Single UID based POP3 box HOWTO

By Paul Gregg, 1998

신상철 2000년9월5일, 2000년9월28일

이 문서는 부분적으로 재 발행될 수 없음을 알립니다. 이 문서의 최신판은 항상 http://linux.mdworld.com/qmail/ 에서 구하실 수 있습니다. 이 문서는 Qmail을 별도의 시스템 계정 없이 독립된 POP3 계정만으로 다수의 사용자와 다 수의 메일 계정을 다루는 방법을 설명합니다. 이 문서는 Qmail에 대해 대충 알려고 하는 사람이 아닌, 그리고 Qmail을 이용해서 안전하 고 신뢰할 수 있는 POP3 시스템(시스템 사용자가 아닌)을 만들기 위해서 작성되었습니다. 시스템 사용자를 이용하길 원한다면 다른 문서를 읽으십시오. 그렇지 않으면 이 문서가 당 신을 잘못된 방향으로 이끌 것입니다. 어떤 시스템에서 Qmail을 설치할 때 유지보수가 쉽고, 사용자와 도메인의 추가, 변경, 삭제 가 쉽도록 Qmail을 설계하는 일은 매우 권장할 만한 일입니다. 나의 시스템에서는 수백개의 도메인이 정상적으로 작동하고 있으며, 또한 시스템적으로 이상이 없도록 기술적으로 지원을 하고 있습니다. 필자는 이것또한 쉽게 다룰 수 있기를 원합니다.

목 차

제 1 절 시작 **1**

1.1 어떻게 작동하나? 2

1.2 어떻게 domain을 정의할 수 있습니까? 2

1.3 그러면 "domain-com" 유저를 어떻게 정의하고, "domain-com" 유저가 그 domain.com에 해당하는 메일들을 어떻게 받을 수 있게 할 수 있습니까? 2

1.4 위의 내용은 무엇을 뜻합니까? 3

1.5 일단 메일은 분류가 되어 각각 저장되었지만, 그것을 어떻게 POP3 서버로부터 꺼낼 수 있습니까? 3

1.6 그래서 저는 어떤 checkpasswd를 사용해야 합니까? 3

1.7 좋습니다. 그럼 그 파일을 어떻게 설정하고, 어디에 그 파일이 존재하죠? 4

제 2 절 Dot Qmail files. (.qmail) **4**

제 3 절 users/assign 파일 운영하기 **5**

제 1 절 시작

가정 : 이미 Qmail을 설치했고 정상적으로 동작한다는 것을 전제로 합니다. 아주 중요한 파일들 :

```
control/rcpthosts
control/virtualdomains
users/assign
users/poppasswd (checkpasswd를 위한 비표준 password 파일- 밑에서 다시 언급)
```

Note : control/rcpthosts, control/virtualhosts를 변경할 때에는 qmail-send 에 HUP signal 을 보내서 qmail-send가 그 파일들의 변경 사항을 읽을 수 있도록 해야 합니다. 또한 users/assign 파일을 변경할 때에는 아래 부분에 나오는 "users/assign 운영하기"를 참조하 십시오.

[qmail 1.01 또는 그 이전버전의 수신자선택체계는 (수신자 mapping) 여러개의 이 메일 주소에서 당신이 이메일 주소를 mapping할 수 있도록 해주었습니다. 필자는 qmail 1.03에서는 그 자체의 사용을 저하시킬것이라고 생각합니다. - 아마도 필자와 같은 사람들은 메일 포워딩 (forwarding)과 알리아싱 (alias)를 이용하여 그것을 사용하기 때문입니다.]

앞으로 우리는 추가 디렉토리와 도메인마다 하나의 configuration 파일(해당 도메인의 모든 메일계정에 대한 내용을 가지고 있는 파일)을 작성할 것입니다.

1.1 어떻게 작동하나?

users/assign 파일의 구조는 email을 다루기에 매우 유연합니다. 개별적으로 email address 들을 지정할 수도 있고, 다수의 email address를 사용하게 할 수도 있습니다. (예: user-*@domain.com) 또한 여러 도메인의 메일이 하나의 POP3 서버로 갈 수 있도록 domain mapping을 지원합니다.

우리는 alias user는 사용하지 않을 것입니다. (나는 단순히 alias/.qmail-(mailer-daemon | postmaster | root) 만을 사용합니다.) 그리고 내가 다루고 있는 UUCP 사용을 위해서 하나 의 .qmail-uucp-default 만을 사용할 것입니다.(이것은 이 문서의 범위를 벗어납니다.)

1.2 어떻게 domain을 정의할 수 있습니까?

보통 메일 서버에 하나의 도메인을 추가할 때 당신은 control/rcpthosts에 해당 도메인을 맨 밑에 추가합니다. 또한 control/virtualdomains 파일에도 해당 도메인을 추가할 것입니다. 그러나 시스템 유저를 사용하지 않는다면 어떤 형식으로 virtualdomains를 사용해야 할까 요?

다들 아시겠지만 Qmail은 도메인의 "."을 "-"로 변환합니다.(Qmail의 컴파일시에 특별한 옵 션을 주지 않았다면) 그래서 아래와 같이 virtualdomains를 구성할 수 있게 됩니다.

```
domain.com:domain-com
```

Note : control/locals에 위의 domain.com이 포함되어 있지는 않는지 확인해 보십시오. (보통 많은 사람들이 이 부분을 잘못 설정합니다.) control/locals에는 절대 포함되면 안됩니다.

위의 형식은 무엇을 뜻합니까? 이것은 이 도메인의 모든 email이 "domain-com"이라는 사 용자에게 전달될 것을 의미합니다.

1.3 그러면 "domain-com" 유저를 어떻게 정의하고, "domain-com" 유저가 그 domain.com에 해당하는 메일들을 어떻게 받을 수 있게 할 수 있습니까?

그것은 users/assign 파일로부터 시작됩니다. 이 파일은 우리가 나중에 살펴볼 email address를 지정할 수 있는 방법을 제공합니다. 시스템에 email을 추가하기 위해서 당신은 이 파일에 새로운 줄을 추가하게 될 것입니다. 예를 들어 joe@domain.com 라는 email address를 추가한다고 합시다. 아시다시피 domain.com은 "domain-com" 이라는 Qmail 사용 자로 취급이 되기 때문에 Qmail은 "domain-com-joe"란 Qmail 사용자를 users/assign에서 찾게 됩니다.

예)

```
=domain-com-joe:popuser:888:888:/var/qmail/popboxes/domain-conm/joe:::
```

1.4 위의 내용은 무엇을 뜻합니까?

= - 이 기호는 메일 주소와 일치함을 뜻하며 만약 "+" 기호가 나오면 해당 유저가 joe-anything@domain.com 과 같이 확장 전자 우편 주소를 사용할 수 있게 합니다. domain-com-joe - 이것은 virtualdomain에서 정의한 가상 도메인 유저 부분(domain-com) 과 전자 우편 주소 @ 앞에 나오는 계정(joe) 부분, 이렇게 두 부분으로 나뉘어집니다. popuser - 이것은 가상 도메인의 모든 email을 처리할 실제 사용자 (/etc/passwd에 존재)입니다.

```
888 - popuser 사용자의 UID입니다.
888 - popuser 사용자의 GID입니다.
```

/var/qmail/popboxes/domain-com/joe - joe@domain.com 앞으로 온 메일을 어느 디렉토리 에 저장할지를 결정하는 역할을 하는 .qmail 의 위치입니다. 여기서 지정한 디렉토리는 퍼미 션을 반드시 0700으로 지정해야 하며 popuser의 UID/GID를 가져야만 합니다. 또한 여기서 지정한 디렉토리에 .qmail 또는 .qmail-default를 만들고 그 안에 어떻게 메일이 전달될지를 지정해야 합니다. (예의 경우 Maildir로 지정해야 할 것입니다. 아래에 나오는 Dot Qmail 부 분을 참조하십시오.)

나의 경우 위의 각 도메인에 해당하는 email address 지정을 각각의 도메인별로 쪼개어 하 나의 파일로 관리하는 최선의 방법을 발견하였습니다. 아래 부분에 나오는 "users/assign 운 영하기" 부분을 참조하십시오.

이것은 또한 메일을 받을 각각의 디렉토리에도 적용이 됩니다. (아래쪽에 나오는 /var/qmail/popboxes/*/* 파일을 참조하십시오)

1.5 일단 메일은 분류가 되어 각각 저장되었지만, 그것을 어떻게 POP3 서버로부터 꺼낼 수 있 습니까?

위에서 이야기했던 것처럼 모든 메일은 popuser(UID 888, GID 888)의 사용자의 소유로 되 어있습니다. 나는 당신이 Qmail을 처음 설치해서 새로 설정을 한다면 Maildir 형식을 사용 할 것을 권합니다. 이것은 Mailbox 형식보다는 덜 자유롭지만 이 형식을 사용한다면 1년 안 에 나의 이 충고에 대한 고마움으로 나에게 맥주를 사게 될 것입니다.

만약 Qmail이 Maildir 형식을 사용한다면, 당신은 qmail-popup -> checkpasswd -> qmail-pop3d를 사용해야 할 것입니다. 이것들이 무엇이고, 왜 하나의 데몬으로 구동되지 않 느냐구요?

당신도 아시다시피 Qmail은 매우 module 식으로 구성되어 있으며 POP3라고 예외는 아닙니 다. qmail-popup의 역할은 사용자의 계정과 암호를 추출하는 일입니다. 일단 계정과 암호가 추출이 되면 그후에 checkpasswd 가 실행됩니다.(그후 qmail-popup의 역할은 끝나게 됩니다.)

그 다음에 checkpasswd는 사용자의 계정과 암호를 가지고 인증을 시도합니다.(인증의 방법 은 당신이 선택하기에 달려있습니다. 아래 부분을 보십시오) 만약 인증이 성공하면 checkpasswd는 USER, SHELL, HOME 환경변수에 각각의 값을 넣고, 그후에 $HOME/Maildir 아래 USER의(우리가 살펴본 예의 경우 이것은 항상 popuser 이고 HOME의 값은 매번 다르다.) 메일 디렉토리에 있는 메일을 사용자가 POP3를 통해서 꺼낼 수 있도록 qmail-pop3d를 실행하게 됩니다.

여기서 Qmai의 진정한 매력은 당신이 원하는 형태로 인증을 수행할 수 있도록 만들 수 있 다는 것입니다. 시스템 사용자의 인증을 이용할 수도 있고, Radius 인증, PAM 인증 또는 별도의 암호 파일을 통한 인증을 수행할 수도 있습니다.

1.6 그래서 저는 어떤 checkpasswd를 사용해야 합니까?

나는 처음 www.qmail.org에 있는 Jedi's chckpoppasswd를 이용했었습니다. 이것은 당신이 다음의 형태로 이루어지는 암호 파일로 인증을 수행할 수 있게 합니다.

사용자 계정:암호화된(encrypted) 암호:시스템상의 실계정:메일이 저장될 홈디렉토리

POP3 메일만을 사용할 때 위의 내용은 인증으로 충분합니다. Jedi's checkpoppasswd를 약 간 고쳐서 올려 놓은 파일이 http://www.tibus.net/pgregg/projects/qmail/checkpoppasswd.c 에 위치해 있습니다. 나는 언제 사용자가 login 했는지, 인증이 실패했을 때에 무슨 이유로 인증이 실패됐는지를 syslog가 기록하도록 하였고, 또한 해킹이 지연될 수 있도록 암호를 잘못 입력시에 2초를 지연하는 부분을 추가하였습니다.

또한 암호를 잘못 입력할 때에 잘못 입력된 암호를 기록하는 부분도 추가되었습니다. (물론 이것은 syslog와 관련된 부분을 변경함으로써 잘못 입력된 암호를 기록하지 않을 수도 있습 니다.)

1.7 좋습니다. 그럼 그 파일을 어떻게 설정하고, 어디에 그 파일이 존재하죠?

기본적인 나의 설정엔 /var/qmail/users/poppasswd로 되어 있습니다. 간단히 파일을 만들고 아래와 같은 줄을 추가하면 됩니다.

예)

```
testid:DmIMm9e5hc8ic:popuser:/var/qmail/popboxes/domain-com/joe
```

위의 내용은 POP3 사용자로 testid를, 암호로서 testpw를(암호화(encrypted) 되었음.), 또한 실제로 위의 메일을 받을 실계정으로 popuser를, 메일이 저장될 디렉토리로 /var/qmail/popboxes/domain-com/joe를 지정하는 부분입니다.

FAQ#1:그렇다면 어떻게 같은 이름의 joebloggs라는 2명의 유저를 가질 수 있습니까? 나는 joebloggs@domain.com 과 joebloggs@bloggs-n-co.com 이 두 개의 메일을 가지고 있습니 다. 위의 파일 형식대로라면 같은 이름 2명의 joebloggs를 가질 수 없습니다. 어떻게 해야 같은 이름 2명의 joebloggs를 가질 수 있죠?

A: 나는 위의 파일에서 같은 이름 2명의 유저를 가질 수 있다고 말하지 않았습니다. 나는 POP3계정과 전자 우편 주소의 @ 앞 부분에 붙이는 계정과 같아야만 한다고 말한 적이 없 습니다. 다만 대부분의 사람들이 그럴거라고 가정하는 것뿐입니다. 나는 숫자를 매겨가며 계 정을 발급할 것을 추천합니다. 예) 1.pop1, pop2, pop3 ..... pop### 2.pop00001, pop00002, pop00003 .... pop99999 또는 내가 사용하는 방법으로는 3.??0001, ??0002, ??0003, ... ??99999 ?? 는 보통 임의의 문자를 넣거나 사용자의 회사의 이름에 기초를 둔 문자를 사용합니다. 이런 방법은 사용자의 이름과 암호를 추측하여 POP3 서버를 공격하는 해커로부터 보다 안 전합니다.

FAQ#2: 그렇다면 암호화된(encrypted) 암호를 어떻게 만들 수 있습니까?

A: 보통의 경우엔 C나 Perl의 crypt() 함수를 사용함으로써 만들어질 수 있습니다. (unix 시 스템에서 쓰이는 man 3 crypt를 참조하십시오) 그러나 만약 당신이 이것을 잘 모르거나 할 수 없다면 나의 프로젝트 디렉토리에 있는 mkpasswd.pl을 이용할 수 있습니다.

제 2 절 Dot Qmail files. (.qmail)

users/assign 파일에 전자 우편 주소와 그것에 따른 home 디렉토리를 지정하였다면, Qmail 은 그 home 디렉토리에서 Qmail이 어떤 방식으로 메일을 전달할지를 알기 위해 .qmail 파 일을 찾을 것입니다. 따라서 당신은 dot-qmail의 매뉴얼 페이지를 읽어야만 할 것입니다. 간 단히 설명해 보면 .qmail은 다음과 같은 형식 중의 하나가 포함되어 있습니다.

```
./Maildir/ - 이것은 메일을 Maildir 디렉토리에 저장한다는 것을 의미합니다.
./Mailbox - 이것은 표준 mailbox형식으로 메일을 저장한다는 것을 의미합니다.
```

&otheraddress@otherdomain.com - 이것은 다른 전자 우편 주소로 메일을 포워딩(forward) 한다는 것을 의미합니다.

제 3 절 users/assign 파일 운영하기

이전에 언급한 내용 중에 각각의 도메인별로 users/assign 파일을 운영하는 것이 좋을 것이 라는 이야기가 있었습니다. 이것은 기술적인 면이 아닌 여러 가지 이유로 운영하기가 편리 해 질 수 있습니다. (나의 경우 180여 개의 메일 서비스가 되고 있는 250여 개의 도메인을 갖고 있습니다.)

users/assign 파일은 전자 우편 주소 하나당 단순한 한 줄의 내용만을 포함하고 있습니다. (만일 + 기호를 사용한다면 해당 도메인과 해당 사용자가 잠재적으로 많은 전자 우편 주소 를 가질 수 있을 것입니다.) 또한 users/assign 파일의 마지막은 반드시 "." (period) 로 끝나 야 합니다.

만약 users/assign 파일이 변경이 된다면 그에 따른 cdb 데이터베이스 또한 변경이 될 수 있도록 qmail-newu를 실행해야 합니다.

만약 각 도메인별로 별도의 assign 파일을 작성하여 관리한다면, 이것을 users/assign 파일 로 변경하는 스크립트는 다음과 같이 간단합니다. 예를 들어 /var/qmail/users/domains/* 에 각 도메인별로 assign 파일을 작성하였다면

```
#!/bin/sh
cat /var/qmail/users/domains/* > /var/qmail/users/assign.new
echo "." >> /var/qmail/users/assign.new
mv /var/qmail/users/assign.new /var/qmail/users/assign
/var/qmail/bin/qmail-newu
```

(원한다면 assign.new 파일을 작성하는 것은 생략할 수 있습니다. 그러나 이 스크립트의 일 부분은 >! 없이 이미 존재하는 파일을 덮어씌우기를 거부할 것입니다. 하지만 위의 방법은 모두에게 잘 작동할 것입니다.)

좋습니다. 모든 것이 잘 작동하는 것 같습니다. 어떻게 테스트할 수 있습니까?

```
telnet mailhost 110
USER testid
PASS testpw
LIST
RETR 1
QUIT
```

위의 내용들이 전부 실행되고 로그 파일에 auth.warning 와 같은 에러 메시지를 볼 수 없다 면 당신은 성공한 것입니다.