

Procmail ile Eposta Filtreleme NASIL

Yazan:
Genco Yılmaz
<gencoyilmaz (at) gmail.com>

Ekim 2002

Özet

Procmail, sisteminize gelen iletilerin sizin belirlemiş olduğunuz kurallar çerçevesinde seçilmesini, düzenlenmesini ve istenirse süzülerek yok edilmesini sağlayabilen bir programdır. Örneğin konu kısmında "I love you" yazan bir iletinin sisteminizde hiçbir kullanıcının eline geçmeden /dev/null dizininin uçsuz bucaksız enginliğinde kaybolmasını istiyorsanız bu programı kullanabilirsiniz.

Konu Başlıkları

1. Giriş	3
2. Kurulum	3
2.1. Programı indirelim	3
2.2. Programı kuralım	4
3. Kullanım	4
3.1. Sistem genelinde iletileri süzme	4
3.2. Bir kullanıcıya gelen iletileri süzme	7
3.3. Procmail .rc dosya biçemi hakkında	7
4. Sıkça Sorulan Sorular	7

Geçmiş

1.0

Ekim 2002

GY

İlk sürüm – Belgenin özgün sürümü <https://genco.marketweb.net.tr/Belgeler/> adresinde bulunabilir.

Yasal Uyarı

Bu belgenin, *Procmall ile Eposta Filtreleme NASIL*, 1.0 sürümünün **telif hakkı © 2002 Genco Yılmaz'a** aittir. Bu belgeyi, Free Software Foundation tarafından yayınlanmış bulunan GNU Özgür Belgeleme Lisansının 1.1 ya da daha sonraki sürümünün koşullarına bağlı kalarak kopyalayabilir, dağıtabilir ve/veya değiştirebilirsiniz. Bu Lisansın bir kopyasını <http://www.gnu.org/copyleft/fdl.html> adresinde bulabilirsiniz.

BU BELGE “ÜCRETSİZ” OLARAK RUHSATLANDIĞI İÇİN, İÇERDİĞİ BİLGİLER İÇİN İLGİLİ KANUNLARIN İZİN VERDİĞİ ÖLÇÜDE HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR. AKSİ YAZILI OLARAK BELİRTİLMEDİĞİ MÜDDETÇE TELİF HAKKI SAHİPLERİ VE/VEYA BAŞKA ŞAHISLAR BELGEYİ “OLDUĞU GİBİ”, AŞIKAR VEYA ZIMNEN, SATILABİLİRLİĞİ VEYA HERHANGİ BİR AMACA UYGUNLUĞU DA DAHİL OLMAK ÜZERE HİÇBİR GARANTİ VERMEKSİZİN DAĞITMAKTADIRLAR. BİLGİNİN KALİTESİ İLE İLGİLİ TÜM SORUNLAR SİZE AİTTİR. HERHANGİ BİR HATALI BİLGİDEN DOLAYI DOĞABİLECEK OLAN BÜTÜN SERVİS, TAMİR VEYA DÜZELTME MASRAFLARI SİZE AİTTİR.

İLGİLİ KANUNUN İCBAR ETTİĞİ DURUMLAR VEYA YAZILI ANLAŞMA HARİCİNDE HERHANGİ BİR ŞEKİLDE TELİF HAKKI SAHİBİ VEYA YUKARIDA İZİN VERİLDİĞİ ŞEKİLDE BELGEYİ DEĞİŞTİREN VEYA YENİDEN DAĞITAN HERHANGİ BİR KİŞİ, BİLGİNİN KULLANIMI VEYA KULLANILAMAMASI (VEYA VERİ KAYBI OLUŞMASI, VERİNİN YANLIŞ HALE GELMESİ, SİZİN VEYA ÜÇÜNCÜ ŞAHISLARIN ZARARA UĞRAMASI VEYA BİLGİLERİN BAŞKA BİLGİLERLE UYUMSUZ OLMASI) YÜZÜNDEN OLUŞAN GENEL, ÖZEL, DOĞRUDAN YA DA DOLAYLI HERHANGİ BİR ZARARDAN, BÖYLE BİR TAZMİNAT TALEBİ TELİF HAKKI SAHİBİ VEYA İLGİLİ KİŞİYE BİLDİRİLMİŞ OLSA DAHI, SORUMLU DEĞİLDİR.

Tüm telif hakları aksi özellikle belirtilmediği sürece sahibine aittir. Belge içinde geçen herhangi bir terim, bir ticari isim ya da kuruma itibar kazandırma olarak algılanmamalıdır. Bir ürün ya da markanın kullanılmış olması ona onay verildiği anlamında görülmemelidir.

1. Giriş

Procmail, sisteminize gelen mesajların sizin belirlemiş olduğunuz kurallar çerçevesinde seçilmesini , düzenlenmesini ve istenirse süzülerek yok edilmesini sağlayabilen bir programdır. Örneğin konu kısmında "*I love you*" yazan bir iletinin sisteminizde hiçbir kullanıcının eline geçmeden `/dev/null` dizininin uçsuz bucaksız enginliğinde kaybolmasını istiyorsanız bu programı kullanabilirsiniz. Yapabilecekleriniz sadece bunlarla sınırlı değil. Gelen iletinin başlık bilgisine göre `from` ve `to` satırlarına, iletinin gövdesi ya da boyutuna bakarak sınırlama getirebilirsiniz.

Procmail, Stephen R. van den Berg <[srb\(at\)cuci.nl](mailto:srb@cuci.nl)> abimiz tarafından yazıldı ve bu belgeyi yazarken güncel sürüm numarası "3.22" idi.

Bu programı iki şekilde kullanabiliyorsunuz. Eğer sistem yöneticisi iseniz, sisteminize gelen bütün iletilere süzgeç uygulayabiliyorsunuz. Değilseniz, size gelen iletileri siz görmeden silebilir (tabii ki istemedikleriniz) ya da belli dizinlere otomatik olarak taşıyabilirsiniz.

2. Kurulum

Sisteminizde procmail kurulumu değil mi bir bakın:

```
# procmail -v
```

Komut, aşağıdakine benzer bir çıktı vermiyorsa program kurulu değildir.

```
procmail v3.21 2001/06/29
  Copyright (c) 1990-1999, Stephen R. van den Berg      <srb@cuci.nl>
  Copyright (c) 1997-2001, Philip A. Guenther           <guenther@sendmail.com>

Submit questions/answers to the procmail-related mailinglist by sending to:
  <procmail-users@procmail.org>

And of course, subscription and information requests for this list to:
  <procmail-users-request@procmail.org>

Locking strategies:      dotlocking, fcntl(), lockf(), flock()
Default rcfile:          $HOME/.procmailrc
Your system mailbox:     /var/spool/mail/root
```

Yinede emin olamıyorsanız, programın kurulu olup olmadığını

```
# find / -name procmail -print
```

komutunu vererek öğrenebilirsiniz.

Gördüğünüz gibi programın bendeki sürümü de eski. Birazdan birlikte kuracağız yenisini. Hadi bakalım.

2.1. Programı indirelim

Programı <http://genco.marketweb.net.tr/Documents/download/procmail-3.22.tar.gz> adresinden ya da aşağıdaki adreslerin birinden indirebilirsiniz:

- <ftp://ftp.procmail.org/pub/procmail/>
- <ftp://ftp.psg.com/pub/unix/procmail/>
- <ftp://ftp.ucsb.edu/pub/mirrors/procmail/>
- <ftp://ftp.informatik.rwth-aachen.de/pub/packages/procmail/>
- <ftp://ftp.fu-berlin.de/pub/unix/mail/procmail/>

- <ftp://ftp.fu-berlin.de/pub/unix/mail/smartlist/>
- <ftp://ftp.net.ohio-state.edu/pub/networking/mail/procmail/>
- <ftp://ftp.fdt.net/pub/unix/packages/procmail/>
- <ftp://ftp.tamu.edu/pub/mirrors/procmail/>
- <ftp://ftp.kfki.hu/pub/packages/mail/procmail/>
- <ftp://giswitch.sggw.waw.pl/pub/unix/procmail/>
- <ftp://ftp.meltzer.org/pub/procmail/>
- <ftp://ftp.win.ne.jp/pub/network/mail/procmail/>
- <http://www.ring.gr.jp/archives/net/mail/procmail/>
- <ftp://ftp.ring.gr.jp/pub/net/mail/procmail/>
- <ftp://ftp.ayamura.org/pub/procmail/>
- <ftp://sunsite.cnlab-switch.ch/mirror/procmail/>
- <ftp://ftp.linja.net/pub/mirrors/procmail/>
- <ftp://ftp.stealth.net/pub/mirrors/ftp.procmail.org/pub/procmail/>
- <ftp://ftp.mirror.ac.uk/sites/ftp.procmail.org/pub/procmail/>

2.2. Programı kuralım

İndirdiğimiz paket `procmail-3.22.tar.gz` olsun. Aşağıdaki adımları gerçekleştirelim. Programı açıyor ve yüklüyoruz. `make install` komutunu vermeden önce `Makefile` dosyasını açıp istediğiniz yapılandırmayı kullanabilirsiniz. Ben öntanımlı olanları kullanıyorum.

```
# mv procmail-3.22.tar.gz /usr/local
# cd /usr/local
# tar -zxvf procmail-3.22.tar.gz
# cd procmail-3.22
# make install
```

Programın yüklendiğinden emin olalım.

```
# procmail -v
```

Komut aşağıdaki çıktıyı veriyor.

```
procmail v3.22 2001/09/10
Copyright (c) 1990-2001, Stephen R. van den Berg      <srb@cuci.nl>
Copyright (c) 1997-2001, Philip A. Guenther          <guenther@sendmail.com>

Submit questions/answers to the procmail-related mailinglist by sending to:
    <procmail-users@procmail.org>

And of course, subscription and information requests for this list to:
    <procmail-users-request@procmail.org>

Locking strategies:      dotlocking, fcntl(), lockf(), flock()
Default rcfile:          $HOME/.procmailrc
Your system mailbox:     /var/spool/mail/root
```

Programımız kuruldu, şimdi kullanımına geçiyoruz.

3. Kullanım

3.1. Sistem genelinde iletileri süzme

```
# touch /etc/procmailrc
```

/etc dizininin altında `procmailrc` adında dosyamızı oluşturduk. Bu dosyanın içine aşağıdaki satırları yazın:

```
# Hata ayıklaması yapacağınız zaman 'yes' yazın.
VERBOSE=no

# Hata ayıklaması yapacağınız zaman ## karakterlerini silin;
# olay kayıtları fazla gelirse 'no' yazın.
## LOGABSTRACT=all

# Kendi dizininizi kullanmak isterseniz $HOME/Msgs yazın
# Mutt ve elm $HOME/Mail kullanır
# Pine $HOME/mail kullanır
# Netscape Messenger $HOME/nsmail kullanır
# Bazı NNTP istemcileri, örneğin slrn ve nn, $HOME/News kullanır
# maildir biçimindekiler çoğunlukla $HOME/Maildir kullanır
MAILDIR=$HOME/mail          # Bu dizin mutlaka mevcut olmalı!

# procmail ile ilgili dosyaların saklanacağı dizin
##PMDIR=$HOME/Procmail
PMDIR=/etc/Procmail
# Olay kayıtlarının tutulmamasını istiyorsanız
# LOGFILE satırının başına ## koyunuz (önerilmez)
LOGFILE=$PMDIR/log
INCLUDEDRC=$PMDIR/Rc/subject.rc
INCLUDEDRC=$PMDIR/Rc/spamlist.rc
INCLUDEDRC=$PMDIR/Rc/body.rc
INCLUDEDRC=$PMDIR/Rc/trailer.rc
```

Yukarıdaki `MAILDIR=$HOME/mail` ifadesini ev dizininizde bulunan posta kutunuzun biçimine göre değiştirin. Örneğin bende `/home/genco` dizininde `mail` adında bir dizin bulunduğu için bu ifade olduğu gibi kalıyor.

`PMDIR` değişkenini, `procmail`'in kullanacağı dosyaların bulunduğu dizin adına atayalım. Yukarıda bizim tanımımız `PMDIR=/etc/Procmail` şeklinde.

`INCLUDEDRC` değişkeni, `/etc/Procmail/Rc` dizini içindeki süzme işlemini gerçekleştirecek dosyalarımızı gösteriyor. Her bir kural için ayrı bir dosya oluşturarak sistemimize modüler bir yapı kazandırıyoruz. Böylece ileride bir kuralı çıkarmak istediğinizde `procmailrc` dosyasından bu satırı silmeniz yeterli olacaktır.

Dizinlerimizi ve dosyalarımızı oluşturalım.

```
# mkdir /etc/Procmail
# touch /etc/Procmail/log
# mkdir /etc/Procmail/Rc
# touch /etc/Procmail/Rc/subject.rc
# touch /etc/Procmail/Rc/spamlist.rc
# touch /etc/Procmail/Rc/body.rc
# touch /etc/Procmail/Rc/trailer.rc
# mkdir etc/Procmail/Filtered
```

/etc/Procmail/Rc/subject.rc

```
:0:
* ^Subject:.*\<I love you\>
```

```
/etc/Procmail/Filtered/subject
```

`subject.rc` dosyasının içine yukarıda satırları yazalım. Bu dosya yardımıyla procmail, sisteminize gelen epostaların başlığındaki `subject` satırını tarayarak, içinde *"I love you"* olan iletileri `/etc/Procmail/Filtered/subject` adındaki dosyaya gönderir.

Örnekler üzerinden gidilip birkaç örnek sonra bu dosyalardaki sözdizimi ile ilgili açıklama yapılacaktır.

/etc/Procmail/Rc/spamlist.rc

```
FROM_=`formail -rt -xTo: \  
  | expand | sed -e 's/^[ ]*//g' -e 's/[ ]*$//g'`  
  
:0  
  
* $ ? echo ${FROM_} | grep ${FROM_} '/etc/Procmail/black.list'  
  
/etc/Procmail/Filtered/spam
```

`spamlist.rc` dosyasına da yukarıdaki satırları yazalım. Bu satırlar ne anlatıyor?

Gelen iletiden `from` bilgisi `formail` programı ile alınıyor. (Bende `formail` programı var mı diye şüphe içerisindeyseniz, düşünmeyin. Procmail programını kurarken aynı zamanda onu da yüklediniz.) Daha sonra `/etc/Procmail/black.list` dosyasında bu `from` bilgisi var mı yok mu aranıyor. Eğer bulunursa bu ileti, `inbox` yerine `/etc/Procmail/Filtered/spam` dosyasına yazılıyor.

Bu eposta adresinin `spam` olduğuna kesin eminseniz `spam` dosyası yerine `/dev/null`'ın engin derinliğinde gönderebilirsiniz.

`/etc/Procmail/black.list` dosyasını oluşturup bu dosyanın içine sisteminizi rahatsız eden eposta adreslerini kayıt edebilirsiniz. Bu sayede kendi spam listenizi oluşturabilirsiniz.

/etc/Procmail/Rc/body.rc

```
:0 B:  
  
* I send you this file in order to have your advice  
/etc/Procmail/Filtered/dustbin
```

`body.rc` dosyasının içine yazacağınız yukarıdaki satırlar, gelen iletilerin gövdesini tarayarak içinde *"I send you this file in order to have your advice"* yazan satırı bulursa iletiyi `/etc/Procmail/Filtered/dustbin` adlı dosyaya atacaktır. Bu satır bildiğiniz gibi geçenlerde birçok kimseyi rahatsız eden virusun gövdesinde yazıyordu.

Benim `dustbin` dosyamın boyutu aradabir artıyor :))

/etc/Procmail/Rc/trailer.rc

```
:0 fb  
* ? test -r /etc/trailer.txt  
  | cat - ; \  
    sed -e "s/\$/g" \  
      </etc/trailer.txt
```

`trailer.rc` dosyasının içeriğide yukarıdaki gibi. Peki bu dosya ne yapar? Aslında pek bir şey yapmaz. Gelen her iletinin en alt kısmına sizin belirlemiş olduğunuz satırları ekler. Giden iletilere ekleyebilseydi daha iyi olurdu:.)

Bunun çalışması için `/etc/trailer.txt` dosyasını oluşturalım ve içine her iletiye eklemek istediğimiz satırları yazalım.

3.2. Bir kullanıcıya gelen iletileri süzme

Süzme işlemini sadece bir kullanıcı için yapacaksak kullanıcının ev dizininde `.procmailrc` adında bir dosya oluşturmamız yeterli olur.

Bu dosyanın içine yukarıdaki `*.rc` uzantılı dosyaların içeriklerini yazmamız süzme işini başlatır. Bunun haricinde başka bir şey yapmamıza gerek yok.

Bu belgede bulunan RC dosyalarındaki kuralların haricinde örnekler görmek isterseniz, <http://www.uwasa.fi/~ts/info/proctips.html> adresinde 40 adet örnek bulunmaktadır.

3.3. Procmail .rc dosya biçemi hakkında

Sözdizimi	Anlam

:0	Kuralı başlatır.
:	rc dosyasının bulunduğu yerde lock dosyası oluşturur.
*	koşul ifademize başlamamızı sağlar.
^Subject:	başlıkta subject ile başlayan satırı arar. ^TO_ yazarsanız to satırını arar.
/etc/Procmail/Filtered/subject	işlem gören iletinin hangi dosyaya gideceğini belirtir.

4. Sıkça Sorulan Sorular

Gelen eposta iletilerini eklerindeki dosyaların uzantılarına göre nasıl süzebilirim?

`attachment.rc` adında bir dosya oluşturup aşağıdaki tanımlı, dosyanın içine yazıp önceki bölümlerde anlatıldığı şekilde `/etc/Procmail/Rc` dizinine yerleştirelim. (`/etc/procmailrc` dosyasına gerekli tanımlı girmeyi unutmayın. Gerekli işlemler burada anlatılmayacak.)

Aşağıdaki tanımda `bat|bif|exe|pif|com|vbs` satırı dosya uzantılarına karşılık gelmektedir. Bu satıra ekleyeceğimiz uzantılar sistem tarafından `/etc/Procmail/Filtered/virus` adlı dosyaya yazılacaktır. Örneğin `bat|bif|exe|pif|com|vbs` satırını `bat|bif|exe|pif|com|vbs|.jpg` şeklinde değiştirirseniz sisteme gelen eposta iletlerinde `.jpg` uzantılı dosya bulunduğu takdirde ileti `/etc/Procmail/Filtered/virus` dosyasına gönderilir.

```
:0HB
* ^Content-Type: MULTIPART/MIXED
* ^Content-Disposition: (attachment|inline);
* filename=".*\.(bat|bif|exe|pif|com|vbs)"
```

/etc/Procmail/Filtered/virus

Bir dosya içerisinde birden fazla kural belirtebilir miyim?

Elbette :) Bir dosya içerisinde bir kurala başlayıp bitirdikten sonra ikinci kural için tekrar bir başlangıç yapmanız (bir kurala : 0 karakterleriyle başlanıyordu) gerekir.

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

Bu dosya (procmail-nasil.pdf), belgenin XML biçiminin \TeX Live ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

4 Şubat 2007