 메일 수신 흐름

(2) 메일 발신 흐름



2) SMTP relay와 access control

ㄱ. Postfix는 Protocol, Blacklist, Threshold 기반 접근 통제를 할수 있으며,

다른 접근 제한 방법 또한 지원합니다.

ㄴ. header_checks, body_checks, smtpd proxy 등을 지원합니다.

ㄷ. SMTP conversation 각 단계상에서 접근 제한을 할수 있습니다.

Restriction list name	Status	Effect of REJECT or DEFER result
smtpd_client_restrictions	Optional	Reject all client commands
smtpd_helo_restrictions	Optional	Reject HELO/EHLO information
smtpd_sender_restrictions	Optional	Reject MAIL FROM information
smtpd_recipient_restrictions	Required	Reject RCPT TO information
smtpd_data_restrictions	Optional	Reject DATA command
smtpd_end_of_data_restrictions	Optional	Reject END-OF-DATA command
smtpd_etrn_restrictions	Optional	Reject ETRN command

단계상으로 체크를 하려니 이용하기 불편해서, smtpd_delay_reject 옵션을 default yes로 해서

RCPT TO 혹은 EXRN 명령전에 한번에 체크하도록 설정할수도 있습니다.

적용되는 순서에 유의할 필요가 있습니다.

```
[root@tip ~]# postconf |grep restrictions
smtpd_client_restrictions =
smtpd_data_restrictions =
smtpd_end_of_data_restrictions =
smtpd_etrn_restrictions =
smtpd_helo_restrictions =
smtpd_recipient_restrictions = permit_sasl_authenticated,  permit_mynetworks,
reject_unauth_destination
smtpd_sender_restrictions =
```

/etc/postfix/main.cf 에 아래 내용을 추가하고 테스트를 해보겠습니다.

아래는 kisarbl을 사용하는 예시입니다.

```
smtpd_client_restrictions =
 permit_mynetworks,
 reject_rbl_client spamlist.or.kr
```

패킷을 살짝 잡아보면, 아래 쿼리 확인이 가능합니다.

```
18:41:39.492583 IP xxx.xxx.xxx.xxx.51381 > 168.126.63.1.53: 38285+ A? Xxx.xxx.xxx.xxx.spamlist.or.kr. (45)
18:41:39.515617 IP 168.126.63.1.53 > xxx.xxx.xxx.xxx.51381: 38285 NXDomain 0/0/0 (45)
```

* 현재 네임서버가 168.126.63.1 로 잡혀있습니다.

추가로 smtpd_client_restrictions 로 되어 있어 25번 포트 접속 단계에서 차단되어야 하는데,

rcpt to 명령에서 동작하는 이유는 smtpd_delay_reject = yes 이기 때문입니다.

* 참고로 메일서버 운영시 캐싱네임서버를 운영하는 것이 아무래도 속도 향상에 도움이 됩니다.

* 자세한 내용은 http://www.postfix.org/SMTPD_ACCESS_README.html 를 참고하시기 바랍니다.

3) Lookup Table

Postfix는 접근제어, 주소재작성, 컨텐츠 필터링 등의 정보를 저장하고 확인하기 위해

lookup tables를 이용합니다.

Main.cf를 보시면 아시겠지만, type:table 형식으로 정의됩니다.

```
[root@tip ~]# postconf | grep maps
alias_maps = hash:/etc/postfix/aliases              (local aliasing)
header_checks = regexp:/etc/postfix/header_checks (content filtering)
transport_maps = hash:/etc/postfix/transport       (routing table)
virtual_alias_maps = hash:/etc/postfix/virtual     (address rewriting)
```

어떤 타입을 지원하는 지는 아래와 같이 확인 가능합니다.

관련해서는 postmap 이란 명령어가 있습니다.

```
[root@tip ~]# postconf -m
btree
cidr
environ
hash
ldap
mysql
nis
pcre
proxy
regexp
static
unix
```

Lookup tables에 mysql을 지원하므로 MySQL을 이용할수도 있습니다.

4) master.cf

master.cf를 master 프로세스 설정 파일입니다.

Postfix services 서비스를 통제하는 파일이라고 생각하시면 됩니다.

이파일을 수정해서 외부 필터링 시스템을 이용할수 있습니다.

```
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
smtp      inet  n       -       n       -       -       smtpd
#submission inet n       -       n       -       -       smtpd
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       n       -       -       smtpd
#  -o smtpd_tls_wrappermode=yes
```

```
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       n       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       n       -       -       smtp
        -o smtp_fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
```

간단히 smtp 50000 포트를 추가할 경우, 간단히

50000 inet n - n - - smtpd

라인을 추가후

```
root@tip ~]# /etc/init.d/postfix reload
postfix를 재시작 하고 있습니다:                          [  OK  ]
[root@tip ~]# telnet localhost 50000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 tip.365managed.com ESMTP Postfix
```

간단히 설명드리면, type이 inet일 경우 서비스명은 host:port 와 같은 형식을 취하는데,

50000 번이므로 50000번에 smtpd을 오픈하고 있으라는 의미입니다.

5) qshape tool

qshape 명령어를 통해 queue 상태를 체크할 수 있습니다.

```
[root@tip ~]# yum install postfix-perl-scripts
root@tip ~]# qshape | head
                                T  5 10 20 40 80 160 320 640 1280 1280+
                           TOTAL  0  0  0  0  0  0   0   0   0    0     0
```

자세한 사항은 http://www.postfix.org/QSHAPE_README.html 를 참조하시면 됩니다.

-- 수고 많이 하셨습니다. --

[본 문서의 수정 및 재배포를 금합니다.]