

نصب RoundcubeWebmail به همراه Postfix/Devocot

معرفی و بررسی نحوه نصب و راه اندازی نرم افزار متن باز Roundcube به ما این امکان را می دهد با یکی از متداول ترین راهکارهای ارایه سرویس های ایمیل آشنا شده و امکانات و نحوه پیاده سازی آن را جزئی تر بررسی نماییم و به مقایسه محدودیت های این سرویس با دیگر سرویس های توزیع شده با ظرفیت سرویس دهی عمومی بالا در حوزه پست الکترونیک می پردازیم.

نرم افزار متن باز RoundCube:

Roundcube نرم افزار Open Source و رایگان است که برای ارایه سرویس Webmail در حوزه پست الکترونیک بکار می رود. این نرم افزار بر اساس زبان PHP توسعه یافته است و لایسنس آن بصورت General Public License (GPL) می باشد و اولین نسخه آن در سال ۲۰۰۸ عرضه شده است.

وجه تمایز RundeCube بانرم افزارهای دیگر، تحت وب بودن سمت سرویس گیرنده و سادگی آن است که دارای پلاگین های متعدد نیز می باشد.

این نرم افزار در تعداد زیادی از دانشگاه های دنیا با شمار قابل توجهی Account، نصب شده است که می توان از موارد ذیل نام برد:

- دانشگاه پنسیلوانیا
- دانشگاه فلوریدا
- دانشگاه هاروارد
- دانشگاه یوتا
- دانشگاه کمبریج
- انیستیتو تکنولوژی هند
- دانشگاه میشیگان

از قابلیت های شاخص این نرم افزار می توان به موارد ذیل اشاره نمود:

- ✓ واسط کاربر همانند برنامه های دسکتاپی.
- ✓ پشتیبانی از ۷۰ زبان دنیا.
- ✓ پشتیبانی کامل از پیام های MIME و HTML.
- ✓ حفاظت از حریم خصوصی پیشرفته.
- ✓ الحاق فایل ها به ایمیل.
- ✓ پشتیبانی از address book همراه با گروه ها و کانکتورهای LDAP.
- ✓ جستجوی ایمیل.
- ✓ امکان Import و Export.
- ✓ Drag&Drop ایمیل ها در واسط کاربری.
- ✓ نوشتن پیام هایی بصورت صفحات HTML.
- ✓ Spell checking.
- ✓ پشتیبانی از IMAP.

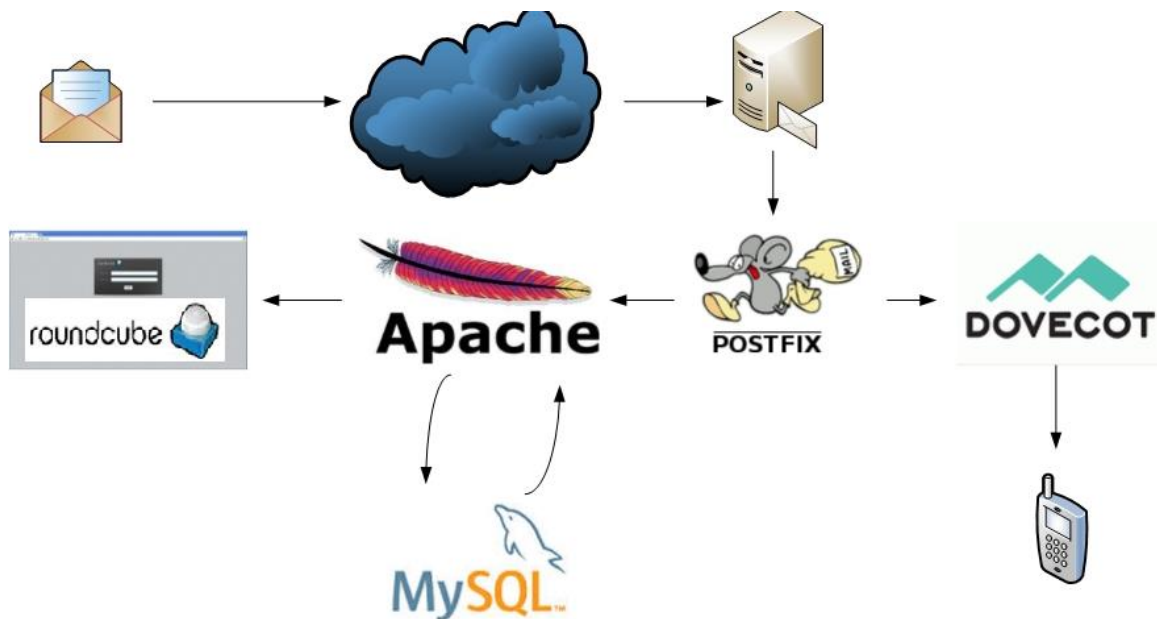
RoundCube Webmail دارای رابط زیبایی برای کاربران بوده و از بسیاری از قابلیت های Ajax در این زمینه

استفاده می کند.

پیاده سازی سرویس ایمیل متن باز مبتنی بر RoundCube بصورت ماژولار بوده و نصب هر بخش آن در سرویس

ایمیل بصورت جداگانه صورت می گیرد. که شامل موارد ذیل می باشد:

- سرویس SMTP : در این بخش نرم افزار Postfix به کار گرفته می شود.
- سرویس IMAP/POP: در این بخش نرم افزار Devocot به کار گرفته می شود.
- سرویس آنتی اسپم: در این بخش نرم افزار spamassassin به کار گرفته می شود.
- سرویس Web Server، PHP و Mysql: در این بخش مجموعه نرم افزار LAMP به کار گرفته می شود.
- رابط کاربری : در این بخش Roundcube در نظر گرفته شده است.



شکل شماره ۱- ساختار نرم افزار roundcube

نصب و راه اندازی واسط های ارتباطی ایمیل

در بخش اول، واسط های ارتباطی ایمیل ، بر روی لینوکسهای خانواده Debian را بررسی و انجام می دهیم که در اینجا از نرم افزار متن باز postfix استفاده می نماییم. این واسط SMTP به همراه Dovecot که ابزاری برای سرویس imap و pop3 می باشد و MySQL که دیتا بیس اصلی سرور بوده و ابزار آنتی اسپم به نام Spam Assassin نصب می گردد.

پیش نیاز ها :

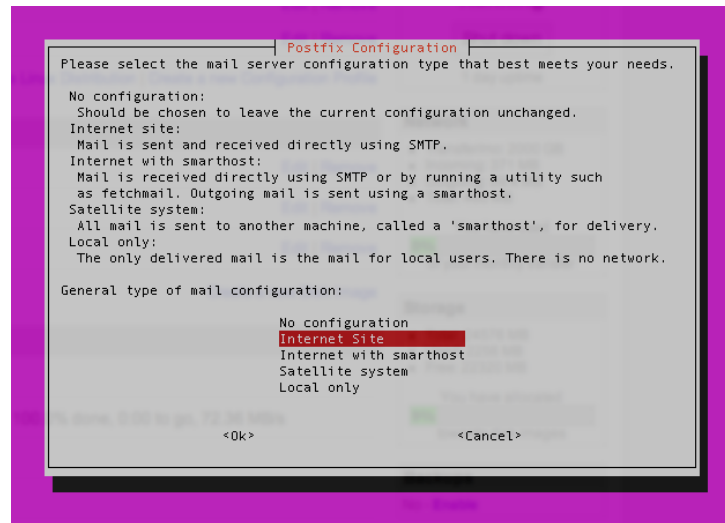
- یک آدرس دامنه پارک شده روی سرور
- نصب سرویس MySQL Server
- دسترسی Root
- استفاده از Hostname معتبر

ابتدا باید آخرین نسخه های پایدار سرویس های Postfix ، Dovecot ، MySQL و SpamAssassin را روی

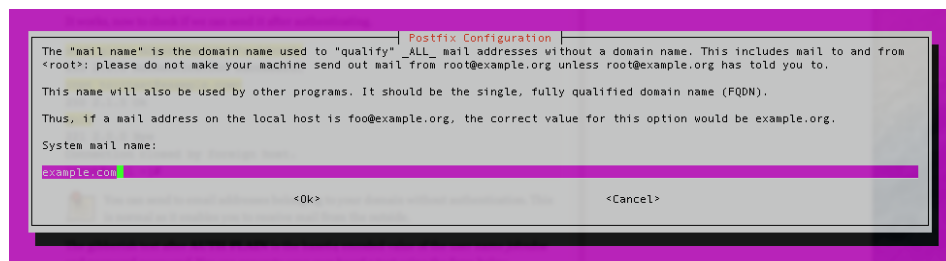
سرور لینوکس نصب کنیم :

```
apt-get install postfix postfix-mysql dovecot-core dovecot-imapd dovecot-lmtpd dovecot-mysql
```

در هنگام نصب سرویس Postfix در لینوکس Debian حتما گزینه internet Site را انتخاب می کنیم :



در ادامه نصب ، Postfix از ما نام Email را سوال می کند که دامنه ایمیل محسوب می شود که باید آن را وارد کنیم:



ساخت یک دیتابیس در MySQL ، User و ساخت Virtual Domain

توجه : این قسمت در بخش نصب و راه اندازی Roundcube به همراه دیتا بیس اصلی توضیح داده خواهد شد. اما در اینجا فقط برای مثال و اطمینان از تنظیمات درست postfix از یک دیتا بیس و دامنه و user تستی استفاده می نمایم:

ابتدا یک دیتابیس MySQL ساخته و ۳ جدول در آن ایجاد می کنیم . یکی برای حساب های کاربری، یکی برای دامنه ها و دیگری برای alias ها

```
mysqladmin -p create servermail
```

```
mysql -u root -p
```

```
mysql<
```

```
mysql > GRANT SELECT ON servermail.* TO 'usermail'@'127.0.0.1' IDENTIFIED BY 'mailpassword';
```

```
mysql > FLUSH PRIVILEGES;
```

```
mysql> USE servermail;
```

```
CREATE TABLE virtual_domains
```

```
id INT NOT NULL AUTO_INCREMENT,
```

```
name VARCHAR(50) NOT NULL,
```

```
PRIMARY KEY (id,
```

```
(ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```
CREATE TABLE virtual_users
```

```
id INT NOT NULL AUTO_INCREMENT,
```

```
domain_id INT NOT NULL,
```

```
password VARCHAR(106) NOT NULL,
```

```
email VARCHAR(120) NOT NULL,
```

```
PRIMARY KEY (id,
```

```
UNIQUE KEY email (email,
```

```
FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
```

```
(ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

```
CREATE TABLE virtual_aliases
```

```
id INT NOT NULL AUTO_INCREMENT,
```

```
domain_id INT NOT NULL,
```

```
source varchar(100) NOT NULL,
```

```
destination varchar(100) NOT NULL,
```

```
PRIMARY KEY (id,
```

```
FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
```

```
(ENGINE=InnoDB DEFAULT CHARSET=utf8
```

بعد از ساخت دیتابیس و جداول مربوط به آن، مرحله بعدی، وارد کردن اطلاعات مورد نظر به دیتابیس است. ابتدا دامنه

های مورد نظر خود را داخل جدول Virtual Domains مربوط به دیتابیس ساخته شده وارد می نمایم.

```
INSERT INTO servermail.virtual_domains
```

```
(id ,name)
```

```
VALUES
```

```
.(?example.com','\')
```

```
;'hostname.example.com','')
```

در مرحله بعدی، اطلاعات مربوط به آدرس های ایمیل و کلمات عبور مربوط به هر آدرس را داخل جدول virtual_users وارد می کنیم .

```
INSERT INTO servermail.virtual_users
```

```
(id, domain_id, password , email(
```

```
VALUES
```

```
,'','')ENCRYPT('firstpassword', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))),
```

```
'email1@example.com,('
```

```
,'','')ENCRYPT('secondpassword', CONCAT('$6$', SUBSTRING(SHA(RAND()), -
```

```
16))), 'email2@example.com,('
```

و سر انجام alias های مربوط به هر آدرس ایمیل که عموماً برای ایجاد Email Forwarder استفاده می شوند را

داخل جدول virtual_aliases وارد میکنیم :

```
INSERT INTO servermail.virtual_aliases
```

```
(id, domain_id, source, destination(
```

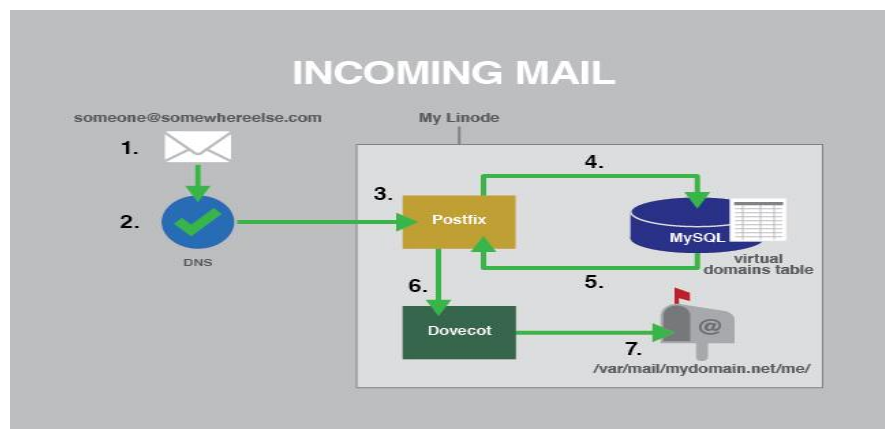
```
VALUES
```

```
,'','')alias@example.com', 'email1@example.com;('
```

و به کمک دستور زیر از MySQL خارج میشویم :

```
mysql > exit
```

شکل زیر مراحل کار را نشان میدهد:



شکل شماره ۲- ساختار ورود می‌ل به نرم افزار نمونه

تنظیمات واسط ارتباطی SMTP

در این مرحله با تنظیمات سرویس Postfix امکان برقراری اتصالات کانکشن های SMTP و همچنین ارسال پیام و ایمیل برای تمامی User های ساخته شده در دیتابیس Mail Server فراهم می گردد .
ابتدا نیاز است که یک کپی از فایل پیش فرض بسازیم:

```
cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
```

سپس مسیر فایل main.cf را تغییر داده و این فایل را ویرایش می کنیم :

```
cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
```

```
nano /etc/postfix/main.cf
```

و مقادیر آن را به شکل زیر تغییر می دهیم .در اینجا از ssl certificate رایگان استفاده می کنیم ولی در پروژه اصلی

می توانیم تنظیمات لازمه در این زمینه را انجام دهیم:

```
TLS parameters #
```

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem#
```

```
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key#
```

```
smtpd_use_tls=yes#
```

```
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache#
```

```
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache#
```

```
smtpd_tls_cert_file=/etc/ssl/certs/dovecot.pem
```

```
smtpd_tls_key_file=/etc/ssl/private/dovecot.pem
```

```
smtpd_use_tls=yes
```

```
smtpd_tls_auth_only = yes
```

تنظیمات TLS :

```
smtpd_sasl_type = dovecot
```

```
smtpd_sasl_path = private/auth
```

```
smtpd_sasl_auth_enable = yes
```

```
= smtpd_recipient_restrictions
```

```
.permit_sasl_authenticated
```

```
.permit_mynetworks
```

```
reject_unauth_destination
```

تنظیمات زیر را بر اساس مثال تکمیل می نماییم .

توجه باید کرد این تغییر به ما اجازه می دهد که سرور ما از virtual domain ها درون جداول MySQL استفاده

نماید.

```
mydestination = example.com, hostname.example.com, localhost.example.com, localhost#
```

تنظیمات Hostname این بخش نیز بهتر است در موقع نصب Roundcube نیز تنظیم گردد:

```
mydestination = localhost
```

برای تحویل ایمیل های local به لیست دامنه های مجازی در جداول MySQL تنظیم زیر را وارد کنید:

```
virtual_transport = lmtp:unix:private/dovecot-lmtp
```

```
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
```

```
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
```

```
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf
```

در مرحله بعدی یک فایل به نام mysql-virtual-mailbox-domaincs.cf ایجاد کرده و مطابق زیر آن را ویرایش

می نماییم :

```
vi /etc/postfix/mysql-virtual-mailbox-domains.cf
user = usermail
password = mailpassword
hosts = 127.0.0.1
dbname = servermail
'query = SELECT 1 FROM virtual_domains WHERE name='%s
```

و سر انجام سرویس Postfix را ریست می کنیم :

```
service postfix restart
```

حالا تست میکنیم تا اطمینان حاصل شود، سرویس Postfix دامنه مورد نظر را پیدا کرده و به درستی با جدول دامنه ها در دیتابیس ایمیل ها ارتباط برقرار می کند و یا خیر . خروجی دستور زیر در صورت عدم وجود مشکل در پیکربندی Posftix عدد ۱ خواهد بود.

نکته مهم: البته این کار را بعد از تنظیمات دامنه در مراحل نصب Roundcube نیز می توانیم انجام دهیم.

```
ostmap -q example.com mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
```

حالا فایلی به نام mysql-virtual-mailbox-maps.cf ایجاد کرده و به شکل زیر آن را ویرایش می نماییم :

```
vi /etc/postfix/mysql-virtual-mailbox-maps.cf
user = usermail
password = mailpassword
hosts = 127.0.0.1
dbname = servermail
'query = SELECT 1 FROM virtual_users WHERE email='%s
```

و مجددا postfix را ریستارت میکنیم :

```
service postfix restart
```

و مجددا جهت اطمینان از دسترسی Postfix این بار به اطلاعات مربوط به آدرس ایمیل ها در جدول مربوطه، دستور زیر را وارد می کنیم :

```
postmap -q email1@example.com mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
```

آخرین فایل مربوط به ایجاد کانکشن بین Postfix و MySQL است :

```
vi /etc/postfix/mysql-virtual-alias-maps.cf
```

```
user = usermail
```

```
password = mailpassword
```

```
hosts = 127.0.0.1
```

```
dbname = servermail
```

```
query = SELECT destination FROM virtual_aliases WHERE source='%s'
```

```
}
```

و ریستارت کردن سرویس Postfix :

```
service postfix restart
```

خروجی دستور زیر در محیط ssh درواقع forwarder های مربوط به alias مورد نظر را به شما نشان خواهد داد :

```
postmap -q alias@example.com mysql:/etc/postfix/mysql-virtual-alias-maps.cf
```

تنظیمات Dovecot

قبل از آغاز کانفیگ سرویس Dovecot در لینوکس و محیط ssh دستورات زیر را اجرا میکنیم :

```
cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.orig
```

```
cp /etc/dovecot/conf.d/10-mail.conf /etc/dovecot/conf.d/10-mail.conf.orig
```

```
cp /etc/dovecot/conf.d/10-auth.conf /etc/dovecot/conf.d/10-auth.conf.orig
```

```
cp /etc/dovecot/dovecot-sql.conf.ext /etc/dovecot/dovecot-sql.conf.ext.orig
```

```
cp /etc/dovecot/conf.d/10-master.conf /etc/dovecot/conf.d/10-master.conf.orig
```

```
cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-ssl.conf.orig
```

حالا فایل پیکربندی dovecot را ویرایش میکنیم :

```
Nano /etc/dovecot/dovecot.conf
```

و خط زیر را اصطلاحاً uncomment میکنیم:

```
include conf.d/*.conf!
```

و تغییرات زیر را در فایل dovecot.conf اعمال کرده و فایل را ذخیره میکنیم:

```
include_try /usr/share/dovecot/protocols.d/*.protocol!
```

```
protocols = imap lmtp
```

در مرحله بعدی فایل مربوط به تنظیمات ایمیل را ویرایش میکنیم:

```
nano /etc/dovecot/conf.d/10-mail.conf
```

خط mail_location را پیدا کرده، آن را uncomment میکنیم و پارامترهای زیر را به آن اضافه میکنیم:

```
mail_location = maildir:/var/mail/vhosts/%d/%n
```

حالا خط mail_privileged_group پیدا کرده و آن را به این شکل تغییر می دهیم:

```
mail_privileged_group = mail
```

بررسی دسترسی ها و مجوزها

خروجی دستور ls -ld /var/mail باید مشابه ذیل باشد:

```
drwxrwsr-x 3 root vmail 4096 Jan 24 21:23 /var/mail
```

حالا به ازای هر دامنه ای که در دیتابیس اضافه کرده ایم یک پوشه در مسیر زیر می سازیم:

```
mkdir -p /var/mail/vhosts/example.com
```

حالا یک گروه و نام کاربری جدید ساخته و مالکیت پوشه var/mail را به آن تغییر میدهیم:

```
groupadd -g 5000 vmail
```

```
useradd -g vmail -u 5000 vmail -d /var/mail
```

```
chown -R vmail:vmail /var/mail
```

حال فایل زیر را ویرایش می کنیم :

```
nano /etc/dovecot/conf.d/10-auth.conf
```

و مقادیر آن را به شکل زیر تغییر می دهیم :

```
disable_plaintext_auth = yes
```

```
auth_mechanisms = plain login
```

```
include auth-system.conf.ext!
```

```
include auth-sql.conf.ext!
```

در ادامه مراحل کانفیگ Mail Server یک فایل جدید ایجاد کرده و به این صورت ویرایش میکنیم :

```
nano /etc/dovecot/conf.d/auth-sql.conf.ext
```

```
} passdb
```

```
driver = sql
```

```
args = /etc/dovecot/dovecot-sql.conf.ext
```

```
{
```

```
} userdb
```

```
driver = static
```

```
args = uid=vmail gid=vmail home=/var/mail/vhosts/%d/%n
```

```
{
```

ویرایش این فایل و انجام تغییرات و ذخیره تغییرات :

```
nano /etc/dovecot/dovecot-sql.conf.ext
```

```
driver = mysql
```

```
connect = host=127.0.0.1 dbname=servermail user=usermail password=mailpassword
```

```
default_pass_scheme = SHA512-CRYPT
```

```
;password_query = SELECT email as user, password FROM virtual_users WHERE email='%u
```

حالا مالکیت های مربوط به پوشه dovecot را نیز تغییر میدهیم :

```
chown -R vmail:dovecot /etc/dovecot
```

```
chmod -R o-rwx /etc/dovecot
```

در ادامه فایل `etc/dovecot/conf.d/10-master.conf` را باز کرده و به این صورت ویرایش میکنیم :

```
nano /etc/dovecot/conf.d/10-master.conf
```

```
Uncomment inet_listener_imap and modify to port 0###
```

```
} service imap-login
```

```
} inet_listener imap
```

```
port = 0
```

```
{
```

```
Create LMTP socket and this configurations#
```

```
} service lmtp
```

```
} unix_listener /var/spool/postfix/private/dovecot-lmtp
```

```
mode = 0600
```

```
user = postfix
```

```
group = postfix
```

```
{
```

```
} inet_listener lmtp#
```

```
Avoid making LMTP visible for the entire internet #
```

```
= address#
```

```
= port#
```

```
{#
```

```
{
```

```
} service auth
```

```
} unix_listener /var/spool/postfix/private/auth
```

```
mode = 0666
```

```
user = postfix
```

```

group = postfix
{
} unix_listener auth-userdb
mode = 0600
user = vmail
= group#
{
} unix_listener /var/spool/postfix/private/auth#
mode = 0666 #
{#
user = dovecot
{
} service auth-worker
Auth worker process is run as root by default, so that it can access #
etc/shadow. If this isn't necessary, the user should be changed to/ #
.default_internal_user$ #
user = vmail
{

```

سرویس dovecot را ریستارت میکنیم :

```
service dovecot restart
```

در ادامه به تنظیمات Antispam برای postfix میپردازیم.

تنظیمات SpamAssassin برای Postfix

در عملیات دریافت ایمیل ابزار spamassassin بین دنیای بیرون و سرویس های ایمیل روی سرور ها قرار خواهد گرفت اگر این ابزار مطابق با سیاست ها و تنظیمات تعریف شده خودش بفهمد که یک پیام ورودی در حقیقت یک spam است خط subject را به گونه ای که کاملاً مشخص باشد تغییر خواهد داد.

در صورت نصب نبودن برنامه از طریق دستور زیر آن را نصب می کنیم:

```
yum install spamassassin
```

فایل کانفیگ اصلی، فایل `etc/mail/spamassassin/local.cf` میباشد و باید مطمئن شویم که آپشن های زیر

موجود باشند. (اگر وجود نداشتند آنها را اضافه می کنیم و یا در صورت نیاز اگر کامنت بودند از کامنت بیرون می آوریم):

```
report_safe 0
```

```
required_score 8.0
```

```
rewrite_header Subject [SPAM]
```

زمانی که `report_safe` برابر با ۰ تنظیم شده باشد (مقدار توصیه شده)، اسپم ورودی تنها با تغییر هدر های ایمیل و

با توجه به `rewrite_header` تغییر خواهد کرد اگر مقدار آن برابر با ۱ باشد پیام کلاً حذف خواهد شد.

برای تعریف میزان حساسیت `spam filter` (فیلتر اسپم) از آپشن `required_score` استفاده می شود که به همراه

آن از یک عدد `integer` یا `decimal` می آید. هرچه این عدد کوچکتر باشد حساسیت فیلتر بالاتر میرود. تعریف یک مقدار

مابین ۸,۰ و ۱۰,۰ برای یکی سیستم بزرگ که تعداد زیادی `Account` ایمیل دارد توصیه میشود. بعد از ذخیره این تغییرات

سرویس `spam filter` را فعال و استارت میکنیم و سپس `Rule` های اسپم را آپدیت می نماییم :

```
systemctl enable spamassassin
```

```
systemctl start spamassassin
```

```
sa-update
```

برقراری ارتباط و SpamAssassin

به منظور برقراری ارتباط موثر `postfix` و `spamassassin` ما نیاز داریم تا یک `user` و گروه اختصاصی برای اجرای

سرویس `spam filter` ایجاد کنیم :

```
useradd spamd -s /bin/false -d /var/log/spamassassi
```

سپس خط زیر را در پایان فایل `etc/postfix/master.cf` اضافه می کنیم :

```
spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc -e  
/usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

و در نهایت باید مشخص کنیم که spam assassin به عنوان content_filter عمل خواهد کرد :

```
o content_filter=spamassassin
```

```
# Postfix master process configuration file. For details on the format  
# of the file, see the master(5) manual page (command: "man 5 master").  
#  
# Do not forget to execute "postfix reload" after editing this file.  
#  
# =====  
# service type private unpriv chroot wakeup maxproc command + args  
#          (yes)   (yes)   (yes)   (never) (100)  
# =====  
smtp      inet  n       -       n       -       -       smtpd -o content_filter=spamassassin  
#smtp     inet  n       -       n       -       1       postscreen  
#smtpd    pass  -       -       n       -       -       smtpd
```

نهایتاً برای اعمال تغییرات postfix را ریستارت می کنیم :

```
systemctl restart postfix
```

تست صحت عملکرد

برای بررسی اینکه آیا spam assassin به درستی کار میکند و اسپم های ورودی را تشخیص می دهد تستی با عنوان GTUBE یا Generic Test for Unsolicited Bulk EMAIL موجود است.

برای اجرای این تست یک ایمیل از دامین خارج از شبکه (مانند Yahoo , Hotmail و یا Gamil) به یک اکانت موجود در ایمیل سرور ارسال می کنیم. subject را به دلخواه تعریف کرده و در متن ایمیل از پیغام زیر استفاده می کنیم :

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

و لاگ های مربوطه هشدار spam را نمایش می دهند :

```
journalctl | grep spam
```

```
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: prefork: child status: 11
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: spamd: connection from TecMint-VPS [::1]:41721
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: spamd: setuid to spamd succeeded
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: spamd: creating default_prefs: /var/log/spamassassin/
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: config: created user preferences file: /var/log/spamassassin/
Nov 05 18:40:04 mail.linuxnewz.com spamd[1199]: spamd: processing message <CAG0nFRL9xCasMBW-2f
Nov 05 18:40:10 mail.linuxnewz.com spamd[1199]: spamd: identified spam (1002.3/8.0) for spamd:
Nov 05 18:40:10 mail.linuxnewz.com spamd[1199]: spamd: result: Y 1002 - DKIM_SIGNED,DKIM_VALID,URIBL_BLOCKED scantime=6.2,size=2994,user=spamd,uid=5001,required_score=8.0,rhost=TecMint-V
+Fcwow0@mail.gmail.com> autolearn=no autolearn_force=no
```

همانطور که در تصویر بالا می بینیم این پیغام یک spam score برابر با ۱۰۰۲٫۳ دارد. علاوه بر این ما میتوانیم

spam assassin را مستقیماً از طریق command line تست کنیم :

```
spamassassin -D </usr/share/doc/spamassassin-3.4.0/sample-spam.txt
```

دستور فوق یکسری خروجی نمایش خواهد داد که شامل موارد زیر است:

```
pr1_300: 70 (34.6%)
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on mail.linuxnewz.com
X-Spam-Flag: YES
X-Spam-Level: *****
X-Spam-Status: Yes, score=1000.0 required=8.0 tests=GTUBE,NO_RECEIVED,
NO_RELAYS autolearn=no autolearn_force=no version=3.4.0
X-Spam-Report:
* -0.0 NO_RELAYS Informational: message was not relayed via SMTP
* 1000 GTUBE BODY: Generic Test for Unsolicited Bulk Email
* -0.0 NO_RECEIVED Informational: message has no Received headers
Subject: [SPAM] Test spam mail (GTUBE)
Message-ID: <GTUBE1.1010101@example.net>
```

نصب و راه اندازی RoundCube WebMail

در این پیاده سازی حساب های کاربری ایمیل و Alias ها در دیتابیس MySQL ذخیره می گردد و برای تسهیل تنظیمات آن می توان از Phpmyadmin استفاده کنیم. همچنین می توان از طریق اجرای دستورات بصورت CLI این تنظیمات را انجام داد.

قبل از نصب سرویس ابتدا می بایست یک پکیج به منظور دسترسی به آخرین پکیج های مورد نیاز در اینترنت نصب نمود. این پکیج امکان اتصال به Repository جدید را فراهم می سازد. برای این کار دستور زیر را وارد میکنیم.

Apt-get install epel-release

برای ارایه سرویس ایمیل در حوزه اینترنت داشتن ملزومات زیر در حوزه DNS الزامی است:

- A-record که به IP سرور اشاره دارد
- Mx-record که به Hostname سرور ایمیل اشاره دارد
- یک Hostame به شکل FQDN
- یک دامنه معتبر برای Resolve نمودن نام آن
- یک IP معتبر اینترنتی

(پس از فراهم نمودن رکوردهای DNS و IP می توان با ابزارهای DNS Client مانند MxToolbox درستی آنها را چک نمود).

قبل از نصب RoundCube Webmail باید یک Web Server نصب گردد.

لذا (Apache, PHP, MySQL) که LAMP server نامیده می شوند توسط دستور زیر نصب می گردد:

```
sudo apt-get install lamp-server^
```

پس از اتمام نصب LAMP Server ، می توانیم کار نصب RoundCube Webmail را شروع کنیم . البته

mysql در موقع نصب postfix نصب شده است.

ساخت Database & User در MySQL

یک ترمینال باز کرده و دستور زیر را برای ورود به MySQL Server وارد می کنیم (رمز عبور MySQL همان است

که در حین نصب LAMP Server وارد می کنیم)

```
mysql -u root -p
```

سپس دیتا بیس را برای RoundCube Webmail می سازیم که در مورد قبلی ساختیم و در صورت ساخته نشدن

```
create database roundcubedb;
```

دوباره می سازیم:

ساخت نام کاربری از نوع Administrator در Mysql از RoundCube Webmail:

```
create user adminmail;
```

حال رمز عبور را برای نام کاربری فوق بطور مثال admin123 می دهیم:

```
set password for 'adminmail' = password('admin123');
```

نام دیتا بیسی که ساختیم roundcubedb می باشد لذا با دستور زیر Priviledge نام کاربری ساخته شده

adminmail را به این دیتا بیس می دهیم:

```
grant all privileges on roundcubedb.* to adminmail@localhost
```

حالا با دستور زیر از MySQL Server خارج می شویم:

```
FLUSH PRIVILEGES;  
exit
```

نصب RoundCube Webmail

در مثال ما ، مسیر نصب var/www/webmail/ می باشد. لذا پس از دانلود RoundCube Webmail ، آن

را در مسیر var/www/webmail باید Extract کنیم. دستور انجام کار بصورت زیر است:

```
cd /tmp && wget http://sourceforge.net/projects/roundcubemail/files  
/roundcubemail/1.0.5/roundcubemail-1.0.5.tar.gz/download  
sudo tar -xzf roundcubemail-1.0.5.tar.gz -C /var/www  
sudo mv /var/www/roundcubemail-1.0.5/ /var/www/webmail
```

حالا مسیر `var/www/webmail` را برای user و Group به نام `www-data` (`www-data` نام کاربری

و گروه web server می باشد) را `change ownership` می کنیم:

```
sudo chown -R www-data:www-data /var/www/webmail/*  
sudo chown -R www-data:www-data /var/www/webmail/
```

حالا دیتا بیس RoundCube را در MySQL Server باید import کنیم که توسط دستور زیر ابتدا به MySQL

login، کرده و سیس، کار را انجام م، دهیم:

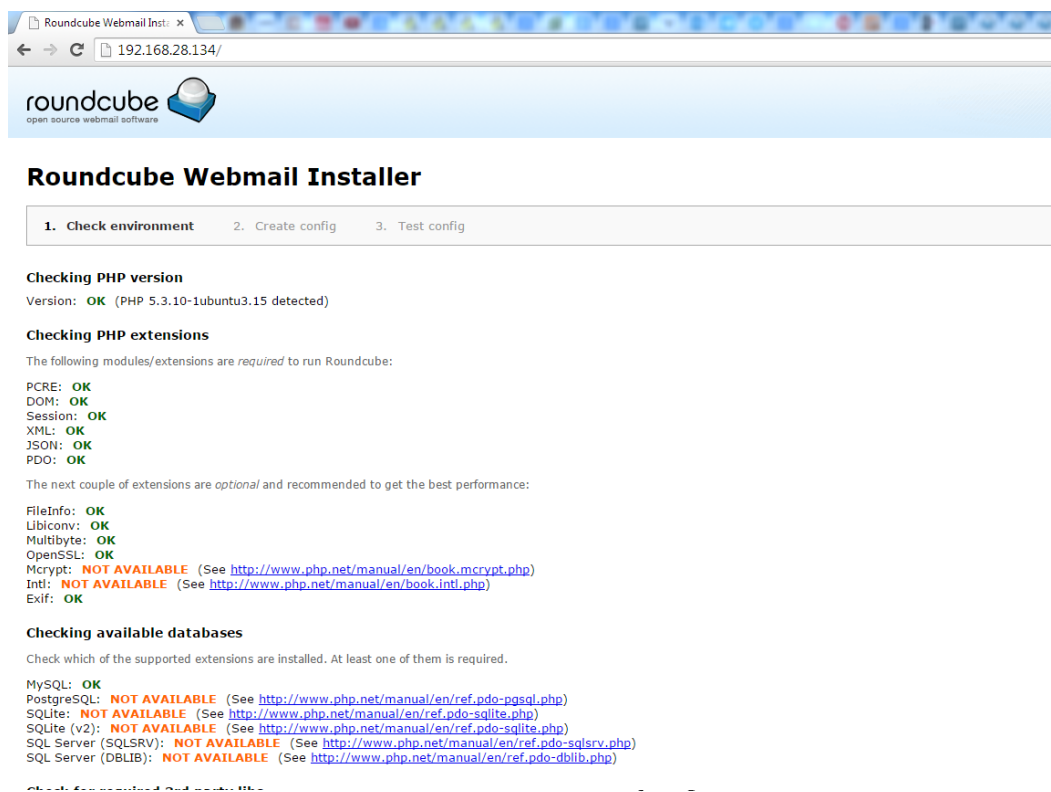
```
mysql -u root -p roundcubedb < /var/www/webmail/SQL/mysql.initial.sql
```

برای شروع نصب Roundcube باید یکی از دو Browser های Chrome و با Firefox را باز کرده و آدرس

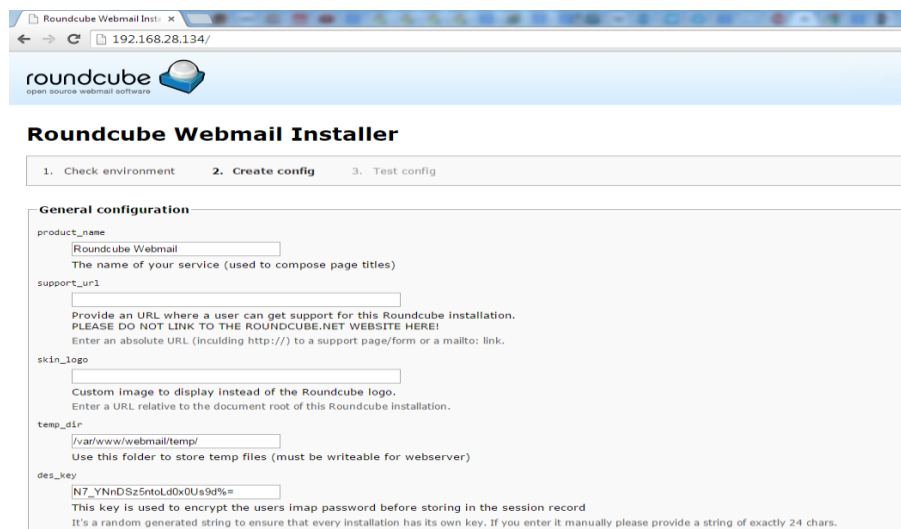
```
http://server-ipaddress/webmail/installer/
```

زیر را در آن وارد می کنیم :

پس از باز شدن همانند تصویر زیر ، کنسول را مشاهده می کنیم:



اگر همانند تصویر بالا تمامی موارد مورد نیاز ، نصب شده اند دکمه continue را برای ورود به مرحله بعد می زنیم:

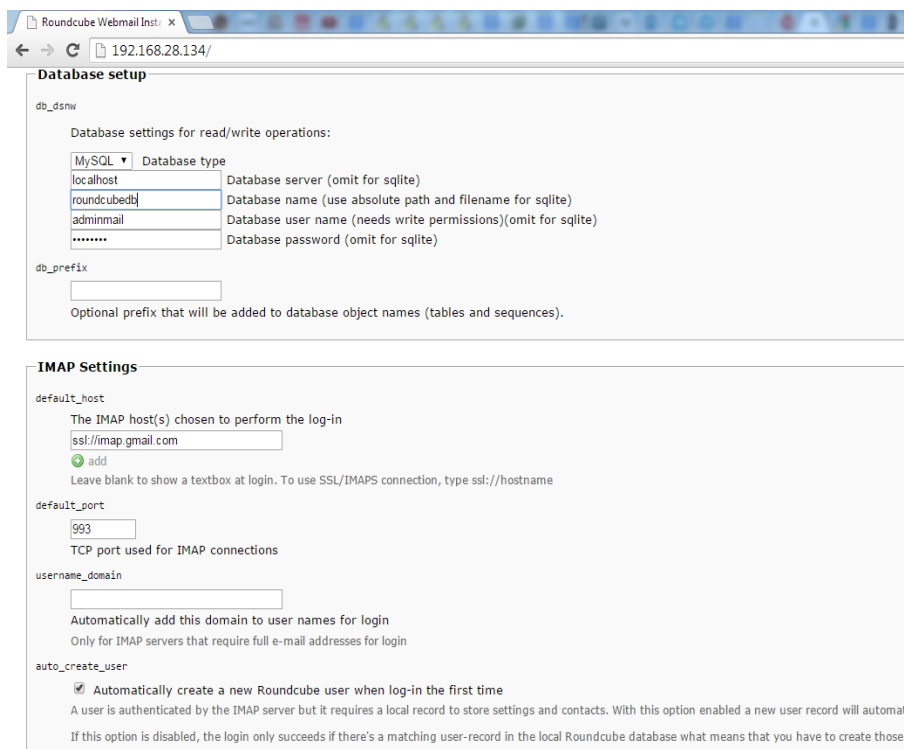


The screenshot shows the Roundcube Webmail Installer interface in a web browser. The browser's address bar displays '192.168.28.134/'. The page header includes the Roundcube logo and the text 'open source webmail software'. Below the header, the title 'Roundcube Webmail Installer' is centered. A progress bar at the top indicates three steps: '1. Check environment', '2. Create config' (which is currently active), and '3. Test config'. The main content area is titled 'General configuration' and contains several input fields and instructions:

- product_name**: A text box containing 'Roundcube Webmail'. Below it, a note states: 'The name of your service (used to compose page titles)'.
- support_url**: A text box. Below it, instructions read: 'Provide an URL where a user can get support for this Roundcube installation. PLEASE DO NOT LINK TO THE ROUNDcube.NET WEBSITE HERE! Enter an absolute URL (including http://) to a support page/form or a mailto: link.'
- skin_logo**: A text box. Below it, instructions read: 'Custom image to display instead of the Roundcube logo. Enter a URL relative to the document root of this Roundcube installation.'
- temp_dir**: A text box containing '/var/www/webmail/temp/'. Below it, a note states: 'Use this folder to store temp files (must be writeable for webserver)'.
- des_key**: A text box containing 'N7_YNnDSz5ntoLd0x0Us9d%='. Below it, instructions read: 'This key is used to encrypt the users imap password before storing in the session record. It's a random generated string to ensure that every installation has its own key. If you enter it manually please provide a string of exactly 24 chars.'

شکل شماره ۴- نصب RoundCube Webmail

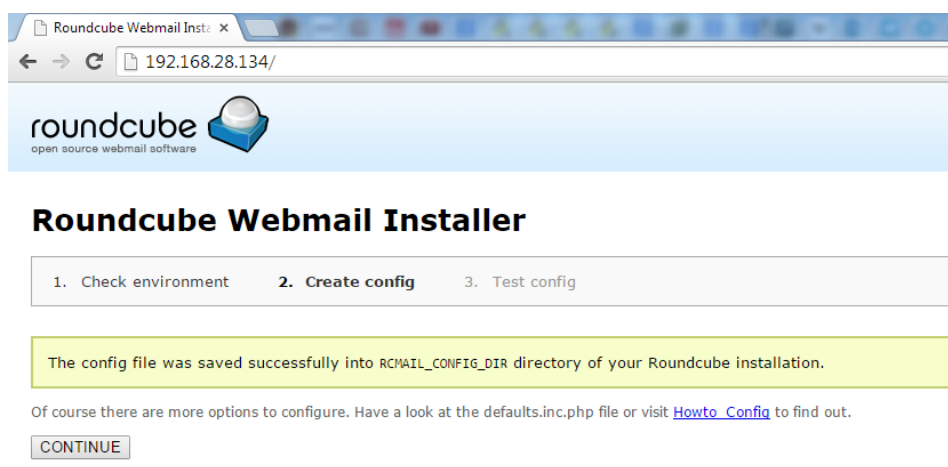
در این مرحله تنظیمات مربوط به دیتا بیسی که قبلا ساخته ایم و همان نام کاربری و رمز و همچنین نام دیتا بیسی را که ساخته شده وارد کرده و سپس تنظیمات SMTP و IMAP را انجام می دهیم.



The screenshot shows the 'Database setup' and 'IMAP Settings' sections of the Roundcube Webmail Installer. In the 'Database setup' section, the 'Database type' is set to 'MySQL', the 'Database server' is 'localhost', the 'Database name' is 'roundcubedb', the 'Database user name' is 'adminmail', and the 'Database password' is masked with dots. The 'db_prefix' is left empty. In the 'IMAP Settings' section, the 'default_host' is 'ssl://imap.gmail.com', the 'default_port' is '993', and the 'auto_create_user' checkbox is checked. The 'username_domain' is also left empty.

شکل شماره ۵- نصب RoundCube Webmail

پس از اتمام تنظیمات ، دکمه Continue را می زنیم تا کار نصب به اتمام برسد:



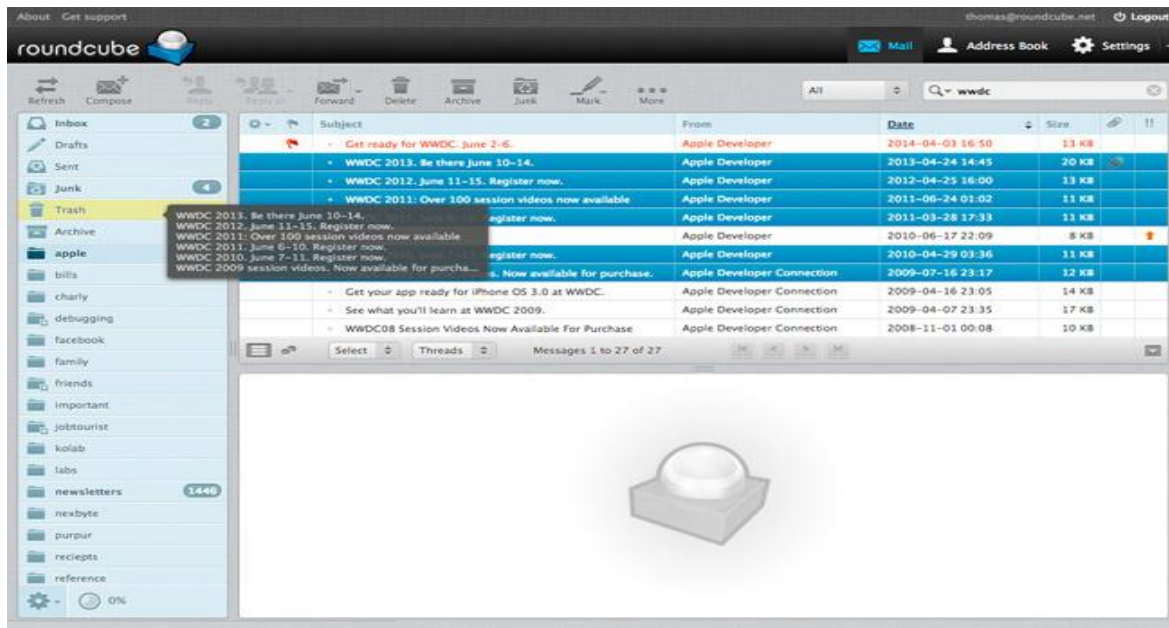
The screenshot shows the Roundcube Webmail Installer interface with a success message. The progress bar shows '2. Create config' as the current step. The message states: 'The config file was saved successfully into RCMAIL_CONFIG_DIR directory of your Roundcube installation.' Below this, it says 'Of course there are more options to configure. Have a look at the defaults.inc.php file or visit [Howto Config](#) to find out.' At the bottom, there is a 'CONTINUE' button.

شکل شماره ۶- نصب RoundCube Webmail

پس از اتمام مراحل نصب ، طبق دستور ، پوشه: `/var/www/webmail/installer/` را پاک می کنیم:

```
sudo rm -rf /var/www/webmail/installer
```

حال Roundcube Webmail آماده است .



شکل شماره ۷- نصب RoundCube Webmail

نصب سرور بصورت توزیع شده

تنظیمات پیش فرض راه اندازی Roundcube بصورت تک سرویس دهنده می باشد. اما Roundcube قابلیت اجرا در چند سرور و پشت یک Load Balancer یا Reverse Proxy جهت سرویس دادن بصورت توزیعی و performance-high را داراست . برای این منظور سرور دیتابیس را بصورت توزیع شده نصب می نماییم.

Roundcube از یک دیتابیس جهت ذخیره تنظیمات کاربران ، دفترچه مخاطبان استفاده می کند. برای بهبود کارایی ایمیل سرور می توان از یک Database سرور اصلی و اختصاصی (Master) به همراه چند سرور ثانویه (Slave) بهره برد. و به منظور ارتباط این دیتابیس ها، تنظیماتی را برای خواندن و نوشتن در دیتابیس در سرور ایجاد می کنیم . برای این منظور تنظیماتی را در پیکربندی Roundcube انجام می دهیم.

```
// PEAR database DSN for read/write operations
$config['db_dsnw'] = 'mysql://roundcube:*****@dbmasterhost/roundcubemail';

// PEAR database DSN for read only operations (if empty write database will be used)
$config['db_dsnr'] = 'mysql://roundcube:*****@localhost/roundcubemail';
```