Sendmail에서 DRAC를 이용한 Dynamic Relay(RedHat 7.0)

Author - Colin Bloch bofh@lsn.net 2000년 12월 04일

허창영 escargo@netsource.co.kr 2001년 1월 19일

이 문서는 Sendmail 하에서 access파일과 DRAC(Dynamic Relay Autohrization Control)를 이용한 동적 릴레이 설정과 그 이용에 대한 문서이다. 동적 아이피를 가지는 메일 클라이언 트들의 메일릴레이를 가능하게 하는데 관심있는 사람들을 대상으로 하고 있다. 이글을 번역하고 이곳에 올리는 것을 허락해주신 원작자 Colin Bloch님께 감사의 말씀을 드린다.

목 차

제 1 절 DRAC 소 개 **1**

제 2 절 필요한 패키지, 설치, 시동 **2**

2.1 기본패키지 (Standard RH7.0 distribution packages) 2

2.2 추가패키지 2

2.3 보조패키지(Optional packages) 2

2.4 2. 시스템준비와 DRACD(DRAC daemon) 시동 3

제 3 절 POP3서버, 센드메일 준비와 테스팅 **3**

3.1 POP3서버 준비와 테스팅 3

3.2 DRAC가 동작하게 Sendmail 세팅하기. 4

3.2.1 DRAC가 동작하게 Sendmail 자동 세팅하기. 4

3.2.2 수동 sendmail.cf 설정 4

제 4 절 sendmail, popper 가 drac와 잘 작동하는지 테스트하기 **4**

제 1 절 DRAC 소 개

Sendmail(SMTP) 버젼 최신버젼은 Relay 금지가 Default로 설정되어 있어 localhost외의 Mail Relay는 /etc/mail/access 파일에 relay IP나 host를 등록함으로써 가능한데, 이 방법은 DHCP등으로 IP 등을 부여받는 고정 아이피가 아닌 메일클라이언트(호스트)들의 Relay 관리 에는 많은 불편과 어려움이 따른다. 물론 모든 Relay가 가능하도록 sendmail.cf나 access파 일을 고쳐주는 것이 가장 손쉬운 방법이긴 하겠지만, 이것은 Spammer들의 주요타킷이 되어 버리는 위험을 내포하고 있기도 하고 무엇보다도 Relay설정의 의미를 망각(?)하는 일이 될 것이다. 이러한 동적아이피를 가지는 메일클라이언트들의 Relay 관리에 어려움을 갖고 얼마 전 동적 아이피들의 Relay 허용 여부를 자동으로 관리해주거나 인증을 통해 할 수 있는 툴들이 없을까 찾아보다가 DRAC(Dynamic Relay Authoriazation Control) 말 그대로 '동적릴레이 인증제어'라는 이름을 가진 프로그램을 찾았다. 물론 이 프로그램을 알고 있는 사람도 있겠 지만, 혹여나 알지 못하는 이들에게 도움이 될까하여 DRAC의 설치와 셋팅 방법을 문서를 참 고하여(참고라기보다는 번역의 수준에 가깝다 하겠다) 기술해보고자 한다. 참고로 이 문서는 Redhat 7.0환경에서 인스톨과 셋팅을 기준으로 하였

다. (나머지 환경하에선 추후 추가하거 나 좀 더 좋은 동적릴레이 설정 프로그램을 발견하게 되면 그 것으로 대체하고자 한다.

DRAC는 동적아이피를 가지는 호스트들의 메일릴레이를 POP3를 통한 인증 매카니즘으로 데이터베이스(/etc/mail/dracd.db)를 구축하여 이를 바탕으로 메일릴레이를 허용하는 daemon이다. 다시말하면 localhost 메일서버에 메일 계정을 가지고 있는 사람이 Relay허용 을 인증받지 못한 호스트에서 pop3서버에 접속하여 pop3의 인증에 성공하면 이를 바탕으로 성공했을 때의 아이피 주소를 데이터베이스화하여 이 데이터를 근거로 그 아이피에게 일정 시간동안 메일 릴레이를 허용하게한다.(DRAC의 기본 메일릴레이 유효시간은 30분이지만 이것은 다르게 설정이 가능하다) 일정의 시간이 지나게 되면 다시 그 아이피로서의 메일릴레 이는 닫혀지게 되고 다시 동일한 사용자가 다른 IP로 POP3 인증에 성공하게 되면 다시 그 다 른 아이피는 데이터베이스에 등록되게 되고 그 아이피로 다시 메일릴레이가 가능하게 되는 개념의 프로그램이라고 보면 된다. 물론 동적인 아닌 정적으로 그러니까 영구적으로 메일릴 레이의 설정이 필요한 부분은 /etc/mail/accss파일을 이용하면 되고 이 accss파일의 설정이 DRAC의 설정을 override 즉 선행한다.

제 2 절 필요한 패키지, 설치, 시동

2.1 기본패키지 (Standard RH7.0 distribution packages)

1) xinetd (xinetd-2.1.8.9pre9-6.i386.rpm) – RedHat 7.0 에서 inetd의 변화된 버젼이다.

2) db3-devel (db3-devel-3.1.14-6.i386.rpm)

3) sendmail (sendmail-8.11.0-8.i386.rpm)

4) portmap (portmap-4.0-29.i386.rpm)

위의 패키지들은 레드햇 7.0 기본패키지인데 모든 것이 다 설치되어 있을 수도 있고 그렇지 못할 수 도 있다. 다음과 같이 확인해보고 설치되어 있지 않으면 설치해준다.

```
*확인
$ rpm -q db3-devel    --  나머지 패키지도 마찬가지
*설치
$ rpm -Uvh package_name
```

2.2 추가패키지

drac 운영을 위해 꼭 필요한 패키지들이다. 다운 필수.

- DRAC : *drac-1.11-1.i386.rpm* <http://www.ls-l.net/drac/redhat/drac-1.11-1.i386.rpm>

- qpopper w/drac : *qpopper-3.1.2-1.i386.rpm* <http://www.ls-l.net/drac/redhat/qpopper-3.1.2-1.i386.rpm>

만약 qmail과 같은 Maildir mbox포멧을 지원하는 pop3데몬이 필요하다면 *http://www.ls-l.net/drac/qmail.html* <http://www.ls-l.net/drac/qmail.html> 를 참조한다.

qpopper 설치시 자동으로 xinetd에 필요한 파일들을 자동으로 설치하면서 xinetd를 재시동 하게 되는데 이때 만약 xinetd가 시동되어 있던 상태가 아니라면 FAILD라는 메세지를 보게되 는데 이는 프로그램 설치와 운영에 전혀 영향이 없으니 무시하라.

2.3 보조패키지(Optional packages)

sendmail w/drac - *sendmail-8.11.0-8.i386.rpm* <http://www.ls-l.net/drac/redhat/sendmail-8.11.0-8.i386.rpm>

이 패키지는 DRAC운영을 위해 sendmail-cf의 재구성을 자동으로 하는 패키지이다. 단 이 패 키지를 설치하면 기존의 sendmail.cf를 sendmail.cf.rpmsave로 교체하기 때문에 sendmail.cf를 재구성해야한다.

2.4 2. 시스템준비와 DRACD(DRAC daemon) 시동

1) portmap 이 실행되고 있는지 확인하여 그렇지 않으면 실행

```
- 실행확인
  $ /etc/rc.d/init.d/portmap status
 - 실행
  $ /etc/rc.d/init.d/portmap start
```

2) dracd 실행 $ /etc/rc.d/init.d/dracd start 실행후 /etc/mail/에 dracd.db화일이 생성되었는지 확인

제 3 절 POP3서버, 센드메일 준비와 테스팅

3.1 POP3서버 준비와 테스팅

1) localhost의 pop-3 포트에 접속하여 pop3인증과정으로 dracd DB를 업데이트한다.

```
# telnet localhost 110
  Trying 127.0.0.1...
  Connected to localhost.
  Escape character is '^]'.
  +OK QPOP (version 3.1.2) at mail.my.net starting.
  user foo          <--- localhost의 이메일 계정
  +OK Password required for foo.
  pass bar         <--- 패스워드
  +OK foo has 0 visible messages (0 hidden) in 0 octets.
  quit
  +OK Pop server at mail.my.net signing off.
```

2) /etc/mail/dracd.db화일이 시스템 date와 일치하는지 확인

```
# ls -l /etc/mail/dracd.db
# date
```

3) dracd.db에 IP Address(여기선 127.0.0.1)가 등록되었는지 확인

```
# grep 127.0.0.1 dracd.db
Binary file dracd.db matches   <--- 제대로 등록이 되었을때 출력 메세지
```

3.2 DRAC가 동작하게 Sendmail 세팅하기.

3.2.1 DRAC가 동작하게 Sendmail 자동 세팅하기.

위의 Optional Package sendmail-8.11.0-8.i386.rpm 은 drac-enabled sendmail 즉 drac 가 sendmail에서 동작하도록 자동으로 sendmail.cf를 설정한다. 설치후 sendmail.cf를 재설 정해주어야 한다. 아래와 같이 두가지 방법으로 할 수 있다.(두가지중 한가지 선택)

```
- 재설치
 # rpm -Uvh --force sendmail-.11.0-8.i386.rpm

- 언인스톨하고 재설치
 # rpm -e --nodeps sendmail
 # rpm -Uvh sendmail-.11.0-8.i386.rpm

자동설치는 대부분 잘 작동하지만 만약 제대로 작동하지 않으면 아래의 수동설정을 참고
```

3.2.2 수동 sendmail.cf 설정

```
1) /etc/sendmail.cf  화일을 열어 아래의 라인을 local info 라인 밑에 추가.

# dynamic relay authorization control map
  Kdrac btree /etc/mail/dracd


2) 아래의 내용을  "SLocal_check_rcpt" 에 추가

  # allow recent POP/IMAP mail clients to relay
  R$*                           $: $&{client_addr}
  R$+                           $: $(drac $1 $: ? $)
  R?                            $@ ?
  R$+                           $@ $#OK
주의) 공백은 space가 아니라 tap 키로

3) sendmail 재시동
# /etc/rc.d/init.d/sendmail restart
```

제 4 절 sendmail, popper 가 drac와 잘 작동하는지 테스트하기

```
1) Relay가 금지된 호스트로부터 smtp서버 접속하여 relay 거부 확인

# telnet mail.my.net 25   <---메일서버의 주소
  Trying 192.168.1.1...
  Connected to mail.my.net.
  Escape character is '^]'.
  220 mail.my.net ESMTP Sendmail 8.11.0/8.11.0; Tue, 21 Nov 2000 10:56:01 -0600
  helo blah    <-- 그대로 써줘야 함.
  250 mail.my.net Hello bofh [192.168.1.2], pleased to meet you
  mail from: bgates@microsoft.com
```

```
  250 2.1.0 bgates@microsoft.com... Sender ok
  rcpt to: president@whitehouse.gov
  550 5.7.1 president@whitehouse.gov... Relaying denied  <-- 릴레이가 거부되었다.
  quit
  221 2.0.0 mail.my.net closing connection

2)  pop-3로 포트로 접속하여 릴레이 권한 획득하기

# telnet mail.my.net 110
  Trying 192.168.1.1...
  Connected to mail.my.net.
  Escape character is '^]'.
  +OK QPOP (version 3.1.2) at mail.my.net starting.
  user foo      <--- Smtp 서버의 메일아이디
  +OK Password required for foo.
  pass bar
  +OK foo has 0 visible messages (0 hidden) in 0 octets.  <-- 릴레이 권한 획득
  quit
  +OK Pop server at mail.my.net signing off.

3) 다시 smtp 포트로 접속하여 릴레이를 할 수 있는지 확인

  [root@bofh /root]# telnet mail.my.net 25
  Trying 192.168.1.1...
  Connected to mail.my.net.
  Escape character is '^]'.
  220 mail.my.net ESMTP Sendmail 8.11.0/8.11.0; Tue, 21 Nov 2000 10:56:01 -0600
  helo blah
  250 mail.my.net Hello bofh [192.168.1.2], pleased to meet you
  mail from: bgates@microsoft.com
  250 2.1.0 bgates@microsoft.com... Sender ok
  rcpt to: president@whitehouse.gov
  250 2.1.5 president@whitehouse.gov... Recipient ok  <-- 릴레이 성공
  quit
  221 2.0.0 mail.my.net closing connection
```

위의 과정을 보면 pop-3포트에 접속을 하여 메일계정의 아이디로 인증에 성공하면 /etc/DRACd.db에 접속되어진 IP를 기록하여 그 IP로 접속한 유저가 Relay가 가능하도록 해주 고 있다. 다시말하면 Mail Client 프로그램으로 pop-3포트에 localhost에 있는 메일 아이디 로 접속을 성공하기만 하면 메일 Relay를 가능하게 하고 있다. 동적아이피를 가지고 있는 메 일유저라 할지라도 localhost에 인증된 메일계정만 있으면 sendmail의 /etc/mail/access에 설정해주지 않더라도 얼마든지 Relay설정을 동적으로 생성하여 Relay를 가능하게 해준다.

참고로 /etc/DRACd.db에 기록되어진 IP data는 기본으로 30분의 데이터유효시간을 가지지만 *http://mail.cc.umanitoba.ca/drac* <http://mail.cc.umanitoba.ca/drac>를 살펴보면 이 유효시간을 조절할 수 있다.

참고로 이 DRAC를 이용해 릴레이 가능하게 하려면 PO3유저는 꼭 POP3 서버에 접속하는 것이 선행되어야 한다. 만약 DRAC 인증 유효시간이 종료되었다면 Relay 거부 메세지를 받을 것이다.

이글의 원문은 번역되어진 것과 약간 다르다. 직역을 하지 않고 의역을 했기 때문이다. 하지만 의미전달에는 별 차이가 없을 줄 안다. 원문을 보고자 하는 분은 *http://www.ls-l.net/drac* <http://www.ls-l.net/

drac/>을 참조하면 된다.