

FUNDACION CENDITEL  
UNIDAD: DESARROLLO.  
PROYECTO: INTERFAZ CORREO PARA EL ESTADO VENEZOLANO.

## MANUAL DE INSTALACIÓN

### Introducción

Se ha realizado una exhaustiva investigación sobre el software libre presentado por la comunidades de desarrollo para la gestión del correo electrónico bajo plataformas web y móviles, seleccionando la herramienta Roundcube WebMail, en su versión más actual 1.1.3.

El presente manual indica como se instala y se conectan los siguientes servicios, en los diversos servidores: OpenLdap, para el manejo de cuentas de usuario, Postgresql para el manejo de las variables de ambiente persistentes y almacenamiento de buzones de correo, Dovecot como servidor IMAP/POP3, Exim como agente de transporte de correos (MTA), Nginx como servidor web y Roundcube como aplicación de interfaz web.

Se da por entendido que ya se encuentran los servidores instalados con el sistema operativo Debian Jessie, y que poseen una conexión via Internet Protocol de dirección fija, y que se encuentran configurados los repositorios para Debian, así como cualquier editor en consola de su preferencia, para este presente informe utilizaremos el vim como editor.

El presente manual presenta un conjunto de comando ejecutados desde una terminal del sistema, para los cuales el prompt del sistema será representado con los símbolos “\$>”, el cual varia según el caso, pero no se ilustrará en el documento por ser característica peculiar, y por medio de esta nota se indica al lector que no debe ser incluido en el comando, que comienza inmediatamente después del mismo

### Instalación

#### *Servidor Ldap*

Una vez autenticado en el sistema como súper usuario, verificamos la dirección IP asignado al servidor:

```
$>ifconfig
```

Es el listado desplegado muestra la dirección IP asignada en nuestro caso 192.168.12.117, recuerde cambiar donde aparezca dicho dirección por la mostrada en el listado anterior.

Editamos el archivo de identificadores de servidores.

```
$>vim /etc/hosts
```

Anexar la siguiente línea (en nuestro caso):

192.168.12.117 correo-ldap

Guardar los cambios del archivo y salir.

Instalamos el OpenLdap desde los repositorios

```
$>apt-get install slapd ldap-utils shellldap
```

Se realiza la reconfiguración del servicio para agregar los parámetros deseados:

```
$>dpkg-reconfigure slapd
```

Se han indicado los siguientes parámetros:

Omit OpenLDAP server configuration?

<No>

DNS domain name:

correo.cenditel

Organization name:

cenditel

Administrator Password:

qwerty

Database:

<MDB>

Do you want the database to be removed when slapd is purged?

<No>

Move old database?

<Yes>



Allow LDAPv2 protocol?

<No>

En este momento el servidor ldap está configurado y funcionando, el archivo de configuración “/etc/ldap/slapd.conf” debe contener los siguientes parametros:

```
BASE dc=correo,dc=cenditel
```

```
URI ldap://correo-ldap.cenditel
```

El directorio:

Para esta configuración se ha definido una “unidad organizacional” (ou) para ordenar los usuarios dentro de este subdirectorio.

Crear el archivo “ou.ldif” con la siguiente información:

```
dn: ou=usuarios,dc=correo,dc=cenditel
```

```
ou: usuarios
```

```
description: Directorio de Usuarios de correo.cenditel
```

```
objectClass: organizationalUnit
```

Creación de usuarios:

Crear el archivo “usuario.ldif” que será usado para generar un registro en el directorio:

```
dn: uid=usuario_uno,ou=users,dc=correo,dc=cenditel
```

```
objectClass: top
```

```
objectClass: inetOrgPerson
```

```
objectClass: person
```

```
objectClass: organizationalPerson
```

```
uid: usuario_uno
```

```
cn: Usuario Uno
```

```
mail: usuario_uno@correo.cenditel
```

```
sn: Uno
```

```
givenName: Usuario
```

Cargar los usuarios de la siguiente manera:

Se crea el directorio de configuración:

```
$>ldapadd -f ou.ldif -x -w qwerty -D cn=admin,dc=correo,dc=cenditel
```

Se crea el usuario:

```
$>ldapadd -f usuario_uno.ldif -x -w qwerty -D cn=admin,dc=correo,dc=cenditel
```

Debe agregarse la contraseña, la mejor manera de hacerlo es la siguiente:

```
$>ldappasswd -h correo-ldap.cenditel -x -w qwerty -D cn=admin,dc=correo,dc=cenditel  
uid=usuario_uno,ou=usuarios,dc=correo,dc=cenditel -s CONTRASENA
```

Puede revisarse la configuración de la siguiente manera:

```
$>ldapsearch -x
```

```
$>slapcat
```

Puede shellldap agregar:

```
$>vim ~/.shellldap.rc
```

Agregar los siguientes parámetros:

```
server: correo-ldap.cenditel  
binddn: cn=admin,dc=correo,dc=cenditel  
bindpass: qwerty  
basedn: dc=correo,dc=cenditel
```

## Servidor Web

IP: 192.168.12.181

Se instala el servicio nginx y los interpretes de php:

```
$>su apt-get install nginx
$>su apt-get install php5-common php5-dev php5-imap php5-ldap php5-pgsql php5-cgi php5-cli
$>su apt-get install php5-curl php5-xmlrpc php5-memcache php5-pspell libgv-php5 zip unzip
$>su apt-get install memcached python-software-properties php-date php5-gd php-apc php5-mcrypt
```

Se reserva el espacio para contener la aplicación:

```
$>su cd /srv
$>su mkdir public
$>su cd public
```

Descarga de software de la aplicación:

```
$>wget http://sourceforge.net/projects/roundcubemail/files/roundcubemail/1.1.3/roundcubemail-1.1.3-complete.tar.gz/download?use_mirror=ufpr
```

Mover el archivo, descomprimir y renombrar la carpeta

```
$>mv ./roundcubemail-1.1.3-complete.tar.gz /srv/public
$>cd /srv/public
$>tar zxvf roundcubemail-1.1.3-complete.tar.gz
$>mv roundcubemail-1.1.3-complete roundcube
```

Configurar el servidor web nginx

```
$>su rm -f /etc/nginx/sites-{enabled,available}/default
```

Crear un nuevo archivo de configuracion:

```
$>vim /etc/nginx/sites-available/roundcube
```

Debe quedar de la siguiente manera:

```
server {
    listen 80;
    server_name correo-web;
    return 301 https://correo-web$request_uri;
}
server {
    # llisten 80 is modified to listen 443 ssl;
    listen 443 ssl;
    server_name correo-web;
    root /srv/public/roundcube;
    index index.php index.html index.htm;
    access_log /var/log/nginx/roundcube_access.log;
    error_log /var/log/nginx/roundcube_error.log;
    location / {
        try_files $uri $uri/ /index.php?q=$uri&$args;
    }

    error_page 404 /404.html;
    error_page 500 502 503 504 /50x.html;

    location = /50x.html {
        root /usr/share/nginx/html;
    }

    location ~ ^/(README.md|INSTALL|LICENSE|CHANGELOG|UPGRADING)$ {
        deny all;
    }

    location ~ ^/(config|temp|logs)/ {
        deny all;
    }
}
```



```
}

location ~ /\. {
    deny all;
    access_log off;
    log_not_found off;
}

# pass the PHP scripts to FastCGI server listening on /var/run/php5-fpm.sock

location ~ \.php$ {
    try_files $uri =404;
    fastcgi_pass unix:/var/run/php5-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    include fastcgi_params;
}

ssl_certificate /etc/ssl/ca.crt;
ssl_certificate_key /etc/ssl/ca.key;
ssl_prefer_server_ciphers On;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers
    ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECD
    H+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+
    AES:RSA+3DES:!aNULL:!MD5:!DSS;

ssl_session_cache shared:SSL:20m;
ssl_session_timeout 10m;
add_header Strict-Transport-Security "max-age=31536000";
}
```

Guardar y salir.

Almacenar los cambios y dejar la edición, para crear los enlaces dinámicos:

```
$>su cd /etc/nginx/sites-enabled  
$>su ln -s /etc/nginx/sites-available/roundcube
```

Instalar el generador de certificados para seguridad y generar el par de claves:

```
$>su apt-get install ssl-cert  
$>su mkdir -p /etc/ssl/localcerts  
$>su openssl req -new -x509 -days 365 -nodes -out /etc/ssl/localcerts/roundcube.pem -keyout  
/etc/ssl/localcerts/roundcube.key  
$>su chmod 600 /etc/ssl/localcerts/*
```

Reiniciar el servicio y comprobar la configuración:

```
$>su service nginx restart  
$>su nginx -t
```

Instalar el cliente para la conexión a bases de datos:

```
$>apt-get install postgresql-9.4 postgresql-client-9.4
```

### **Servidor de Base de Datos** (*Dir IP 192.168.12.135*)

Luego de crear usuarios, asignar permisos, incluir alias en el hosts, así como configurar los repositorios de debian, siguiendo los pasos del anterior servidor se procede a instalar el manejador de base de datos:

```
$>su apt-get install postgresql-9.4 postgresql-client-9.4 postgresql-contrib-9.4
```

Se edita el archivo:

```
$>su nano /etc/postgresql/9.4/main/pg_hba.conf
```

Añaden la siguiente línea para permitir la conexión desde el servidor de la aplicación web a la base de datos:



```
host all all 192.168.12.181/32 md5
```

Se edita el siguiente archivo de configuración y se otorga el permiso correspondiente:

```
$>su nano /etc/postgresql/9.4/main/postgresql.conf
```

```
listen_addresses = '*'
```

(Este parámetro resulta en una configuración básica genérica que permite conexiones desde cualquier host, comprobando que se encuentre dentro de los permitidos)

Se almacenan los cambios y se reinicia el manejador:

```
$>service postgresql restart
```

Ahora siu podemos crear la base de datos, como usuario postgres

```
$>su postgres
$postgres>psql -U postgres -c "CREATE DATABASE roundcube WITH ENCODING 'UTF-8'
    TEMPLATE template0;"
$postgres>psql -U postgres -c "CREATE USER administrador WITH PASSWORD 'clave';"
$postgres>psql -U postgres -c "GRANT ALL PRIVILEGES ON DATABASE roundcube TO
    administrador;"
$postgres>psql -U postgres -d roundcube -f /usr/share/postgresql/9.4/extension/unaccent--1.0.sql
$postgres>psql -U postgres -c "CREATE EXTENSION unaccent;"
```

Se puede verificar la conexión y la creación de la misma desde la herramienta de escritorio en nuestra computadoras pgadmin, por supuesto incluyendo la conexión y autenticación.

**La estructura y contenido de las tablas en la base de datos se crean en el primer momento en que se ejecuta el sistema desde la web.**

## Servidor de Correo

IP: 192.168.12.166

Antes de proceder deben ajustarse algunos parámetros del sistema:

```
$> apt-get remove sendmail
$> echo "correo.cenditel" > /etc/mailname
$> echo "192.168.12.181 correo-web.cenditel " >> /etc/hosts
$> echo "192.168.12.166 correo-mail.cenditel" >> /etc/hosts
```

Instalar los siguientes software:

```
$> apt-get install exim4-daemon-heavy exim4-config dovecot-imapd dovecot-pgsql
```

Verificar que existan los parámetros de conexión con dovecot en “/etc/exim4/exim4.template”:

```
dovecot_login:
driver = dovecot
public_name = LOGIN
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1

dovecot_plain:
driver = dovecot
public_name = PLAIN
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

Reconfigurar el exim4

```
$>dpkg-reconfigure exim4-config
```

**Mail Server configuration**

General type of mail configuration:

internet site; mail is sent and received directly using SMTP  
mail sent by smarthost; received via SMTP or fetchmail  
mail sent by smarthost; no local mail  
local delivery only; not on a network  
no configuration at this time

**<Ok>** <Cancel> I

**Mail Server configuration**

The 'mail name' is the domain name used to 'qualify' mail addresses without a domain name.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.

This name won't appear on From: lines of outgoing messages if rewriting is enabled.

System mail name: I

correo.cenditel

**<Ok>** <Cancel>

### Mail Server configuration

Please enter a semicolon-separated list of IP addresses. The Exim SMTP listener daemon will listen on all IP addresses listed here.

An empty value will cause Exim to listen for connections on all available network interfaces.

If this system only receives mail directly from local services (and not from other hosts), it is suggested to prohibit external connections to the local Exim daemon. Such services include e-mail programs (MUAs) which talk to localhost only as well as fetchmail. External connections are impossible when 127.0.0.1 is entered here, as this will disable listening on public network interfaces.

IP-addresses to listen on for incoming SMTP connections:

192.168.12.166

<Ok>

<Cancel>

### Mail Server configuration

Please enter a semicolon-separated list of recipient domains for which this machine should consider itself the final destination. These domains are commonly called 'local domains'. The local hostname (correo-mail.cenditel) and 'localhost' are always added to the list given here.

By default all local domains will be treated identically. If both a.example and b.example are local domains, acc@a.example and acc@b.example will be delivered to the same final destination. If different domain names should be treated differently, it is necessary to edit the config files afterwards.

Other destinations for which mail is accepted:

correo-mail.cenditel;correo.cenditel

<Ok>

<Cancel>

**Mail Server configuration**

Please enter a semicolon-separated list of recipient domains for which this system will relay mail, for example as a fallback MX or mail gateway. This means that this system will accept mail for these domains from anywhere on the Internet and deliver them according to local delivery rules.

Do not mention local domains here. Wildcards may be used.

Domains to relay mail for:

**<Ok>** <Cancel>

**Mail Server configuration**

Please enter a semicolon-separated list of IP address ranges for which this system will unconditionally relay mail, functioning as a smarthost.

You should use the standard address/prefix format (e.g. 194.222.242.0/24 or 5f03:1200:836f::/48).

If this system should not be a smarthost for any other host, leave this list blank.

Machines to relay mail for:

**<Ok>** <Cancel>

### Mail Server configuration

In normal mode of operation Exim does DNS lookups at startup, and when receiving or delivering messages. This is for logging purposes and allows keeping down the number of hard-coded values in the configuration.

If this system does not have a DNS full service resolver available at all times (for example if its Internet access is a dial-up line using dial-on-demand), this might have unwanted consequences. For example, starting up Exim or running the queue (even with no messages waiting) might trigger a costly dial-up-event.

This option should be selected if this system is using Dial-on-Demand. If it has always-on Internet access, this option should be disabled.

Keep number of DNS-queries minimal (Dial-on-Demand)?

<Yes>

<No>

### Mail Server configuration

The Debian exim4 packages can either use 'unsplit configuration', a single monolithic file (/etc/exim4/exim4.conf.template) or 'split configuration', where the actual Exim configuration files are built from about 50 smaller files in /etc/exim4/conf.d/.

Unsplit configuration is better suited for large modifications and is generally more stable, whereas split configuration offers a comfortable way to make smaller modifications but is more fragile and might break if modified carelessly.

A more detailed discussion of split and unsplit configuration can be found in the Debian-specific README files in /usr/share/doc/exim4-base.

Split configuration into small files?

<Yes>

<No>

## ANEXO 3

```
//-----Inicio del archivo /etc/nginx/sites-available/roundcube
server {
    listen 80;
    server_name correo-web;
    return 301 https://correo-web$request_uri;
}
server {
    # llisten 80 is modified to listen 443 ssl;
    listen 443 ssl;
    server_name correo-web;
    root /srv/public/roundcube;
    index index.php index.html index.htm;
    access_log /var/log/nginx/roundcube_access.log;
    error_log /var/log/nginx/roundcube_error.log;
    location / {
        try_files $uri $uri/ /index.php?q=$uri&$args;
    }

    error_page 404 /404.html;
    error_page 500 502 503 504 /50x.html;

    location = /50x.html {
        root /usr/share/nginx/html;
    }

    location ~ ^/(README.md|INSTALL|LICENSE|CHANGELOG|UPGRADING)$ {
        deny all;
    }
}
```

```
location ~ ^/(config|temp|logs)/ {
    deny all;
}
```

```
location ~ /\. {
    deny all;
    access_log off;
    log_not_found off;
}
```

```
# pass the PHP scripts to FastCGI server listening on /var/run/php5-fpm.sock
```

```
location ~ \.php$ {
    try_files $uri =404;
    fastcgi_pass unix:/var/run/php5-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
    include fastcgi_params;
}
```

```
ssl_certificate /etc/ssl/ca.crt;
ssl_certificate_key /etc/ssl/ca.key;
ssl_prefer_server_ciphers On;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

```
ssl_ciphers
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+
3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS;

ssl_session_cache shared:SSL:20m;
ssl_session_timeout 10m;
add_header Strict-Transport-Security "max-age=31536000";

}
```

```
//-----Fin del archivo /etc/nginx/sites-available/roundcube
```