

# Zimbra

## Comandos



para la ejecución de estos comandos hay que primero validarse como el usuario zimbra

```
su - zimbra
```

Para ver el estado del servidor

```
zmcontrol status
```

Para parar o arracnr zimbra

```
zmcontrol start/stop
```

Para saber la versión

```
zmcontrol -v
```

## Configurar un proxy de salida

Globalmente

```
zmprov mcf zimbraHttpProxyURL <ip>:<puerto>
```

Por servidor

```
zmprov ms SERVERNAME zimbraHttpProxyURL <ip>:<puerto>
```

Para que el antivirus se actualize a través del proxy hay que editar el fichero

```
vim /opt/zimbra/conf/freshclam.conf.in
```

y cambiar

```
# Proxy settings
# Default: disabled
HTTPProxyServer miproxy
HTTPProxyPort 3128
#HTTPProxyUsername myusername
#HTTPProxyPassword mypass
```



OJO el fichero a modificar es el freshclam.conf.in y no el freshclam.conf

Para saber si el antivirus se está actualizando correctamente

```
less /opt/zimbra/log/freshclam.log
```

## Listas de distribución

Una vez creada la lista de distribución y añadidos los usuarios, debemos asignar a la misma un/unos usuarios propietarios de la lista.

Estos usuarios deberán de refrescar su navegador y en la pestaña de contactos → lista de correo → botón derecho sobre la lista de correos de la que es propietario → editar lista de correo.

Se abre una ventana en la pestaña de propiedades de la lista podemos definir parámetros como quien puede enviar correos a dicha lista de distribución o gestionar las altas y bajas de usuarios para esa lista concreta.

## Activar chequeo de SPF en Zimbra

Ejecutar todo como usuario zimbra

Comprobar si ya está corriendo policyd:

```
zmprov gs `zmhostname` zimbraServiceEnabled
```

Si no está corriendo activarlo:

```
zmprov ms `zmhostname` +zimbraServiceEnabled cbpolicyd
```

Activar chequeo de SPF

```
zmlocalconfig -e cbpolicyd_module_checkspf=1
```

Crear /tmp/check-spf.sql con el contenido:

```
BEGIN TRANSACTION;
INSERT INTO "checkspf"
(PolicyID,Name,UseSPF,RejectFailedSPF,AddSPFHeader,Comment,Disabled) VALUES
(6,"SPF Policy",1,1,1,"Zimbra CheckSPF Policy",0);
COMMIT;
```

Importar el fichero en la base de datos:

```
sqlite3 /opt/zimbra/data/cbpolicyd/db/cbpolicyd.sqlitedb < /tmp/check-spf.sql
```

Ahora cambiamos las puntuaciones para que el SPF-FAIL tenga mayor peso que por defecto editando `/opt/zimbra/data/spamassassin/localrules/local.cf` y añadiendo:

```
# SPF Check
score SPF_SOFTFAIL 2.000
score SPF_FAIL 10.000
score SPF_HELO_FAIL 10.000
```

Para que los cambios se apliquen debemos reiniciar:

```
zmcontrol restart
```

## Crear DKIM

En `/root/scripts/activarKIM.sh` podemos generar un script para generar el DKIM que contenga lo siguiente:

```
#!/bin/bash
/opt/zimbra/libexec/zmdkimkeyutil -a -d dominio.org
```



Para comprobar el SPF y el DKIM → <http://www.mail-tester.com/spf-dkim-check>

## Certificado de Servidor

En `/root/scripts/regenerarcert.sh` creamos el siguiente fichero para generar el certificado del servidor

```
#!/bin/bash
#####
#####
# Regenerate SSL Cert
#####
#####
su - zimbra -c 'zmlocalconfig -e ssl_allow_untrusted_certs=true'
su - zimbra -c 'zmcontrol stop'
rm -rf /opt/zimbra/ssl/*
rm -rf /opt/zimbra/ssl/.rnd
/opt/zimbra/java/bin/keytool -delete -alias my_ca -keystore
/opt/zimbra/java/jre/lib/security/cacerts -storepass changeit
/opt/zimbra/java/bin/keytool -delete -alias jetty -keystore
/opt/zimbra/mailboxd/etc/keystore -storepass `su - zimbra -c 'zmlocalconfig
-s -m nokey mailboxd_keystore_password'`
nano /opt/zimbra/bin/zmcertmgr

# Find line
# SUBJECT="/C=US/ST=N\A/L=N\A/O=Zimbra Collaboration Suite/OU=Zimbra
```

```
Collaboration Suite/CN=${zimbra_server_hostname}"
# and change to your company name

# then find and change you want value days expire cert validation_days=365
to validation_days=18250
# save /opt/zimbra/bin/zmcertmgr

/opt/zimbra/bin/zmcertmgr createca -new
/opt/zimbra/bin/zmcertmgr deployca -localonly
/opt/zimbra/bin/zmcertmgr createcrt self -new
/opt/zimbra/bin/zmcertmgr deploycrt self

su - zimbra -c 'zmcontrol start'

/opt/zimbra/bin/zmcertmgr deploycrt self
/opt/zimbra/bin/zmcertmgr deployca

su - zimbra -c 'zmupdateauthkeys'
/opt/zimbra/bin/zmcertmgr viewdeployedcrt

#####
#####
```

## Enlaces

- <http://cygnux.org/2012/11/autenticacion-zimbra-8-active-directory/>
- <https://www.jorgedelacruz.es/category/zimbra/>
- <http://endebian.wordpress.com/2013/03/13/z-push-en-zimbra-8/>
- <http://www.nathanmino.com/2013/04/12/upgrade-zimbra-network-edition-appliance-to-open-source-edition/>
- <http://www.cadinor.com/blog/zimbra-distribution-list/#more-276>

From:

<http://intrusos.info/> - **LCWIKI**

Permanent link:

<http://intrusos.info/doku.php?id=aplicaciones:zimbra&rev=1423659963>

Last update: **2023/01/18 13:51**

