Servidor de Correo

BIND, Postfix, Cyrus-imapd, SASL

Instalación y configuración básica de un servidor de correo electrónico, en CentOS-5, con uso de buzones virtuales.

2007-06-22
Alain Reguera Delgado
alain.reguera@gmail.com

Indice

1. Datos Generales

Hardware:

- CPU a 2.6GHz
- RAM 256MB
- HDD 40GB

Dominio por defecto:

- dmotos.tld

Dominios virtuales utilizados:

1. ventas.dmotos.tld
2. comercial.dmotos.tld

Distribución del espacio

- /boot 100MB
- swap 512MB
- / 10000MB
- /var 29388MB

Administración de Puertos y Seguridad

Todo nuestro servidor de correo será instalado y configurado en una sola computadora. Para que nuestro sistema de correo funcione es necesario que, en esta computadora, se abran los puertos siguientes:

Alias	Puerto	Protocolo	Descripción
domain	53	UDP	Para resolver nombres e direcciones IP (DNS)
domain	53	TCP	Para resolver nombres e direcciones IP (DNS)
SMTP	25	TCP	Para el Agente de Transferencia de Correo (MTA).
POP3	110	TCP	Para poder descargar los mensajes del servidor.
IMAP	143	TCP	Para poder revisar los mensajes directamente en el servidor.
HTTP	80	TCP	Para revisar y enviar correo vía Web.
SSH	22	TCP	Para la administración del servidor desde una computadora remota.

Utilice el comando **`system-config-securitylevel-tui`** para administrar los puertos y el modo de trabajo de SELinux. Para nuestro ejemplo utilizamos el modo permisivo de SELinux.

2. Instalación mínima de CentOS-5

Todo el sistema de correo será instalado y configurado sobre la distribución CentOS-5 de GNU/Linux. Para ello haremos una instalación mínima de la distribución y luego iremos instalando cada uno de los programas a medida que sea necesario.

Para hacer una instalación mínima de CentOS-5 usted necesita:

- Tener el primer CD (o el DVD) de instalación de CentOS-5.
- Comenzar el proceso de instalación.
- En la sección "Selección de categorías" especificar que desea hacer una instalación personalizada.
- En la sección de "Selección de los paquetes por categoría" deshabilitar todos los paquetes para todas las categorías.
- Continuar con la instalación.

3. Instalación y configuración de BIND

BIND es un servidor de nombres de dominio. Una de sus ventajas es que nos permite manejar las direcciones IP en forma de nombres. Además, en él es donde especificamos cual o cuales serán nuestros servidores intercambiadores de correo. Si queremos recibir correo desde Internet es conveniente instalar y configurar un servidor de nombres para nuestro dominio.

3.1. Instalación

Para instalar BIND ejecute el comando:

```
yum install bind bind-chroot
```

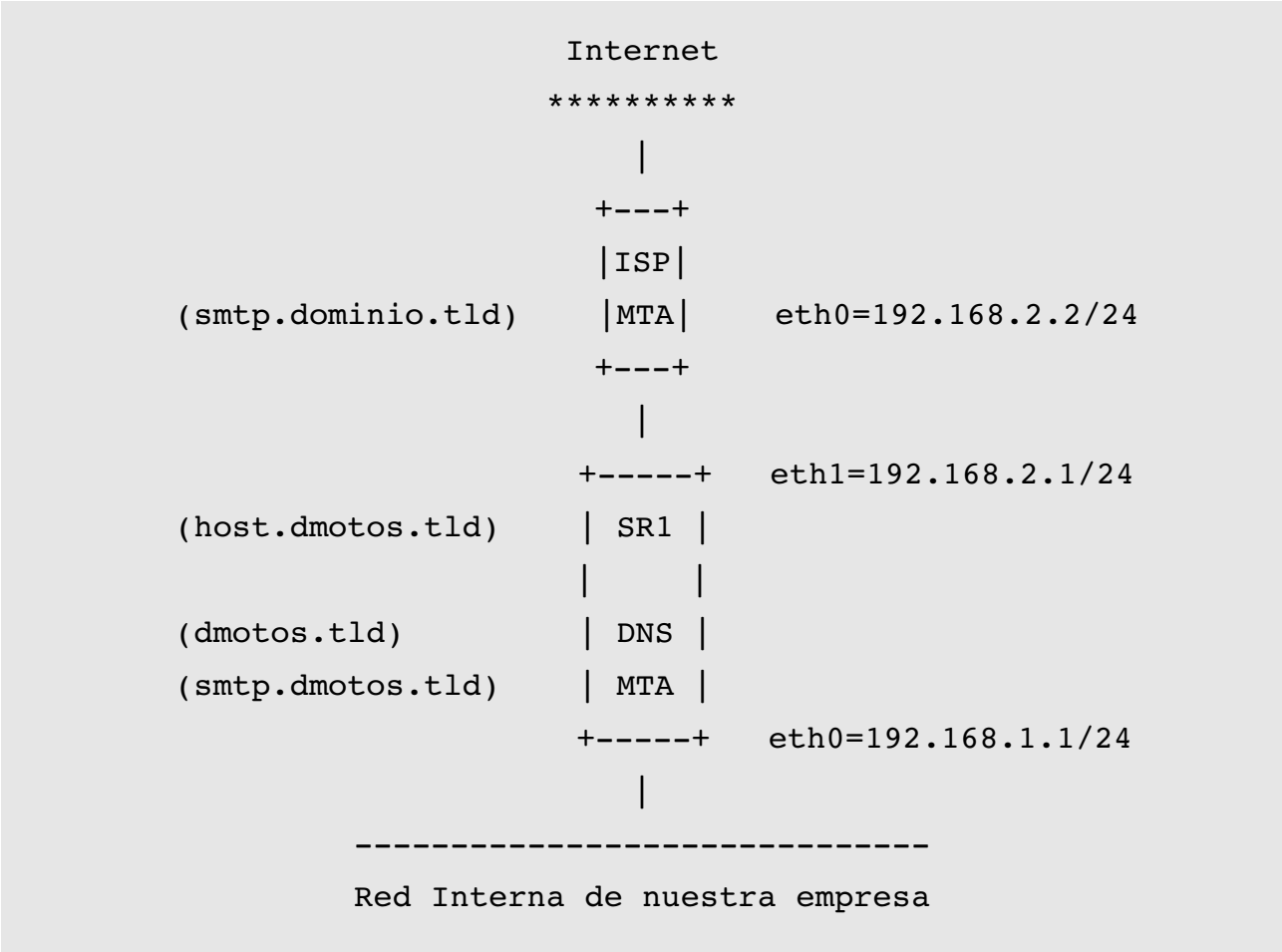
Para ahorrarnos algunos teclazos a la hora de crear los ficheros de configuración, podemos instalar el paquete `caching-nameserver` y adaptar los ficheros de configuración instalados a nuestra configuración específica. Para ello ejecutamos el comando:

```
yum install caching-nameserver
```

Para ilustrar nuestra explicación basaremos la configuración en una empresa ficticia llamada *Dmotos*. Los ficheros de configuración en este documento están construidos para esta estructura. Usted puede adaptarlos a su estructura en caso que sea diferente, o mejorarlos si coinciden con esta.

> **ATENCIÓN:**
>
> Las direcciones IP utilizadas en este documento son con fines demostrativos. Las direcciones IP utilizadas en este documento están reservadas para uso local y no son visibles desde Internet directamente. Para intercambiar correo con otros servidores en Internet es necesario enviar los mensajes a una computadora con dirección verdadera de Internet. Para que dos computadoras puedan intercambiar correo directamente necesitan "verse" entre sí. Ver punto 2.3.

3.2. Estructura de conexión



- ISP: Proveedor de Servicios de Internet
- SR1: Abreviatura para referirnos al Servidor 1.
- **`host.dmotos.tld`**: Nombre completo de la computadora SR1. En esta computadora es donde instalaremos y configuraremos todo nuestro sistema de correo.
- **`dmotos.tld`**: Zona bajo nuestro control. Este es el dominio por defecto con el cual nuestros mensajes se enviarán.
- **`mail.dmotos.tld`**: Alias utilizado para referirnos a la computadora SR1.
- **`eth0=192.168.1.1/24`**: La interfases de red que conecta el SR1 a la red interna de nuestra empresa. Esta es la dirección que los usuarios en la red interna utilizarán para resolver los nombres, enviar y recibir correos.

- **eth01=192.168.2.1/24**: La interfase de red que conecta el SR1 con la red del ISP. Esta es la interfase que el SR1 utilizará para comunicarse con el mundo exterior. Esta interfase permite que los correos que tienen como recipiente de destino una dirección con un dominio externo a dmotos.tld (o a los virtualmente definidos en SR1) puedan ser entregados a su destino.

- **eth0=192.168.2.2/24**: La interfase de red del proveedor que se puede utilizar para entregar mensajes. Útil en los casos que no esté permitido la conexión directa de el SR1 a la dirección IP de la computadora devuelta en la consulta realizada al registro MX del dominio externo vía DNS, al cual se desea enviar correo.

  Nota: En este documento se asume que el SR1 puede comunicarse directamente con las direcciones IP de las computadoras en Internet a las cuales desea enviar correo.

  Nota: En este documento se asume que el SR1 puede recibir conexiones entrantes de computadoras en Internet para recibir los mensajes destinados a los usuarios de la red interna de nuestra empresa.

3.3. Comprobar conexión

Por ejemplo si desea comprobar el envío directo de correos al dominio gmail.com siga los pasos siguientes:

- Buscamos las direcciones IP de los intercambiadores de correo de GMail.

```
dig mx gmail.com
```

```
;; ANSWER SECTION:
gmail.com.          3238   IN     MX     50 gsmtp183.google.com.
gmail.com.          3238   IN     MX     5 gmail-smtp-in.l.google.com.
gmail.com.          3238   IN     MX     10 alt1.gmail-smtp-in.l.google.com.
gmail.com.          3238   IN     MX     10 alt2.gmail-smtp-in.l.google.com.
gmail.com.          3238   IN     MX     50 gsmtp163.google.com.
```

- Comprobamos si podemos acceder directamente a uno de los intercambiadores de correo de gmail.com:

```
ping gmail-smtp-in.l.google.com
```

- En otros casos puede que el servidor no permita consultas directas mediante el comando **ping**. Para ello encuestamos directamente el puerto 25 (donde escuchan generalmente los MTAs) del servidor para ver si está recibiendo conexiones entrantes.

```
telnet gmail-smtp-in.l.google.com 25
```

3.4. Configuración

La versión de BIND que viene con CentOS-5 incorpora la facilidad Views (Vistas). Las Vistas nos permiten con una sola instalación de BIND configurar respuestas diferentes según los orígenes que hagan la petición y los destinos hacia donde estas peticiones estén dirigidas. Útil para los casos que una computadora tenga dos interfaces de red para servir a redes diferentes.

En nuestro servidor de nombre crearemos dos vistas, una responde a los usuarios de la red interna de nuestra empresa y la otra responde a las peticiones de Internet. Los usuarios que pregunten desde la red interna obtendrán una respuesta y los que pregunten desde Internet tendrán otra.

Veamos los ficheros de configuración:

/var/named/chroot/etc/named.conf

```
 1      options {
 2            listen-on port 53 { 192.168.2.1; 192.168.1.1; 127.0.0.1; };
 3            directory "/var/named";
 4            dump-file “/var/named/data/cache_dump.db";
 5            statistics-file "/var/named/data/named_stats.txt";
 6            memstatistics-file "/var/named/data/named_mem_stats.txt";
 7       };
 8
 9       controls {
10            inet 127.0.0.1 allow { localhost; }
11            keys { "rndckey"; };
12       };
13
14       include "/etc/rndc.key";
15
16       logging {
17            channel default_debug {
18                    file "data/named.run";
19                    severity dynamic;
20            };
21       };
22
23       acl "intranet" { 192.168.1/24; };
24
25       view "external_resolver" {
26            match-clients { any; };
27            match-destinations { 192.168.2.1; };
28            recursion yes;
29            include "/etc/named.rfc1912.zones";
30
31            zone "dmotos.tld" IN {
32                    type master;
33                    file "dmotos.tld.external.zone";
34                    allow-update { none; };
35            };
36
37       };
38
```

```
39       view "internal_resolver" {
40            match-clients { "intranet"; };
41            match-destinations { 192.168.1.1; };
42            recursion yes;
43            include "/etc/named.rfc1912.zones";
44
45            zone "dmotos.tld" IN {
46                    type master;
47                    file "dmotos.tld.zone";
48                    allow-update { none; };
49            };
50
51            zone "0.168.192.in-addr.arpa" IN {
52                    type master;
53                    file "192.168.1.zone";
54                    allow-update { none; };
55            };
56       };
```

En las líneas 25 y 39 del fichero **`/var/named/chroot/etc/named.conf`** se definen las vistas. `external_resolver` hace referencia a la vista externa, la que se verá desde Internet. `internal_resolver` hace referencia a la vista interna, la que se verá desde la red interna de nuestra empresa.

/var/named/chroot/var/named/dmotos.tld.zone

```
 1      $TTL 3h
 2      dmotos.tld. IN SOA host.dmotos.tld. al.dmotos.tld. (
 3                                2007052300 ; Serial
 4                                3h         ; Refresh after 3 hours
 5                                1h         ; Retry after 1 hour
 6                                1w         ; Expire after 1 week
 7                                1h )       ; Negative caching TTL of 1 hour
 8      ;
 9      ; Name Server
10      ;
11                      IN      NS      host
12      ;
13      ; Mail Server
14      ;
15                      IN      MX 10   host
16      ;
17      ; Addresses for the canonical names
18      ;
19                      IN A    192.168.1.1
20      host            IN A    192.168.1.1
21      host2           IN A    192.168.1.2
22      hostn           IN A    192.168.1.3
23
24      ;
25      ; Aliases
26      ;
27      mail                CNAME   host
```

En este fichero es donde configuramos los registros que resuelven las direcciones IP cuando se pregunta un nombre o alias desde la red interna de nuestra empresa. Para esta vista el intercambiador de correo es la computadora **`host.dmotos.tld`** (línea 15).

Como esta información fue definida dentro de la vista `internal_resolver`, estará disponible solo para los usuarios de la red interna[1] y que interroguen al servidor de nombre ubicado internamente[2].

[1] Vea definición en la línea 23 de **`/var/named/chroot/etc/named.conf`**

[2] Vea definición en las líneas 39, 40 y 41 de **`/var/named/chroot/etc/named.conf`**

En esta configuración se ha dicho que para los usuarios de la red interna de nuestra empresa las computadoras **`host`**, **`host1`** y **`hostn`** tienen las direcciones IP 192.168.1.1, 192.168.1.2 y 192.168.1.3 respectivamente. Usted puede adicionar más nombres y direcciones de computadoras en esta sección.

En el caso de los Aliases, los usuarios de la red interna de nuestra empresa podrán acceder a la computadora **`host.dmotos.tld`** de dos formas:

3. **`dmotos.tld`** (ver línea 19 en **`/var/named/chroot/etc/named.conf`**)
4. **`mail.dmotos.tld`** (ver línea 27 en **`/var/named/chroot/etc/named.conf`**)

Más adelante le puede ser conveniente adicionar nuevos aliases.

`/var/named/chroot/var/named/192.168.0.zone`

```
 1      $TTL 3h
 2      0.168.192.in-addr.arpa.   IN    SOA     host.dmotos.tld. al.dmotos.tld.
(
 3                                2007052300 ; Serial
 4                                3h         ; Refresh after 3 hours
 5                                1h         ; Retry after 1 hour
 6                                1w         ; Expire after 1 week
 7                                1h )       ; Negative caching TTL of 1 hour
 8
 9      ;
10      ; Name servers
11      ;
12                IN NS  host.dmotos.tld.
13
14      ;
15      ; Addresses point to canonical name
16      ;
17      1         IN PTR host.dmotos.tld.
18      2         IN PTR host2.dmotos.tld.
19      3         IN PTR hostn.dmotos.tld.
```

En este fichero es donde configuramos los registros que resuelven los nombres cuando se pregunta una dirección IP desde la red interna de nuestra empresa.

Los registros que se listen aquí deben coincidir con los del fichero de configuración anterior donde se definieron los registros que resuelven las direcciones IP cuando se pregunta un nombre. Si usted relaciona el nombre de una computadora a una IP, luego debe relacionar esa IP al mismo nombre, haciendo que las dos búsquedas coincidan. De no ser así, puede que algunos programas que realicen la búsqueda inversa funcionen incorrectamente.

/var/named/chroot/var/named/dmotos.tld.external.zone

```
 1      $TTL 3h
 2      dmotos.tld. IN SOA host.dmotos.tld. al.dmotos.tld. (
 3                                2007052300 ; Serial
 4                                3h         ; Refresh after 3 hours
 5                                1h         ; Retry after 1 hour
 6                                1w         ; Expire after 1 week
 7                                1h )       ; Negative caching TTL of 1 hour
 8      ;
 9      ; Name Server
10      ;
11                IN      NS      host
12
13      ;
14      ; Mail Server
15      ;
16                IN      MX 10   host
17      ;
18      ; Addresses for the canonical names
19      ;
20                IN A    192.168.2.1
21      host      IN A    192.168.2.1
22
23      ;
24      ; Aliases
25      ;
26      mail              CNAME   host
```

En este fichero es donde configuramos los registros que resuelven las direcciones IP cuando se pregunta un nombre o alias desde Internet. Para esta vista el intercambiador de correo es la computadora **`host.dmotos.tld`** (ver línea 16).

Seguramente ya se dio cuenta que tanto el fichero que relaciona la vista externa como interna hacen referencia a la misma computadora. La diferencia está en la direcciones IPs que se especifican. Para la vista interna utilizamos la IP 192.168.1.1/24 pues es la dirección que las computadoras en la red interna de nuestra empresa pueden contactar. Para la vista externa utilizamos la IP 192.168.2.1/24 pues es la dirección que las computadoras en Internet pueden contactar.

La computadora que actúa como intercambiador de correo es la que tiene por nombre **`host.dmotos.tld`**. Más abajo en este fichero vemos que **`host.dmotos.tld`** tiene asignada la dirección IP 192.168.2.1/24 en la interfaz que conecta a Internet. De esta forma cuando se intente

enviar un correo a nuestro dominio desde Internet, el servidor de nombre de nuestro dominio responderá enviando la IP 192.168.2.1/24.

Cuando un programa cliente (generalmente un MTAs) en Internet desea enviar un mensaje de correo a nuestro dominio, pregunta al sistema de nombres de dominio cuál es el registro MX para nuestro dominio. Con esta dirección como respuesta, el cliente de Internet intenta iniciar una conversación hacia ella para entregar los mensajes que desea enviar a nuestro dominio.

> **Nota:** para especificar y hacer coincidir la búsqueda inversa de la dirección IP de la interfase de red que apunta a Internet usted debe ponerse en contacto con su proveedor de servicio, la institución que le asignó la dirección IP y mostrarle su deseo y necesidad de actualizar el registro (PTR) de la zona inversa en la base de datos relacionado con la IP que le fue asignada. Siempre que cambie el nombre de la computadora **`host.dmotos.tld`** deberá actualizar esta información con su proveedor de servicio. Ellos son los que tienen la autoridad sobre la búsqueda inversa de las direcciones que asignan.

`/etc/resolv.conf`

```
nameserver 192.168.2.1
```

Este es el fichero de configuración del resolver de la computadora donde esta instalado el servidor de nombres de dominio. Aquí se especifica que: cuando una consulta se origine en esta computadora será dirigida a la vista externa. Si en la vista externa o en la cache del servidor no está la respuesta, entonces se inicia el proceso de resolución del nombre o IP desde los dominios topes de Internet.

`/etc/host.conf`

```
order hosts, bind
```

En este fichero de configuración que especifica el orden en el que consultará el resolver de la computadora donde tenemos instalado el servidor de nombre de dominio. En este caso se ha fijado que primeramente se consulte la tabla de hosts (ver `/etc/hosts`) del sistema y luego al servidor de nombres de dominio bind.

3.5. Puertos y seguridad

Ejecutamos el comando **`system-config-securitylevel-tui`** y habilitamos las conexiones entrantes a los puertos siguientes:

Alias	Puerto	Protocolo	Descripción
domain	53	UDP	Para resolver nombres nombres de dominio (DNS)
domain	53	TCP	Para resolver nombres nombres de dominio (DNS)

SELinux	Permisivo

3.6. Iniciar el servicio

Para iniciar el servicio ejecutamos el comando:

```
service named start
```

Adicionalmente fijamos que, para el próximo arranque del sistema el servicio iniciará automáticamente. Para ello ejecutamos el comando:

```
chkconfig --level 2345 named on
```

3.7. Probar la configuración

Una vez que hayamos configurado nuestro servidor de nombre pasamos a probarlo. Es conveniente realizar pruebas desde tres posiciones distintas:

1. Comprobamos la resolución de la vista interna, desde la red interna.
   - **`nslookup mail.dmotos.tld`**
   - **`nslookup 192.168.1.1`**
2. Comprobamos la resolución para Internet, desde la propia computadora donde está instalado el servidor de nombre, con el resolver apuntando a la vista externa.
   - **`dig mx google.com`**
   - **`dig mx yahoo.com`**
3. Comprobamos la resolución de la vista externa, desde Internet.
   - http://www.kloth.net/services/dig.php
     - En esta página se muestra una interfase web que nos permite consultar dominios desde Internet haciendo uso de la herramienta **`dig`**. Nos viene muy bien en este punto pues nos permite verficiar que la computadora que está haciendo de intercambiador de correo, cuando se intenta enviar un correo a nuestro dominio desde Internet, es la que nosotros especificamos.
     - Utilice el formulario que muestra esta página para realizar las comprobaciones.
     - En el menú de selección de los registros, utilice el registro MX para verificar el intercambiador de corre del dominio especificado.

Nota: Los comando **`nslookup`**, **`dig`**, **`host`** y **`nsupdate`** no se instalan cuando se hace una instalación mínima de CentOS-5. Para ello necesitamos instalar el paquete **`bind-utils`** ejecutando el comando:

```
yum install bind-utils
```

Cuando hayamos comprobado el correcto funcionamiento del servicio de nombres para nuestro dominio, entonces es hora de instalar y configurar el programa que se encargará de intercambiar correos para nuestro dominio.

4. Instalación y configuración de Postfix

Postfix es el programa que utilizaremos para enviar y recibir mensajes.

Postfix será instalado en la computadora que definió como MX en su servidor de nombres de dominio. En nuestro caso instalamos Postfix en la misma computadora donde instalamos el servidor de nombres de dominio (`host.dmotos.tld`).

4.1. Instalación

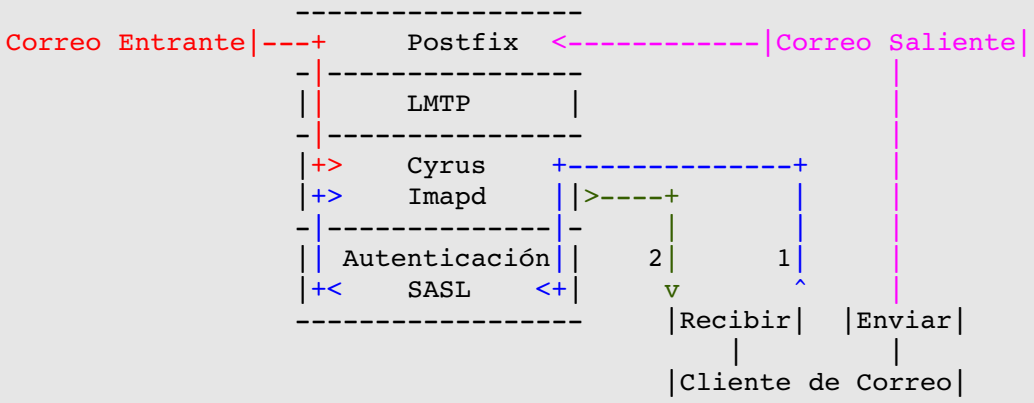
Para instalar Postfix ejecute el comando:

```
yum install postfix
```

4.2. Configuración

Para configurar Postfix necesitamos tener en mente que tipo de configuración queremos implementar.

En esta sección nuestro objetivo es la creación de buzones que no se almacenan en Postfix y que no utilizan cuentas del sistema. El programa que utilizaremos para crear los buzones de los usuarios es Cyrus-Imapd y para gestionar la autenticación de usuario SASL. En esta configuración, para entregarle a Cyrus-Imapd el mensaje, Postfix utiliza el protocolo LMTP.



Nota: A la hora de recibir, el paso número 2 solo tiene lugar si la Autenticación SASL es satisfactoria (el nombre de usuario y la contraseña suministrada por el usuario coincide con los datos existentes en la base de datos sasl). En el paso 2 el usuario recibe los mensajes de correos almacenados en su buzón.

En esta sección veremos solamente la configuración de Postfix.

En Postfix creamos dos dominios virtuales:

4. ventas.dmotos.tld

5. comercial.dmotos.tld

También utilizaremos el dominio por defecto:

- dmotos.tld

Esto quiere decir que en nuestro sistema de correo tendremos cuentas que terminarán de la siguiente forma:

- @dmotos.tld
- @ventas.dmotos.tld
- @comercial.dmotos.tld

En la configuración fijamos las direcciones de correo para las cuales el intercambiador de correo permitirá correos entrantes. Otras direcciones que no sean estas, serán rechazadas. Ver los ficheros de configuración más abajo.

/etc/postfix/main.cf

```
...

# INTERNET HOST AND DOMAIN NAMES
#
# The myhostname parameter specifies the internet hostname of this
# mail system. The default is to use the fully-qualified domain name
# from gethostname(). $myhostname is used as a default value for many
# other configuration parameters.
#
myhostname = host.dmotos.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = dmotos.tld

...

# RECEIVING MAIL

# The inet_interfaces parameter specifies the network interfase
# addresses that this mail system receives mail on.  By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all

...

# ADDRESS REDIRECTION (VIRTUAL DOMAIN)
```

```
#
# The VIRTUAL_README document gives information about the many forms
# of domain hosting that Postfix supports.

virtual_transport = lmtp:unix:/var/lib/imap/socket/lmtp
virtual_mailbox_domains =
      dmotos.tld
      ventas.dmotos.tld
      comercial.dmotos.tld
virtual_mailbox_maps =
      hash:/etc/postfix/vmailbox
      hash:/etc/postfix/vmailbox_ventas
      hash:/etc/postfix/vmailbox_comercial
virtual_alias_maps = hash:/etc/postfix/virtual
```

/etc/postfix/vmailbox

```
al    Cualquier                    Valor
# ... Más cuentas de usuarios @dmotos.tld.
```

/etc/postfix/vmailbox_ventas

```
al@ventas.dmotos.tld               Valor
# ... Más cuentas de usuarios virtuales @ventas.dmotos.tld.
```

/etc/postfix/vmailbox_comercial

```
al@comercial.dmotos.tld            Valor
# ... Más cuentas de usuarios virtuales @comercial.dmotos.tld.
```

/etc/postfix/virtual

```
root                               root@host.dmotos.tld
postmaster@ventas.dmotos.tld       postmaster
postmaster@comerial.dmotos.tld     postmaster
```

myhostname

fija el nombre completo de la computadora. En nuestro ejemplo host.dmotos.tld.

mydomain

fija el nombre del dominio de nuestra computadora. En nuestro ejemplo dmotos.tld.

inet_interfaces

fija por cuales interfaces de red Postfix estará escuchando. La palabra all nos dice que estará escuchando por todas las interfaces que existan en la computadora. En nuestro caso estas son eth0=192.168.1.1/24 y eth1=192.168.2.1/24.

virtual_transport

fija el transporte que utilizará postfix para entregar mensajes a los buzones de los usuarios. Como manejaremos los buzones de los usuarios con Cyrus-Imapd, utilizamos el trasporte

LMTP que viene siendo un protocolo común de comunicación local o remota (en este caso local) entre Postfix y Cyrus-Imapd.

`virtual_mailbox_domains`

nos permite definir cuales son los dominios para los que Postfix recibirá mensajes. En nuestro ejemplo queremos que los dominios dmotos.tld, ventas.dmotos.tld y comercial.dmotos.tld puedan recibir mensajes.

`virtual_mailbox_maps`

Permite definir un fichero con las direcciones de nuestros usuarios y sus dominios. Las direcciones que no se encuentren en esta lista serán rechazadas. Cuando terminemos de editar el fichero ejecutamos el comando **`postmap /camino/al/fichero`** para actualizar los cambios en la base de datos relacionada al fichero. Ej.

```
postmap /etc/postfix/vmailbox
postmap /etc/postfix/vmailbox_ventas
postmap /etc/postfix/vmailbox_comercial
```

`virtual_alias_maps`

Permite crear alias entre usuarios virtuales. Es necesario que liste el usuario con el dominio correspondiente. En caso contrario se asumirá el dominio que se definió por defecto en el parámetro **`mydomain`**. Cuando terminemos de editar el fichero ejecutamos el comando **`postmap /camino/al/fichero`** para actualizar los cambios en la base de datos relacionada al fichero. Ej.

```
postmap /etc/postfix/virtual
```

4.3. Puertos y seguridad

Ejecutamos el comando **`system-config-securitylevel-tui`** y habilitamos las conexiones entrantes a los puertos siguientes:

Alias	Puerto	Protocolo	Descripción
smtp	25	TCP	Para el Agente de Transferencia de Correo (MTA).

SELinux	Permisivo

4.4. Iniciar el servicio

Para iniciar el servicio ejecutamos el comando:

```
service postfix start
```

Adicionalmente fijamos que, para el próximo arranque del sistema el servicio iniciará automáticamente. Para ello ejecutamos el comando:

```
chkconfig --level 2345 postfix on
```

5. Instalación y configuración de Cyrus-Imapd

Cyrus-Imapd es la aplicación que utilizaremos para gestionar los buzones de los usuarios en nuestro sistema de correo. Además, Cyrus-Imapd es la aplicación que permite que los usuarios puedan descargar los mensajes a su computadora o leerlos directamente en el servidor.

Cyrus-Imapd tiene la característica que utiliza una base de datos interna para almacenar los buzones de los usuarios. Esto hace posible que el servidor corra en una forma "sellada". Los usuarios de correo no necesitan una cuenta en el sistema operativo para poder revisar su buzón de correo.

Para manejar la autenticación de usuarios Cyrus-Imapd trae consigo una biblioteca que implementa una capa de seguridad y autenticación simple (SASL) que es utilizada cuando los usuarios intentan establecer conexión con Cyrus-Imapd.

Cyrus-Imapd tiene la posibilidad de asignación de cuotas y permisos de accesos a a los buzones creados.

5.1. Instalación

Para instalar Cyrus-Impad ejecute el comando siguiente:

```
yum install cyrus-imapd
```

5.2. Configuración

Cyrus-Imapd viene configurado por defecto para trabajar sin dominios virtuales. Para adaptarlo a nuestro ejemplo es necesario hacer algunos cambios en el fichero de configuración (`/etc/imapd.conf`).

Para la autenticación de los usuarios también haremos algunos cambios, debido a que la configuración por defecto no nos permite autenticar usuarios de dominios virtuales.

Para organizar el contenido de esta sección vamos a crear las subsecciones siguientes:

5.2.1. Configuración para dominios virtuales.
5.2.2. Administración de los buzones de correo.
5.2.3. Administración de la base de datos sasldb2.

5.2.1. Configuración para dominios virtuales

La configuración siguiente fue la que utilizamos para nuestro ejemplo:

/etc/imapd.conf

```
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: cyrus cyrusadm
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
sasl_pwcheck_method: auxprop
sasl_mech_list: PLAIN
tls_cert_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_key_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_ca_file: /etc/pki/tls/certs/ca-bundle.crt
virtdomains: yes
defaultdomain: dmotos.tld
unixhierarchysep: yes
```

Algunos parámetros relevantes:

admins: cyrus cyrusadm

Con este parámetro definimos quienes van a administrar Cyrus-Imapd.

Por defecto el usuarios cyrus viene como administrador pues es el usuario que se utiliza para correr la aplicación.

`cyrusadm` fue el usuario que creamos para realizar las tareas administrativas y de mantenimiento de los buzones de correo en el servidor.

sasl_pwcheck_method: auxprop

Con este parámetro especificamos cual será el mecanismo que se utilizará mediante SASL para autenticar los usuarios. En este caso, con **auxprop** fijamos que la autenticación se realizará mediante la base de datos interna de SASL ubicada en el fichero **/etc/sasldb2**.

virtdomains: yes

Con este parámetro especificamos que vamos a utilizar dominios virtuales.

defaultdomain: dmotos.tld

Con este parámetro especificamos cual será el dominio por defecto de nuestro sistema de correo. Cuando no se especifique un dominio este será el que se asuma por defecto.

unixhierarchysep: yes

Con este parámetro definimos que vamos a utilizar el separador tradicional de unix (/) y no el

de las news (.). Esto nos va a posibilitar la creación de cuentas tales como: nombre.apellido@dmotos.tld.

La información del resto de los parámetros la puede encontrar en la página man de impad.conf. Para ello ejecute el comando:

```
man imapd.conf
```

5.2.2. Administración de los buzones de correo.

Para la administración de los buzones de correo tenemos el programa `cyradm`.

A continuación listamos la secuencia para crear, modificar y borrar un buzón usando cyradm:

1. Crear cuenta para el administrador o administradores del servidor Cyrus-Imapd. Para crear el usuario `cyrusadm` y ponerle una contraseña ejecutamos el comando siguiente:

   ```
   saslpasswd2 cyrusadm
   ```

2. Conectamos al servidor Cyrus-Imapd en host con el usuario cyrusadm.

   ```
   cyradm --user cyrusadm --server host
   ```

   Cuando se nos pregunte introducimos la contraseña que le fijamos al usuario cuando ejecutamos el comando **`saslpasswd2 cyrusadm`**.

3. Creamos los buzones para los usuarios al y lili en el dominio por defecto dmotos.tld.

   ```
   createmailbox user/al
   cm user/lili
   ```

4. Creamos buzones para los usuario lili en los dominios virtuales comercial.dmotos.tld y ventas.dmotos.tld

   ```
   cm user/lili@comercial.dmotos.tld
   cm user/lili@ventas.dmotos.tld
   ```

   Nota: aunque los dos buzones creados tienen el mismo nombre de usuario, son buzones diferentes debido a que se encuentran en dominios distintos.

5. Fijamos cuota de 20MB al buzón de lili en el dominio comercial.dmotos.tld y en dmotos.tld.

   ```
   setquota user/lili@comercial.dmotos.tld 20000
   ```

```
setquota user/lili 20000
```

Nota: recuerde que cuando no se especifica un dominio se toma el que fijamos en el parámetro `defaultdomain` en el fichero de configuración (`/etc/imapd.conf`).

6. Eliminamos el buzón de lili en el dominio comercial.dmotos.tld

   Para eliminar un buzón primero necesitamos darle permisos administrativos al usuario que definimos como administrador en (/etc/imapd.conf) sobre el buzón que se quiere eliminar. Para eso ejecutamos el comando:

   ```
   setacl user/lili@comercial.dmotos.tld cyrusadm c
   ```

   y luego eliminamos el buzón con el comando:

   ```
   dm user/lili@comercial.dmotos.tld
   ```

Esta es una lista de acciones administrativas comúnmente realizadas con `cyradm`. Para ver la lista completa de los comandos de `cyradm` ejecute el comando `help`.

Más información del comando `cyradm` y la administración de buzones puede encontrarla en los documentos que vienen con la instalación de Cyrus-Imapd. Para ver los documentos relacionados al paquete Cyrus-Imapd ejecute el comando:

```
rpm -qd cyrus-imapd
```

5.2.3. Administración de la base de datos de usuarios sasldb2.

Esta es la base de datos con la información de autenticación de los usuarios de nuestro sistema de correo. Aquí se almacenarán todos los nombres de usuario y contraseñas de los usuarios de nuestro sistema. Este es el fichero que Cyrus-Imapd utilizará para verificar las credenciales de autenticación suministradas por los usuarios cuando intenten revisar su buzón de correo.

Nota: Verifique que el fichero de la base de datos `/etc/sasldb2` sea accesible por el usuario que corre Cyrus-Imapd (cyrus). Para hacer este fichero accesible por Cyrus-Impad ejecute el comando siguiente:

```
chmod 660 /etc/sasldb2
chown root:cyrus /etc/sasldb2
```

Para adicionar nuevos usuarios a la base de datos sasldb2 utilice el comando **`saslpasswd2`**. Por

ejemplo para adicionar el usuario **lili@ventas.dmotos.tld** a la base de datos ejecutamos el comando:

```
saslpasswd2 lili@ventas.dmotos.tld
```

en cambio para el usuario **lili@dmotos.tld** ejecutamos el comando:

```
saslpasswd2 lili
```

Fíjese que cuando insertamos usuarios que pertenecen al dominio por defecto (en nuestro ejemplo, dmotos.tld) no adicionamos el dominio.

> **Nota**: Para las cuentas de usuarios con dominios virtuales inserte la dirección de correo completa del usuario.

> **Nota**: Para las cuentas locales de usuario utilice solamente el nombre de usuario.

Para actualizar la contraseña a una determinada cuenta de usuario en la base de datos sasldb2 ejecute los mismos pasos que acabamos de ver y cuando le pregunte la contraseña del usuario adicione la contraseña nueva.

Para eliminar una cuenta de usuario de la base de datos salsdb2 ejecute el comando **saslpasswd2** con la opción **-d**. Por ejemplo si necesita eliminar la cuenta lili@ventas.dmotos.tld ejecute el comando siguiente:

```
saslpasswd2 -d lili@ventas.dmotos.tld
```

Para listar todas las cuentas que han sido creadas en la base de datos sasldb2 ejecute el comando **sasldblistusers2**. En el caso que desee comprobar la existencia de una determinada cuenta puede ejecutar el comando **sasldblistusers2** combinándolo con **grep**. Por ejemplo si necesita saber si la cuenta lili@ventas.dmotos.tld existe en la base de datos sasldb2 ejecute el comando:

```
sasldblistusers2 | grep 'lili@ventas.dmotos.tld'
```

Más información de estos dos comandos pueden ser encontrados en sus respectivas páginas man.

5.3. Puertos y seguridad

Ejecutamos el comando **system-config-securitylevel-tui** y habilitamos las conexiones entrantes a los puertos siguientes:

Alias	Puerto	Protocolo	Descripción
POP3	110	TCP	Para poder descargar los mensajes del servidor.
IMAP	143	TCP	Para poder revisar los mensajes directamente en el servidor.

SELinux	Permisivo

5.4. Iniciar el servicio

Para iniciar el servicio ejecutamos el comando:

```
service cyrus-impad start
```

Adicionalmente fijamos que, para el próximo arranque del sistema el servicio iniciará automáticamente. Para ello ejecutamos el comando:

```
chkconfig --level 2345 cyrus-impad on
```

6. Instalar y configurar Squirrelmail

Squirrelmail es un cliente de correo web escrito en php.

6.1. Instalación

Para instalar Squirrelmail ejecuteel comando:

```
yum install squirrelmail
```

Esto instalará los ficheros necesarios para Squirrelmail y sus dependencias (Servidor Web Apache y PHP).

6.2. Configuración

Para configurar Squirrelmail ejecutamos el comando:

```
/usr/share/squirrelmail/conf/conf.pl
```

En este punto, nuestros usuarios podrán utilizar el navegador web (Ej. Firefox) para enviar y revisar sus mensajes de correo electrónico.

http://dmotos.tld/webmail/

Como dato adicional, si utiliza las cuotas para las cuentas que creó en Cyurs-Impad puede descargar y luego instalar el plugin quota-usage que está disponible en la página:

http://www.squirrelmail.org/plugin_view.php?id=59

para que los usuarios sepan en que estado está su cuota de almacenamiento.

6.3. Puertos y seguridad

Ejecutamos el comando **`system-config-securitylevel-tui`** y habilitamos las conexiones entrantes a los puertos siguientes:

Alias	Puerto	Protocolo	Descripción
HTTP	80	TCP	Para revisar y enviar correo vía Web.

SELinux	Permisivo

6.4. Iniciar el servicio

Para iniciar el servicio ejecutamos el comando:

```
service httpd start
```

Adicionalmente fijamos que, para el próximo arranque del sistema el servicio iniciará automáticamente. Para ello ejecutamos el comando:

```
chkconfig --level 2345 httpd on
```

7. Ejemplo Práctico

Supongamos que nuestra empresa se dedica a la venta de motocicletas, es una pequeña empresa pero esta creciendo.

Recientemente se han creado los departamentos "ventas" y "comercial". La empresa compró el dominio `dmotos.tld` y necesita habilitar el servicio de correo para sus empleados. La empresa decidió que los empleados de la oficina de ventas tendrían la dirección de correo **`@ventas.dmotos.tld`** y los de comercial **`@comercial.dmtos.tld`**. El resto de los trabajadores quedarían con la dirección **`@dmotos.tld`**.

El sistema que describimos en este documento se ajusta a esta empresa. Decidimos instalarlo. Después de la instalación, pasamos a configurarlo.

Para comenzar revisamos la lista que la administración de la empresa nos dio con los usuarios que necesitan correo electrónico:

```
Departamento de Ventas (3 empleados)
   1. Lilibet       lili@ventas.dmotos.tld
   2. Maria         mari@vnetas.dmotos.tld
   3. Odenia        ode@ventas.dmotos.tld

Departamento Comercial (1 empleado)
   1. Liliana       lili@comercial.dmotos.tld

Resto de la empresa (6 empleados)
   1. Alain         al@dmotos.tld
   2. Lili          lili@dmotos.tld
   3. Alfredo       fred@dmotos.tld
   4. Guillermo     guille@dmotos.tld
   5. Luis          luis@dmotos.tld
   6. Brian         brian@dmotos.tld
```

Con esta lista en mano, nuestro primer paso es decirle a nuestro MTA que puede recibir mensajes para estas direcciones de correo.

Así que creamos un fichero para almacenar las direcciones. Pensando en un futuro crecimiento de la empresa creamos un fichero para cada dominio que vamos a utilizar.

Ej.

Para las direcciones de correo que tengan el dominio definido por defecto (dmotos.tld) creamos el fichero de texto:

/etc/postfix/vmailbox

Para las direcciones de correo que tengan el dominio virtual "ventas.dmotos.tld" creamos el fichero de texto:

/etc/postfix/vmailbox_ventas

Para las direcciones de correo que tengan el dominio virtual "comercial.dmotos.tld" creamos el fichero de texto:

/etc/postfix/vmailbox_comercial

A continuación editamos cada uno de estos ficheros de textos y le adicionamos la información correspondiente. La estructura de los ficheros es: primero la dirección de correo y luego, separado por espacio o tabulador, un valor cualquiera (generalmente utilizamos el nombre completo del usuario).

/etc/postfix/vmailbox

```
al                  Alain
lili                Lili
fred                Alfredo
guille              Guillermo
luis                Luis
brians              Brians

# Nota: En este caso no hace falta especificar el dominio del
# usuario. Se toma el dominio por defecto especificado en el
# fichero de configuración /etc/postfix/main.cf.
```

/etc/postfix/vmailbox_ventas

```
lili@ventas.dmotos.tld       Lilibet
mari@ventas.dmotos.tld       Maria
ode@ventas.dmotos.tld        Odenia
```

/etc/postfix/vmailbox_comercial

```
lili@comercial.dmotos.tld    Liliana
```

Luego que tenemos las direcciones de correo en cada uno de sus ficheros correspondientes, creamos las bases de datos correspondientes a cada uno. Para eso ejecutamos los comandos siguientes:

```
postmap /etc/postfix/vmailbox
postmap /etc/postfix/vmailbox_ventas
postmap /etc/postfix/vmailbox_comercial
```

Siempre que cambiemos el contenido de alguno de estos ficheros es necesario actualizar la base de

datos correspondiente ejecutando el comando **postmap** y el nombre del fichero que actualizó. De lo contrario sus cambios no tomarán efecto para el MTA Postfix.

Listo!! Con esto ya el MTA permitirá que los mensajes dirigidos a las direcciones especificadas anteriormente puedan entrar al sistema para ser procesados y luego enviados a su buzón de destino.

Buzón de destino ? cuál buzón de destino ? dónde están ?

Claro, ahora necesitamos crear los buzones que archivarán los mensajes para las direcciones de correo que permitimos. Para eso hacemos uso del comando **cyradm** como vimos en la sección: "4.2.2 Adminsitración de los buzones de correo":

```
cm user/al
cm user/lili
cm user/fred
cm user/guille
cm user/luis
cm user/brians
cm user/lili@ventas.dmotos.tld
cm user/mari@ventas.dmotos.tld
cm user/ode@ventas.dmotos.tld
cm user/lili@comercial.dmotos.tld
```

Si le vamos a fijar cuotas de 20 megas a cada uno de los usuarios ejecutamos los comandos:

```
setquota user/al 20000
setquota user/lili 20000
setquota user/fred 20000
setquota user/guille 20000
setquota user/luis 20000
setquota user/brians 20000
setquota user/lili@ventas.dmotos.tld 20000
setquota user/mari@ventas.dmotos.tld 20000
setquota user/ode@ventas.dmotos.tld 20000
setquota user/lili@comercial.dmotos.tld 20000
```

Y después que el correo está en el buzón, ¿ Cómo lo recoge el usuario ?

El usuario recoge los mensajes de correo haciendo uso de los protocolos IMAP o POP3.

Para que el usuario pueda recoger el correo es necesario que introduzca un nombre de usuario y contraseña que lo identifiquen ante el buzón para el cual desea recuperar los mensajes. Estos datos son necesario especificarlos en la base de datos **/etc/sasldb2** haciendo uso del comando **saslpasswd2**, como explicábamos más arriba en la sección "4.2.3 Administración de la base de datos de usuarios sasldb2".

En el caso de los usuarios virtuales, a la hora de autenticarse es necesario que introduzcan su dirección de correo completa como nombre de usuario. De esta forma Cyrus-Imapd puede identificar de entre todos los buzones virtuales que tiene cual es el que se está solicitado.

Esta es una razón por la cual las personas con cuentas de correo pertenecientes a dominios virtuales necesitan autenticarse con su dirección de correo completa como nombre de usuario.

De esta forma Cyrus-Imapd puede identificar el usuario y el buzón al mismo tiempo cuando es solicitado por un cliente.

Para seguir con nuestro ejemplo, vamos a crear las credenciales de acceso para los usuarios. Para eso ejecutamos los comandos siguientes:

```
saslpasswd2 al
saslpasswd2 lili
saslpasswd2 fred
saslpasswd2 guille
saslpasswd2 luis
saslpasswd2 brians
saslpasswd2 lili@ventas.dmotos.tld
saslpasswd2 mari@ventas.dmotos.tld
saslpasswd2 ode@ventas.dmotos.tld
saslpasswd2 lili@comercial.dmotos.tld
```

En este punto ya tenemos la configuración básica de un servidor de correo con dominios virtuales corriendo satisfactoriamente.

Para iniciar los servicios ejecutamos los comandos siguientes:

```
service named start
service cyrus-imapd start
service postfix start
```

Ahora solo nos resta configurar los clientes de correo a los usuarios para que puedan recibir y enviar correos desde sus estaciones de trabajo.

Para configurar los clientes de correo algunos datos básicos son:

1. Servidor que recibe los correos (IMAP/POP3) : **mail.dmotos.tld**
2. Servidor que envía los correos (SMTP) : **mail.dmotos.tld**
3. Nombre de usuario.
4. Contraseña de usuario correspondiente.

Nota: Es necesario que en la configuración de la interfase de red y el resolver de la

computadora cliente estén correctamente configurados.

En caso que necesite que los usuarios revisen el correo a través de la web, instale un servidor web y un cliente de correo web para ello. Para más información consulte la sección "5. Instalar y configurar Squirrelmail".

8. Resumen

A la hora de administrar el sistema necesitamos comprender que nuestro sistema de correo electrónico está compuesto por cuatro componentes.

5. Un servidor de nombres de dominio (Bind).
6. El Agente de Transferencia de Correos (Postfix).
7. El servidor de Buzones de correo y acceso a ellos (Cyrus-Imapd)
8. Una base de datos con los nombres de usuario y contraseña de cada uno de los usuarios (SASL).

Para administrar nuestro sistema es necesario atender cada una de estas partes. Si una de estas partes está mal configurada o la desatendemos, nuestro sistema de correo puede que no funcione correctamente.

En esta configuración, cuando un mensaje llega a nuestro dominio el MTA lo recibe y lo evalua. Si el mensaje es aceptado, el MTA entrega el mensaje al programa que se encarga de almacenarlo. Por último cuando los clientes intentan abrir su buzón de correo, el programa que maneja los buzones consulta la base de datos donde tiene los nombres de usuarios y contraseñas para verificar las credenciales que el cliente pasó. Si las credenciales que utilizó el usuario coinciden con las especificadas en la base de datos entonces el usuario tendrá acceso a los mensajes de correo correspondientes.

Esta es una instalación muy básica de un servidor de correo electrónico con buzones virtuales utilizando Bind, Postfix, Cyrus-Imapd y SASL. Todo el sistema se instaló y configuró sobre la distribución CentOS-5.

9. Enlaces Relacionados

- http://www.centos.org/
- http://www.isc.org/bind.html
- http://www.postfix.org/
- http://asg.web.cmu.edu/cyrus