DOCUMENTO

TROUBLESHOOTING PLATAFORMA ZIMBRA

Caracas, 04 de Marzo de 2024

INDICE

1. DOCUMENTO CONFIDENCIAL

El contenido de este documento se destinará exclusivamente para análisis de **CANTV** no siendo permitida la divulgación a otros que no sean personas autorizadas por **ITECH-HC**.

ITECH-HC y **CANTV** se comprometen a mantener confidenciales todos los datos e informaciones, a la cual tengan acceso en razón de este documento.

Este documento es propiedad de **ITECH-HC**, no siendo permitido el uso, hacer copias o divulgación de todo o parte del contenido, para cualquier otro propósito que no sea el de evaluación de la propuesta, sin autorización previa y por escrito de **ITECH-HC**

Todas las premisas asumidas en la elaboración de esta Propuesta son estrictamente fundadas en informaciones suministradas por **CANTV**

Cualquier alteración que sea realizada en el contenido de la información suministrada, así como la emisión / publicación de cualquier documento que afecte directa o indirectamente las premisas aquí referidas y definidas, implicarán revisión de las condiciones de la propuesta por **ITECH-HC** en este material.

2. OBJETIVO

El siguiente documento describe las fallas concurrentes y sus soluciones en la plataforma de correo zimbra versión 10 (Daffoil) implantada en Cantv.com.ve. Dependiendo del tipo de problema, la solución será aplicada bajo el entorno grafico (GUI) o bajo la consola Linux (CLI).

Consideraciones Generales – Conexiones a consolas administrativas.

- Solución aplicada bajo el entrono gráfico GUI.

URL de sesión administrativa:

DNS:

https://zimbraloggerpro01.cantv.com.ve:7071

Sin DNS

https://10.2.37.175:7071

El usuario de sesión debe contar con los permisos administrativos, ser recomienda un usuario con administración Global.

- Solución aplicada bajo consola Linux (CLI)

EL usuario que aplique la solución debe existir en el destino (servidor que presenta la falla) y tener privilegios de "su" a root,

Una vez identificado el servidor que presenta la falla, a través de un cliente SSH conéctese con un usuario existente en dicho servidor, puerto 22 default:

#> ssh usuario@(FQDN o dirección ip del servidor)

Establecida la sesión, cámbiese a root y luego a usuario zimbra

#> sudo su -

#> su - zimbra

Establecida la sesión con el usuario zimbra puede aplicar la solución.

Observación:

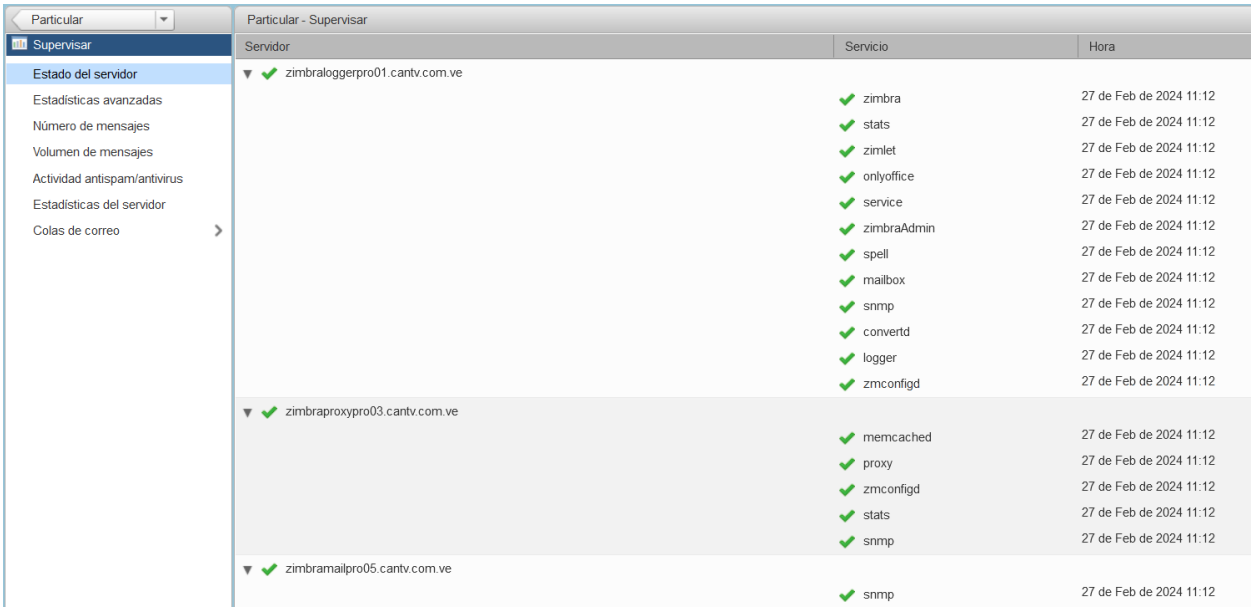
Algunos comandos se aplican con usuario zimbra y otros con root, según sea el caso.

Consideraciones Generales – Identificación de falla a través de la GUI.

A través del entorno gráfico se puede determinar de forma directa el problema y el servidor que la presenta.

Establecida la sesión a través de la GUI puede observar el estado del servicio en toda la arquitectura.

En la columna Runtime, el campo servicio se observa un check de color verde el cual indica que no existe ningún proceso con problemas en ningún servidor, para observarlo mas detalladamente pulse sobre supervisar en el panel de menú a la izquierda.



Aquí observará los servidores que integran la arquitectura con sus distintos procesos, el check de color verde indica que el proceso este "ok", es caso de que el check sea una "X" de color rojo nos informa que dicho proceso en ese servidor tiene problemas.

Recomendación:

Una vez observada la X en color rojo espere entre 1 o 2 minutos y actualice la página, si el problema persiste, tome las acciones necesarias para levantar el proceso en el servidor identificado con la falla.

FALLAS CONCURRECTES Y SUS SOLUCIONES.

1.- Falla de procesos, Identificación de falla a través de la GUI.)

Sea cual sea el proceso observado con un check "X" de color rojo, establezca conexión con el servidor que identifica la falla a través de la consola CLI (Consideraciones Generales – Conexiones a consolas administrativas)

Solución.

Una vez conectado al servidor que presenta la falla y estando bajo usuario zimbra, ejecute:

#>zmcontrol stop

Luego, ejecute

ps -fea | grep -i zimbra (identifica una vez detenido el servicio que procesos siguen ejecutándose)

proceda a la detención forzada del proceso

kill – 9 (# de procesos)

vuelva a ejecutar:

ps -fea | grep -i zimbra (no debe existir corriendo procesos bajo el usuario zimbra)

procesa a levantar el servicio

#>zmcontrol start

2.- Problemas en las colas de correo.

Problemas presentes solo en los servidores MTA, imposibilidad de entrega de correo, Interno o Externo.

Interno: problemas en él envió de correo a cuentas de sus propios dominios:

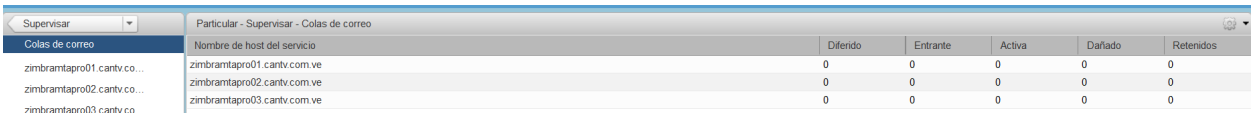
Externo: problemas en él envió de correo a cuentas de otros dominios:

Visualización de las colas.

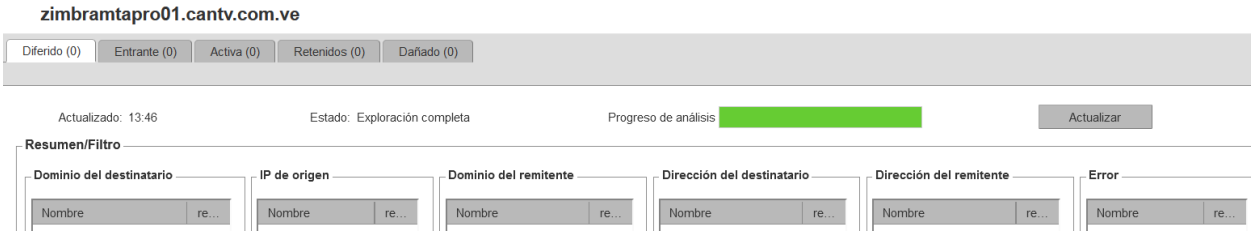
Entorno grafico GUI.

Establezca sesión bajo el entorno grafico con usuario con privilegios, en el panel de menú del lado izquierdo puse sobre:

Supervisar -> Colas de correo.



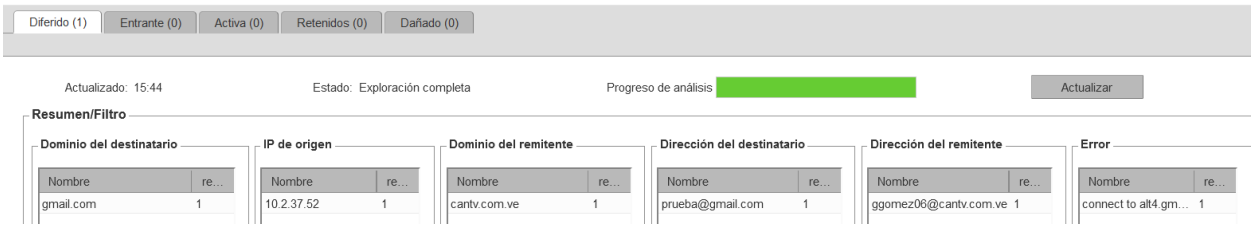
Como puede observar solo muestra los servidores MTA, pulse sobre uno de ellos



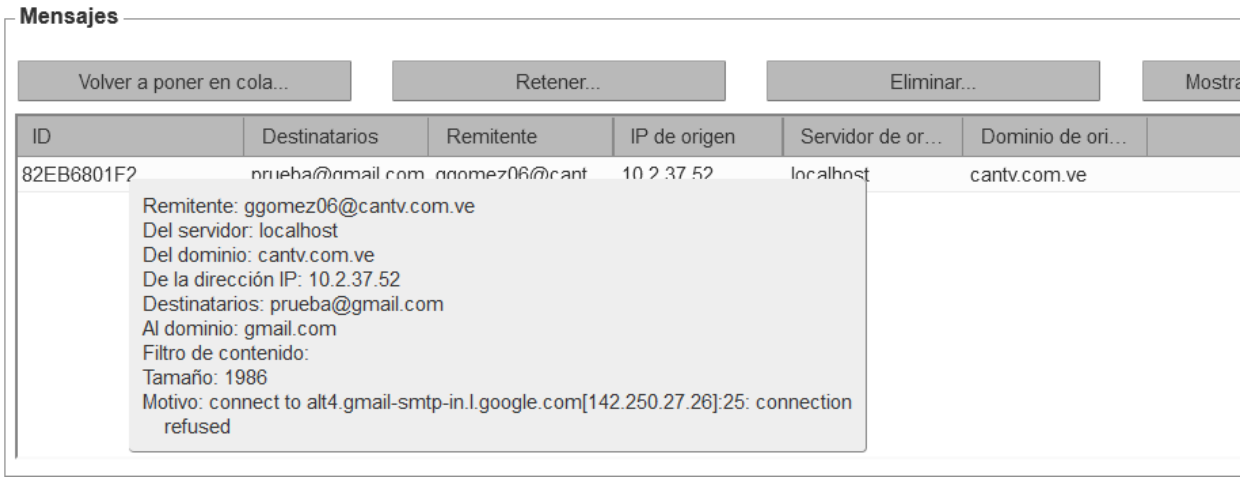
Cambios en los estados de las colas:

Cuando el MTA recibe un correo llega a la cola incoming (entrante) pasa a la cola active (activa) y es aquí donde se aplican todas las políticas, una vez terminadas el proceso smtp intenta sacar el correo hacia su destino, si por algún motivo no lo pudo enviar lo coloca en la cola defer (Diferido) y cada cierto tiempo (máximo 48 horas continuas) realiza reintentos hasta enviarlo a su destino, de no poderlo enviarlo durante ese periodo el sistema envía una notificación al origen informándole al usuario que el correo no se pudo ser entregado donde se exponen los motivos.

Ejemplos e interpretación



Observamos que existe un correo en diferidos, nos ubicamos en la parte de abajo, Coloque el apuntador del ratón sobre el correo para observar la descripción.



Observe los siguientes campos:

Destinatario: Prueba@gmail.com

Al dominio: gmail.com

Motivo, "connection refuse" conexión rechazada

Como se observa el correo va dirigido hacia un dominio externo Gmail.com (142.250.27.26) pero este rechaza la conexión.

Conclusión:

La plataforma destino Gmail.com tiene problemas para aceptar la conexión del MTA de Cantv.

Caso 2 (correo Interno):

Destinatario: ggomez06@cantv.com.ve

Al dominio: Cantv.com.ve

Motivo, "over quota"

El buzón destino (ggomez06@cantv.com.ve) esta al máximo de su capacidad por tanto no puede recibir el correo.

Conclusión:

Cuando el problema de envío es hacia usuarios internos (Cantv.com.ve), el usuario debe existir en la arquitectura de correo, para validar su existencia, diríjase a la GUI

Pulse sobre administrar -→ Cuentas

En la parte superior, en el campo búsqueda coloque el ID del usuario y pulse enter.

En el resultado de la búsqueda coloque el apuntador del mose sobre el usuario encontrado, sino lo encuentra es que el usuario a quien se le envió el correo no existe o está mal escrito.

La cuenta ggomez06 está en el servidor zimbramail.cantv2.com.ve, ahora a través de la consola CLI, conéctese al MAILBOX y reinicie las tareas, siga el punto (**1.- Falla de procesos, según (Consideraciones Generales – Identificación de falla a través de la GUI.)**

3.- Falla en los proxys – Front de Usuarios.

Todos los usuarios se conectan a través de la URL https://correoweb.cantv.com.ve, este host responde por DNS a la IP del balanceador.

Correoweb.cantv.com.ve A 10.1.218.41

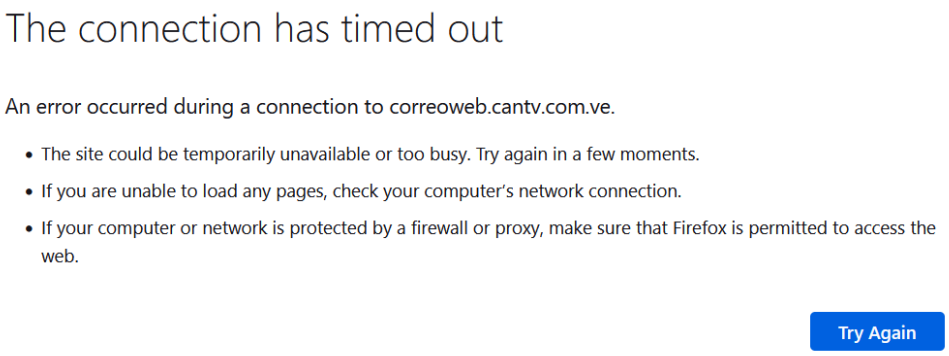
A su vez el balanceador envía la solicitud a uno de los 3 proxys que conforman la arquitectura para la sesión de usuario.

zimbraproxypro01.cantv.com.ve A 10.1.219.46

zimbraproxypro02.cantv.com.ve A 10.1.219.47

zimbraproxypro03.cantv.com.ve A 10.1.219.48

Si el usuario al momento de intentar hacer sesión a través de https://correoweb.cantv.com.ve arroja el siguiente mensaje, indica que uno de los 3 proxys esta caído o no responde.



Como lo indica la imagen el servidor proxy que esta atendiendo al usuario presenta problemas de servicio o de conectividad.

Solución:

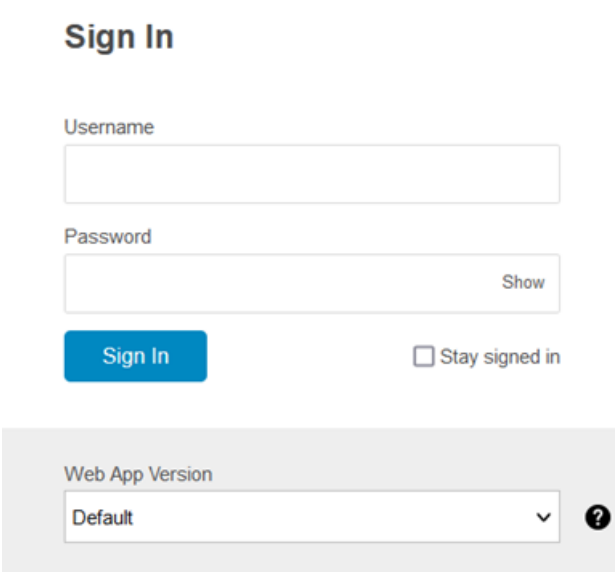
Acceda directamente por URL a cada uno de los proxys:

http://zimbraproxypro01.cantv.com.ve

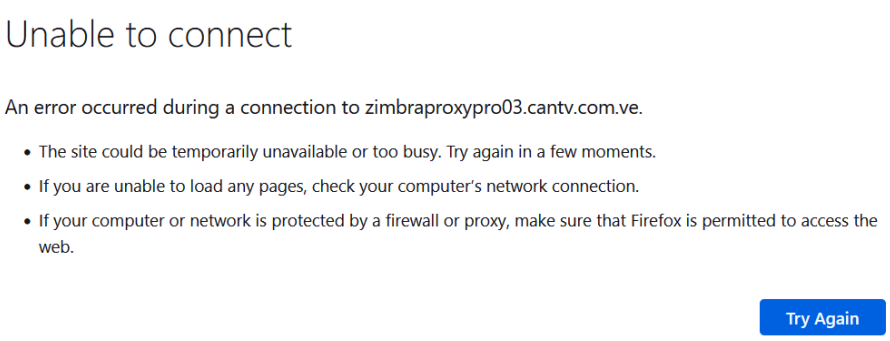
http://zimbraproxypro01.cantv.com.ve

http://zimbraproxypro01.cantv.com.ve

Mensaje si el proxy este operativo:



Mensaje si el proxy tiene problemas, e indica su nombre



Una vez determinado el proxy con problemas ejecute los pasos del punto **1.- Falla de procesos, Identificación de falla a través de la GUI.)**

Hasta apreciar que todos los procesos están running.

zimbra@zimbraproxypro03:~$ zmcontrol start

Host zimbraproxypro03.cantv.com.ve

Starting zmconfigd...Done.

Starting memcached...Done.

Starting proxy...Done.

Starting snmp...Done.

Starting stats...Done.

zimbra@zimbraproxypro03:~$ zmcontrol status

Host zimbraproxypro03.cantv.com.ve

memcached Running

proxy Running

snmp Running

stats Running

zmconfigd Running

Una vez validado que todos los procesos están running, pero el problema persiste, se considera que es un proceso de comunicación.

Servidor con problemas zimbraproxypro03.cantv.com.ve

a- Ejecutar ping al servidor.

zimbra@zimbraproxypro02:~$ ping zimbraproxypro03.cantv.com.ve

PING zimbraproxypro03.cantv.com.ve (10.1.219.48) 56(84) bytes of data.

64 bytes from zimbraproxypro03.cantv.com.ve (10.1.219.48): icmp_seq=1 ttl=64 time=1.24 ms

64 bytes from zimbraproxypro03.cantv.com.ve (10.1.219.48): icmp_seq=2 ttl=64 time=1.48 ms

64 bytes from zimbraproxypro03.cantv.com.ve (10.1.219.48): icmp_seq=3 ttl=64 time=1.11 mss

Con el ping validamos la resolución DNS y el servidor es accesible en la red.

b- Ejecutar Telnet al servidor, puerto 443.

zimbra@zimbraproxypro02:~$ telnet zimbraproxypro03.cantv.com.ve 443

Trying 10.1.219.48...

Connected to zimbraproxypro03.cantv.com.ve.

Escape character is '^]'.

Validamos que el servidor tiene habilitado el puerto 443.

Conclusión:

Si los resultados son diferentes a los mostrados anteriormente indican una falla ya sea por servicio o por conectividad.

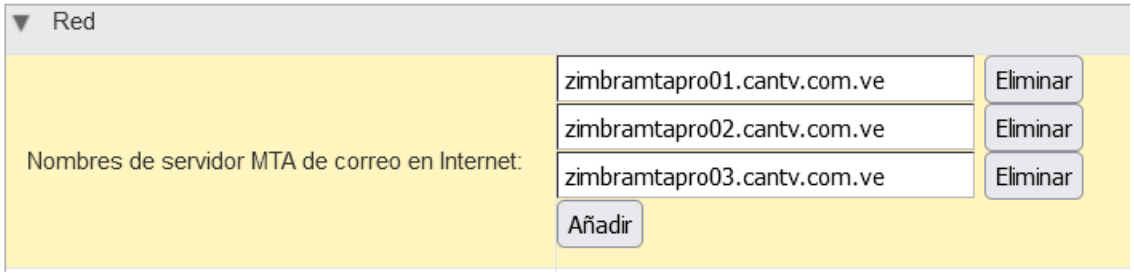
3.- Falla en los MTA – Envió de correo interno y externo.

La arquitectura implantada cuenta con 3 servidores MTA.

zimbramtapro01.cantv.com.ve	A	10.1.219.52
zimbramtapro02.cantv.com.ve	A	10.1.219.53
zimbramtapro03.cantv.com.ve	A	10.1.219.54

Los servidores MAIL son los servidores que alojan las cuentas de usuarios y estos reciben o envían correo a través de los MTA. En la configuración de cada servidor MAIL tienen registrados todos los servidores MTA como se observa a través de la GUI.

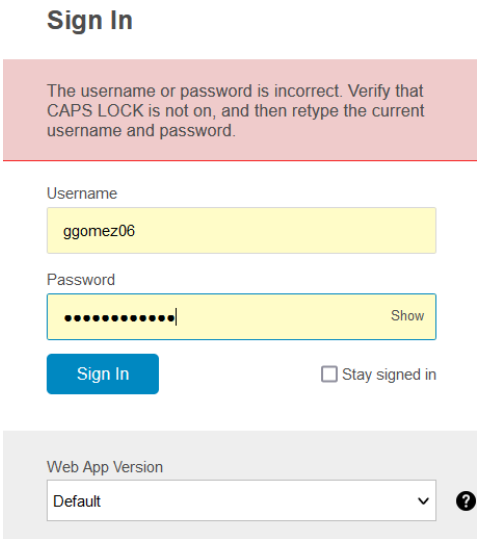
Configuración → Servidores → ejemplo seleccionamos zimbramailpro01.cantv.com.ve → MTA



En este caso el servidor zimbramailpro01.cantv.com.ve utiliza esos MTA para enviar correo, en caso de falla del algún MTA es conveniente sacar (ELIMINAR) de esa lista al MTA que tiene problemas, una vez solucionado se vuelve a agregar.

Si no se efectúa lo antes mencionado, la plataforma sigue funcionando sin problemas, el contratiempo es que el servidor MAIL intentaría enviarle correo al Servidor MTA dañado y al no responderle escogería a otro, produciendo un mínimo retardo.

4.- Falla en la autenticación de Usuario.



Posibles causas:

a- El usuario o clave son incorrectos.

b- El Usuario no existe en el Controlador de Domino (LDAP).

c- El usuario cambio la clave de red.

Soluciones:

a- Validar que el usuario y la clave es la correcta.

b- Solicitar al equipo correspondiente información sobre su cuenta de red.

c- Cuando el usuario cambia de clave de red, por favor esperar mas o menos 30 minutos mientras replica el cambio con el resto de los controladores y vuelva a intentarlo.

3. COMANDOS DE ZIMBRA

Comandos de Zimbra

1.- Comandos de servicio

##

$> su - zimbra

verificar el estado de todos los servicios en zimbra

$> zmcontrol status

detener todos los servicios

$> zmcontrol stop

iniciar todos los servicios

$> zmcontrol start

reiniciar todos los servicios

$> zmcontrol restart

ver la versión de zimbra

$> zmcontrol -v

2.- Comandos individuales de servicio (start, stop, restart, status)

##

Ej: detenemos todos los servicios e iniciaremos uno a uno

$> zmcontrol stop

$> zmcontrol status

Iniciar LDAP server

$> ldap start

$> zmcontrol status

Iniciar MySQL Server

$> mysql.server start

Iniciar zmconfigd

$> zmconfigdctl start

Iniciar MTA (postfix, saslauthd)

$> zmmtactl start

Iniciar Amavis, Antivirus y AntiSpam (amavis, spamassassin, clamav)

$> zmamavisdctl start

$> zmcontrol status

##

Iniciar Mailbox (webmail, panel de administracion, servidores imap y pop3, servidores de filtros)

$> zmmailboxdctl start

Iniciar spell (servidor de ortografía)

$> zmapachectl start

Iniciar monitoreo

$> zmswatchctl start

Iniciar estadísticas

$> zmstatctl start

Iniciar Logger (logs del sistema)

$> zmlogswatchctl start

Reiniciar solo el antivirus

$> zmantivirusctl restart

Reiniciar solo el antispam

$> zmantispamctl restart

3.- zmprov: comando de administración de zimbra

##

Loguearse primero como usuario zimbra

$> su - zimbra

Lista la ayuda general de zmprov

$> zmprov help

Listar la ayuda para gestionar las cuentas

$> zmprov help acount

Consola Interactiva

$> zmprov

prov>

Ver ayuda de cuentas

prov> help account

Salir de la consola interactiva

prov> quit

4.- Administración de Cuentas

##

Obtener listado de todas las cuentas del servidor (todos los dominios) $> zmprov -l gaa

Obtener todas las cuentas de administración $> zmprov -l gaaa

Obtener información de una sola cuenta $> zmprov -l ga

tuxito@dominio.com

Cuentas de un dominio específico

$> zmprov -l gaa dominio.com

Detalle de cuentas de un dominio especifico

$> zmprov -l gaa -v dominio.com

Detalle de cuentas de un dominio especifico con Cuenta, Nombre y Quota

$> zmprov -l gaa -v dominio0.com | grep -e zimbraMailDeliveryAddress -e displayName -e zimbraMailQuota |sed -e "s/zimbraMailDeliveryAddress/Cuenta/" -e "s/displayName/Nombre/" -e "s/zimbraMailQuota/Quota/" Crear una cuenta, con cos default

$> zmprov ca pepito@dominio.com pepitopass displayName "Pepito Pérez"

Crear un usuario con un cos específico ej: gerente

$> cos=`zmprov gc gerente | grep zimbraId: | cut -d ' ' -f2` $> zmprov ca

juanito@dominio.com juanitopass displayName "Juanito Martinez" zimbraCOSId $cos

Crear una cuenta con detalle

$> zmprov ca windozero@dominio.com passwinbugs cn 'Nombre(s) ApMaterno ApPaterno' displayName 'Nombre(s) ApMaterno ApPaterno' givenName 'Nombre(s)' zimbraCOSId $cos

5.- Modificar opciones de una cuenta

Cambiar de password de una cuenta

$> zmprov sp usuario1@dominio.com passnuevo

Modificar un atributo de una cuenta

$> zmprov ma usuario1@dominio.com displayName "Luser Noob 1"

Nota: se puede modificar cualquier atributo del usuario para la lista de atributos ejecutar

$> zmprov -l ga usuario1@dominio.com

6.- Busqueda de cuentas

* Búsqueda por atributos

Se puede buscar las cuentas por un atributo en común

$> zmprov sa parametro=cadena

Buscar todas las cuentas activas

$> zmprov sa zimbraAccountStatus=active

Buscar todas las cuentas bloqueadas

$> zmprov sa zimbraAccountStatus=locked

Buscar en cuales listas se encuentra una cuenta

$> zmprov gam cuenta@dominio.com

##

7.- Listas de correo

Buscar todas las listas, y por dominio

$> zmprov gadl

$> zmprov gadl dominio.com

Crear una lista

$> zmprov cdl

lista@dominio.com

Ver una lista específica

$> zmprov gdl

lista@dominio.com

Encontrar todas las listas de un dominio y sus miembros

$> for i in $(zmprov gadl dominio.com | grep -v abuse | grep -v postmaster | sort) ; do echo

`zmprov gdl $i | grep -e 'mail: ' -e 'zimbraMailForwardingAddress: ' | sed 's/mail/Lista/' | sed

's/zimbraMailForwardingAddress: //'` ; done ;

agregar un miembro a la lista

$> zmprov adlm lista@dominio.com cuenta@dominio.com

Remover un miembro de la lista

$> zmprov rdlm lista@dominio.com cuenta@dominio.com

Borrar una lista

$ zmprov ddl lista@dominio.com

##

8.- Buzones (zmmailbox)

Entrar a la consola interactiva

$> zmmailbox

mbox>

Ver ayuda general del comando

$> zmmailbox help

Ver ayuda de las cuentas

$> zmmailbox help account

Ver ayuda de los mensajes

$> zmmailbox help message

* Tamaño de un buzón

Ver tamaño ocupado del buzón

$> zmmailbox -z -m cuenta@dominio.com gms

Ver el tamaño de las quotas asignadas y ocupadas de todos los buzones

$> zmprov gqu `zmhostname` | awk {'print " "$3" "$2" "$1'}

Revisar mensajes por carpetas en el buzón

$> zmmailbox -z -m cuenta@dominio.com gaf

Borrar una carpeta completa de un buzón

$> zmmailbox -z -m cuenta@dominio.com emptyFolder Junk

Importar mensajes de una carpeta Maildir existente en el INBOX

$> echo addMessage /INBOX /path/to/Maildir/cur | /opt/zimbra/bin/zmmailbox -z -m

cuenta@dominio.com

Buscar un mensaje

$> zmmailbox -z -m cuenta@dominio.com search -t message "prueba"

##

Buscar un mensaje en todas las cuentas

$> zmprov -l gaa | awk '{print "zmmailbox -z -m "$1" search \"linux\" "}' | sh -v

linux es la palabra de búsqueda

Buscar correos anteriores a una fecha: (formato mes/dia/año)

$> zmmailbox -z -m cuenta@dominio.com search -t message "in:INBOX (before: 12/19/13)"

##
##########################

Obtener contenido de un correo

$> zmmailbox -z -m cuenta@dominio.com gm 21940

21940 es el ID del mensaje

Ver contactos:

$> zmmailbox -z -m cuenta@dominio.com gact | less

Vaciar casilla usuario:

$> zmmailbox -z -m accoun@domain.com ef "/Inbox"

Ver correos de una carpeta

$> zmmailbox -z -m cuenta@dominio.com search -l 100 "in:Inbox"

Ver metadata de un correo:

$> zmmetadump -m cuenta@dominio.com -i 26747

Borrar un mensaje

$> zmmailbox -z -m cuenta@dominio.com dm 4543

4543 es el id del mensaje

##
##########################

Comandos para la administración de mailbox:

Anuncio publicitario

. Ver estructura de directorios

zmmailbox -z -m account@domain.com gaf

. Buscar un correo en mailbox de un usuario

zmmailbox -z -m account@doamin.com search -t message "prueba"

. Buscar correos anteriores a una fecha:

zmmailbox -z -m account@domain.com search -t message "in:INBOX (before: 28/07/12)"

. Obtener contenido de un correo

zmmailbox -z -m account@domain.com gm <id> 21940

. Obtener contenido de una conversación

zmmailbox -z -m account@domain.com gc <id> 21940

. Ver contactos:

zmmailbox -z -m account@domain.com gact | less

. Vaciar casilla usuario:

zmmailbox -z -m accoun@domain.com ef "/Inbox"

Ver correos de una carpeta

zmmailbox -z -m account@domain.com search -l 100 "in:Inbox"

. Ver detalle de un correo:

zmmetadump -m account@domain.com -i 26747

Reindexar casilla:

zmprov rim account@domain start

##########

Comprobar estado de indización:

zmprov rim account@domain status

##########

Comandos para la administración de listas de distribución:

Crear lista de distribución

zmprov cdl listname@domain.com

Eliminar una lista de distribución

zmprov rdla listname@domain.com

##

Renombrar una lista de distribución

zmprov rdl listname@domain.com newListName@domain.com

##

Agregar un miembro a una lista

zmprov adlm listname@domain.com member1@domain.com member2@domain.com

##

Remover un miembro de la lista

zmprov rdlm listname@domain.com member1@domain.com

Ver miembros pertenecientes de una lista

zmprov gdl listname@domain.com

Permitir de forma pública el envío a una lista

zmprov grr dl distributionlist@domain.com pub sendToDistList

##

Permitir una dirección para el envio hacia una lista

zmprov grr dl listname@domain.com usr user@domain.com sendToDistList

##
##################

Revocar el envío permitido en una cuenta

zmprov grr dl listname@domain.com usr user@domain.com -sendToDistList

Ver si un usuario tiene permisos para enviar hacia una lista

zmprov ckr dl listname@domain.com user@domain.com sendToDistList

ALLOWED

Via:

target type : dl

target : listname@domain.com

grantee type : usr

grantee : user@domain.com

right : sendToDistList

*** Para que los cambios tomen efecto, siempre se tiene que reiniciar el servicio mta: zmmtactl restart

##
#####################

Comandos para la administración backups y restorea. Backup full

zmbackup -f -a all -s server1.domain.com

Backup incremental

zmbackup -i -a all -s server1.domain.com

Backup full a cuenta

zmbackup -f -a user1@domain.com -s server1

Backup incremental a una cuenta

zmbackup -i -a user1@domain.com -s server1

Restauración full incluyendo incrementales

zmrestore -a all -s server1.domain.com

Restauración full incremental

zmbackup -i -a all -s server1.domain.com - -exclude-hsm-blobs

Restauración full especificando el backup

zmrestore -a user@domain.com -ca -pre "restored_" -restoreToTime "2010/11/14 01:00:00" -lb full-20101113.040005.715

##

Comandos para la administración certificados:

##

Ver fecha de caducidad certificados

/opt/zimbra/bin/zmcertmgr viewdeployedcrt

##

Comandos para la administración de dominos:

Listar dominios configurados

zmprov gad

##

Comandos para administración del servidor

Cambiar la modalidad de acceso

zmtlsctl both (http,https,both,mixed,redirect)

Cambiar el puerto del webmail

zmprov ms `zmhostaname` zimbraMailPort 8081

Añadir segmento de ip en las redes de confianza (mta)

zmprov ms `zmhostname` zimbraMtaMyNetworks "127.0.0.1/32 10.0.0.1/32 192.168.1.15/32"

zmmtactl restart

Comandos para log

Listar todos los envíos realizados por un usuario

grep 'from=<user@domain.com' /var/log/zimbra.log

Buscar envío de usuario a otra cuenta

grep 'user@domain.com> -> .*user2@domain2.com' /var/log/zimbra.log

Buscar correo por destinatario

grep '> ->.*destination@domain.com' /var/log/zimbra.log

Ver autentificaciones sasl

grep sasl_username /var/log/zimbra.log

Ver problemas de autentificación credenciales

grep "authentication failed for" /opt/zimbra/log/audit.log

Ver problemas de cuentas y password

grep "invalid password" /opt/zimbra/log/audit.log

Incrementar el log para una cuenta

zmprov aal user@domain.com zimbra.index debug

zmprov aal user@domain.com zimbra.op debug

zmprov aal user@domain.com zimbra.misc debug

zmprov aal user@domain.com zimbra.filter debug

zmprov aal user@domain.com zimbra.mailbox debug

Remover log

zmprov ral user@domain.com zimbra.imap

##

Rechazar falsos «mail from» en Zimbra

Posted on agosto 5, 2015

Para proteger los entornos Zimbra Collaboration 8.5 en adelante, rechazando los «falsos mail from», se debe aplicar los siguientes comandos:

#su – zimbra

zimbra@server:~$ zmprov mcf zimbraMtaSmtpdRejectUnlistedRecipient yes

zimbra@server:~$ zmprov mcf zimbraMtaSmtpdRejectUnlistedSender yes

zimbra@server:~$ zmmtactl restart

zimbra@server:~$ zmconfigdctl restart

Importar datos entre diferentes versiones de servidores ZCS usando Zimbra Migration Tool

Posted on

Usar la herramienta de Zimbra migration tool **zmztozmig** ipara importar los datos de los cuentas de correos desde un Zimbra Collaboration Server para otro Zimbra Collaboration Server que ejecuten diferentes versiones de ZCS.

El proceso de migración de ZCS server incluyen:

- ❒ Provisionamiento de las cuentas al servidor de destino que ejecuta zmztozmig
- ❒ Editar el archivo de configuración **zmztozmig.conf** ubicado en **/opt/zimbra/conf** en el servidor de destino.
- ❒ Ejecutar **zmztozmig** para importar los datos de las cuentas al servidor de destino.

Ejemplo del archivo de configuración «zmztozmig.conf»

#Source ZCS server IP/name,admin user name and password, server port

SourceZCSServer=192.168.211.20

SourceAdminUser=admin

SourceAdminPwd=PASSADMIN

SourceAdminPort=7071

#Destination/Target ZCS server IP/name,admin user name and password, server port

TargetZCSServer=192.168.211.129

TargetAdminUser=admin

TargetAdminPwd=PASSADMIN

TargetAdminPort=7071

Threads=3

WorkingDirectory=/tmp/ztozmig/mailboxdumps/

FailedDirectory=/tmp/ztozmig/mailboxfailures/

SuccessDirectory=/tmp/ztozmig/successes/

LogDirectory=/opt/zimbra/log/ztozmiglogs

KeepSuccessFiles=FALSE

Domains=zimbra.local

Accounts=all

Herramientas para medir el consumo de ancho de banda Linux

jnettop: Un visualizador del tráfico y el consumo de ancho de banda.

jnettop -i [eth] -x “dst x.x.x.x” -x “src x.x.x.x”

iftop: Proporciona una visión continua e interactiva del tráfico de red que pasa por una interfaz.

#iftop -i eth0

En modo promiscuous:

#iftop -p

Mientras se esté ejecutando el comando puede presionar la tecla:

p: Para mostrar los puertos de las conexiones (remoto y local).

n: Para habilitar/deshabilitar la resolución de nombres (DNS).

l: Para filtrar, arriba de la lista pedirá que ingresar la cadena ha filtrar.

t: Para alternar entre los distintos modos de visualización.

bmon: permite ver el ancho de banda al estilo CACTI, desde la consola.

#bmon

Para activar el visualizador modo gráfico es necesario presionar la tecla g (una vez que se esté ejecutando el programa).

Permitir otras redes en postfix zimbra

Verificar las redes actuales:

postconf mynetworks

mynetworks = 127.0.0.0/8 10.10.130.0/24

Agregar redes

zmprov ms zimbra.example.com zimbraMtaMyNetworks '127.0.0.0/8 10.10.130.0/24 10.10.200.25/32'

postfix reload

Zimbra mensaje de error «Se ha producido un error en el servicio de red»

Si el servidor Zimbra arroja el mensaje de rerror «Se ha producido un error en el servicio de red», puede ser un falso positivo de un ataque DoS, revisar los logs para verificar:

/opt/zimbra/log/sync.log

2013-01-15 15:52:20,426 WARN [qtp1635701107-91:https://10.10.0.54:443/Microsoft-Server-ActiveSync?User=zsupport2&DeviceId=Appl5K0113UN3NR&DeviceType=iPhone&Cmd=FolderSync][name=zsupport2@domain.com;mid=64;ip=71.194.89.54;Cmd=FolderSync;DeviceID=Appl5K0113UN3NR;Version=12.1;] sync - Service exception

com.zimbra.common.service.ServiceException: error while proxying request to target server: HTTP/1.1 503 Service Unavailable

ExceptionId:qtp1635701107-91:https://10.10.0.54:443/Microsoft-Server-ActiveSync?User=zsupport2&DeviceId=Appl5K0113UN3NR&DeviceType=iPhone&Cmd=FolderSync:1358286740426:c5ca7f36bb0a038f
Code:service.PROXY_ERROR Arg:(url, STR,"http://mail.domain.com:80/service/soap/SyncRequest")

cat /opt/zimbra/log/zmmailboxd.out | grep DoSFilter

at org.eclipse.jetty.servlets.DoSFilter.doFilter(DoSFilter.java:299)

/opt/zimbra/log/zmmailboxd.out

2013-01-15 15:57:32.537:WARN:oejs.DoSFilter:DOS ALERT:ip=127.0.1.1,session=null,user=null

Si coinciden los mensajes anteriores, hacer los siguientes ajustes en zimbra:

zmprov mcf +zimbraHttpThrottleSafeIPs 192.168.1.0/24

Reiniciar los servicios

zmmailboxdctl restart

Eliminar archivos con guión «-» adelante

Posted on agosto 31, 2015

Si por ejemplo, se crea un archivo accidentalmente con el nombre: -, -add -l, no se puede eliminar directamente con el comando rm.

Una solución es utilizar el inodo del archivo:

#ls -il *

16777232 drwxrwxr-x 2 – 4096 nov 2 2012 -l

##

Obtenido el número del inodo del archivo, aplicar la búsqueda con find y eliminar:

#find . -inum 16777232 -exec rm -i {} \;

rm: ¿borrar el fichero regular «./–»? (s/n) s

Generar reportes de acceso Squid3 proxy

Posted on septiembre 30, 2015

aptitude install apache2

aptitude install lightsquid

##

Editar la configuración de Apache

vim /etc/apache2/conf-available/lightsquid.conf

<Location "/lightsquid/">

    # add ExecCGI

    Options +ExecCGI

    Require local

    # add IP addresses you permit

Require ip 192.168.0.0/24

vim/etc/apache2/mods-enabled/mime.conf

line 219: Descomentar la línea y agregar la extensions for CGI

AddHandler cgi-script .cgi .pl

##

Habilitar el módulo y einiciar los servicios de apache2

root@prox:~# a2enmod cgi

Enabling module cgi.

To activate the new configuration, you need to run:

service apache2 restart

root@prox:~# a2enconf lightsquid

Enabling conf lightsquid.

To activate the new configuration, you need to run:

service apache2 reload

root@prox:~# service apache2 restart

* Restarting web server apache2

...done.

Generar los reportes

root@prox:~# /usr/share/lightsquid/lightparser.pl

reports are generated daily by /etc/cron.d/lightsquid

Para recolectar información de navegación por direcciones IP, habilitar:

$ip2name="ip" en lightsquid.cfg

Para generarlo por usuarios autenticados:

$ip2name="squidauth" en lightsquid.cfg