

Postfix ile E-Posta Sistemi

Devrim GÜNDÜZ
PostgreSQL Geliştiricisi
Red Hat Certified Engineer

devrim@gunduz.org
devrim.gunduz@linux.org.tr

10.02.2010
Muğla

Akademik Bilişim 2010



Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix nedir?

- Wietse Zweitze Venema tarafından geliştirilen bir MTA.
- <http://www.postfix.org>
- Sendmail'e alternatif olarak geliştirildi.
- Ancak Sendmail'den çok daha güvenli ve hızlıdır -- ayrıca çok daha fazla özelliklere sahiptir.

Postfix nedir?

- LDAP, Veritabanı ve SMTP auth desteđi
- Birçok AV ile beraber çalışabilme
- Greylisting, antispam destekleri
- Son sürüm: 2.6.5

Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix kurulumu

- Tüm dağıtımlarda Postfix gelir.
- Paket yöneticisi ile kurulabilir.
- Özelleştirme için kaynak koddan derlenebilir ya da dağıtım paketleri özel olarak baştan derlenebilir.

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix kurulumu

- Fedora/Red Hat/CentOS
yum install postfix
- Bu paket içindeki özellikler sınırlıdır.
Veritabanı, TLS gibi destekler için
SRPM'den derlemek gereklidir.
- <http://postfix.wl0.org/en/>
adresinden SRPM indirilebilir.

Postfix kurulumu

- Debian/Ubuntu

`apt-get install postfix`

`postfix-gld, postfix-policyd-spf-perl, postfix-policyd,
postfix-cdb, postfix-dev, postfix-doc, postfix-ldap,
postfix-mysql, postfix-pcre, postfix-pgsql, postfix,
postfix-policyd-spf-python`

Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix'in temel yapılandırması

- /etc/postfix dizini
- main.cf, master.cf
- Düzgün, okunabilir yapılandırma dosyaları

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix'in temel yapılandırması : main.cf

myhostname: Postfix'in çalıştığı
makinanın tam alan adı (FQDN)

Örnek: myhostname = mail.gunduz.org

mydomain: Makinanın alan adı.

Örnek: mydomain = gunduz.org

myorigin: Öntanımlı alan adı. Bu alan
adının reverse DNS kaydı olması
gereklidir:

Örnek: myorigin = gunduz.org

Postfix'in temel yapılandırması : main.cf

`inet_interfaces` : Sunucunun e-postaları kabul ettiği ağ adres(ler)ini belirten parametredir.

Postfix öntanımlı olarak loopback aygıtını dinler. Dışarıdan e-posta kabul etmek için bu parametreyi değiştirmek gereklidir.

Örnek: `inet_interfaces = all`

Postfix'in temel yapılandırması : main.cf

mydestination: Postfix'in e-posta kabul edeceği alan adlarının belirtildiği parametredir. Burada önceden yazdığımız mydomain gibi değişkenleri doğrudan kullanabiliriz.

*Örnek: \$mydomain,
planetpostgresql.org*

Postfix'in temel yapılandırması : main.cf

- mynetworks : Postfix'in relay edilmesine izin verdiği ip adresi ya da adreslerinin belirtildiği parametre.
Örnek : mynetworks = 127.0.0.1/8, 78.189.47.167/32
- home_mailbox : Mailbox/Maildir seçeneklerinin kullanıldığı parametre.
- alias_maps : Aliasların tutulduğu dosya.
- *Örnek: alias_maps= hash:/etc/aliases*

Postfix'in temel yapılandırması : master.cf

- Giriş seviyesinde bir e-posta sunucusu kurmak için bu dosyayı değiştirmenize gerek yoktur.
- Ancak, eğer e-posta sunucunuzun 25. port dışında da(örnek: submission portu) kabul etmesini istiyorsanız:
submission inet n – n - - smtpd
satırını eklemek gereklidir.

Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam engelleme

- Windows virüslerini engellemek gerekli.
- Aslında Windows'un kendisi virüs!
- Her ne kadar sunucu Linux olsa da Windows istemciler arasındaki haberleşmelerde bir virüs kontrolü gerekli.
- Spamcileri de unutmamak gerekli.
- Greylisting kavramını az sonra anlatacağım.

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam engelleme

- Anahtar teslimi çözüm:
 - ClamAV : Antivirüs
<http://www.clamav.net/>
 - AMaViS (amavisd-new): MTA ve AV/SpamAssasin arasındaki katman
<http://www.ijs.si/software/amavisd/>
 - SpamAssassin : Antispam yazılımı
<http://spamassassin.apache.org/>

Postfix ile virüs ve spam engelleme

- ClamAV: Antivirüs yazılımı
- Virüs veritabanı oldukça sık güncelleniyor.
- Yüksek bir başarıımı var.
- Açık kaynak kodlu ve ücretsiz.
- Hemen hemen her dosyayı inceleme yeteneğine sahip.

Postfix ile virüs ve spam engelleme

- ClamAV, Amavisd-new ve SpamAssassin dağıtımlarla genelde beraber geliyor
- ClamAV için CentOS/Red Hat için DAG deposunu kullanmanızı öneririm. EPEL deposundaki paketlerin yapılandırması biraz dertli :-)

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam engelleme

- ClamAV paketleri:
 - Clamav : ClamAV yazılımı
 - Clamd: Daemon
 - Clamav-db: Virüs veritabanı
- Hepsini kurmak gerekiyor.

Postfix ile virüs ve spam engelleme

- ClamAV yapılandırması:
clamd.conf
LocalSocket parametresini belirlemek gerekiyor.
LocalSocket /tmp/clamd.socket gibi birşey yapılabilir. Bu bilgiyi AMaViS içinde kullanacağız.
- Diğer ayarları değiştirmenize genelde **gerek yok.**
- Servisi başlatmayı unutmayın.

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam temizleme: AMaViS

- MTA ile AV ve SpamAssassin arasındaki kontrolü sağlayan bir yazılım.
- Yüksek performanslı. Perl ile geliştiriliyor.
- Açık kaynak kodlu ve ücretsizdir.

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam engelleme : AMaViS

- Amavisd yapılandırması:
/etc/amavisd.conf
- COMMONLY ADJUSTED SETTINGS bölümü ilginizi çekecektir ;)
max_servers, mydomain,
QUARANTINEDIR, mynetworks,
inet_socket_port

Postfix ile virüs ve spam engelleme : AMaViS

- `$sa_tag_level_deflt`
- `$sa_tag2_level_deflt`
- `$sa_kill_level_deflt`
- `$sa_dsn_cutoff_level`
DSN: Delivery Status Notification
- `$sa_spam_subject_tag`
-

Postfix ile virüs ve spam engelleme : AmaViS

amavisd.conf içinde ClamAV ile ilgili satırlar:

- ['ClamAV-clamd',
- \&ask_daemon, ["CONTSCAN {}\n",
"/tmp/clamd.socket"],
- qr/\bOK\$/, qr/\bFOUND\$/,
- qr/^\.*?: (?!Infected Archive)(.*) FOUND\$/],
- # NOTE: run clamd under the same user as amavisd, or run it under its own uid such as clamav, add user clamav to the amavis group, and then add AllowSupplementaryGroups to clamd.conf;

Postfix ile virüs ve spam engelleme - SpamAssassin

- SpamAssassin **genelde** kutudan çıktığı hali ile yeterli oluyor.
- Ancak yoğun sistemlerde bazı ayarlar yapmak gerekebilir.

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile virüs ve spam engelleme

- SpamAssassin

- Fedora / Red Hat / CentOS ayarları /etc/mail/spamassassin altında ayar dosyaları var
- /etc/sysconfig/spamassassin dosyası içinde şu satırı göreceksiniz:
SPAMDOPTIONS="-d -c -m5 -H"
- -m ile aynı anda çalışabilecek child processler ayarlanır. Bunu arttırmak, yoğun sistemlerde maillerin daha hızlı kontrol edilmesini sağlar.

Postfix ile virüs ve spam engelleme - SpamAssassin

- Ubuntu ve Debian'da:
/etc/default/spamassassin
- `OPTIONS="--create-prefs --max-children 10 --helper-home-dir"`
satırını önceki slaytta anlattığım gibi değiştirebilirsiniz.

Postfix'de Virüs ve Spam Engelleme – Postfix tarafı

- AmaViS, ClamAV ve SpamAssassin kurmak yeterli deęil. Postfix'i bundan haberdar etmek gerekiyor :-)
- Yapılandırmalar main.cf içine, port ile ilgili kısımlar master.cf içine eklenecek.

Postfix'de Virüs ve Spam Engelleme – Postfix tarafı

- AMaViS için, main.cf içine::

```
content_filter = smtp-amavis:  
[127.0.0.1]:10024
```

master.cf içine:

```
smtp-amavis unix - - n - 2 smtp  
-o smtp_data_done_timeout=1200  
-o smtp_send_xforward_command=yes  
-o disable_dns_lookups=yes  
-o max_use=20
```


Postfix'de virüs ve spam engelleme – Postfix tarafı

- Yine master.cf içine:

```
127.0.0.1:10025 inet n - n - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_delay_reject=no
-o smtpd_client_restrictions=permit_mynetworks,reject
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o smtpd_data_restrictions=reject_unauth_pipelining
-o smtpd_end_of_data_restrictions=
-o mynetworks=127.0.0.0/8
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o smtpd_client_connection_count_limit=0
-o smtpd_client_connection_rate_limit=0
-o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

10.02.2010

Muğla

Akademik Bilişim 2010



Postfix'de Virüs ve Spam Engelleme – Postfix tarafı

Postgrey için, main.cf içine:

- smtpd_recipient_restrictions =
 permit_mynetworks,
 permit_sasl_authenticated,
 reject_unauth_destination,
 reject_invalid_hostname,
 reject_unauth_pipelining,
 reject_non_fqdn_sender,
 reject_unknown_sender_domain,
 reject_non_fqdn_recipient,
 reject_unknown_recipient_domain,
 check_policy_service inet:127.0.0.1:60000,
 permit

Eklenebilecek diğ̈er Postfix parametreleri

- smtpd_helo_required = yes
- disable_vrfy_command = yes

Postfix ile virüs ve spam engelleme

- Bu kadar mı?
- Değil!
- <http://seminer.linux.org.tr/seminer-notlari/postfix-virus-spam.sxi> adresinde güzel bir sunum var.
- Özellikle body ve header check kısımları okunmalı.
- Ayrıca SpamAssassin ile ilgili belgeler takip edilebilir.

Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Greylisting

- Etkili bir spam engelleme yöntemi
- <http://en.wikipedia.org/wiki/Greylisting>
- E-postaların iletimini gerekli koşullar sağlandığında geciktirme.
- Greylisting çalışma mantığı

10.02.2010
Muğla

Akademik Bilişim 2010



Greylisting: Postgrey

- Postgrey, postfix için bir greylisting yazılımı.
- <http://postgrey.schweikert.ch/>
- /etc/sysconfig/postgrey ya da /etc/default/postgrey ile basitçe ayarlanabilir:,

Greylisting: Postgrey

- `OPTIONS="--inet=127.0.0.1:60000 --whitelist-clients=/etc/postfix/postgrey_whitelist_clients --whitelist-recipients=/etc/postfix/postgrey_whitelist_recipients --delay=300"`
- `POSTGREY_TEXT="Greylisting for %r in action, please retry after %s seconds."`
- Whitelist kavramı

Greylisting: Postgrey

- Whitelist kavramı

10.02.2010
Muğla

Akademik Bilişim 2010



Kurumsal bir e-posta sunucusu örneđi

- Őu anda 42600 kullanıcısı olan bir sunucuda bu seminerde anlatılan bileŐenler kullanılıyor.
- Dakikada bazen 3000 e-posta iŐleniyor.
- ProLiant DL585 G1 üzerinde 1 Quad Core AMD Opteron 850 ve 4 GB ram ile alıŐıyor.
- 2 CPU genel olarak yeterli oluyor :-)

10.02.2010
Muđla

Akademik BiliŐim 2010



Peki adres defteri?

- Çözümler var. Ancak “tak çalıştır” çözüm istiyorsanız Zimbra'yı deneyebilirsiniz.
- Ücretsiz sürümü çok geniş özelliklere sahip.
- Outlook ve Blackberry için de destek.
- Ajax tabanlı bir web arabirimi.
- Arka planda Postfix, Amavis ve ClamAV var :-)
- <http://www.zimbra.com>

10.02.2010
Muğla

Akademik Bilişim 2010



Ajanda

1. Postfix hakkında kısa bir bilgi
2. Postfix kurulumu
3. Postfix'in temel yapılandırması
4. Postfix ile virüs ve spam engelleme
5. Greylisting kavramı ve Postgrey
6. Log analizi

10.02.2010
Muğla

Akademik Bilişim 2010



Log analizi

- pgflogsumm
- awstats
- Isoqlog
- mailgraph
- ...

10.02.2010
Muğla

Akademik Bilişim 2010



Bonus konu: backup mx

- Ana e-posta sunucusu çalışmayı durdurduğunda e-postaları geçici bir süre için başka bir sunucuda bekletebilirsiniz.
- Buna backup MX denir.

Bonus konu: backup MX

- MX sunucusundaki main.cf:
smtpd_recipient_restrictions içinde
permit_mynetworks ve
reject_unauth_destination olmalı.
- *relay_domains = \$mydestination,*
gunduz.org
- *relay_recipient_maps =*

Bonus konu: backup mx

- gunduz.org aŝađıdaki parametreler iinde olmamalı:
 - mydestination
 - virtual_alias_domains
 - virtual_mailbox_domains

Sorular

Sorular?

10.02.2010
Muğla

Akademik Bilişim 2010



Postfix ile E-Posta Sistemi

Devrim GÜNDÜZ

PostgreSQL Geliştiricisi

Red Hat Certified Engineer

devrim@gunduz.org

devrim.gunduz@linux.org.tr

10.02.2010

Muğla

Akademik Bilişim 2010

