Rif. j505838490
Caracas – Venezuela.

## Configuración Final

Una vez finalizada la instalación de los servidores Zimbra 10.1 en varios nodos, se deben configurar las siguientes funciones:

Para la administración remota y la administración de colas de postfix, las claves ssh se deben completar manualmente en cada servidor.

Si el logger está instalado, configure los archivos de configuración de syslog en cada servidor para permitir que las estadísticas del servidor se muestren en la consola de administración y, a continuación, habilite el host de monitorización del registrador. Las estadísticas del servidor incluyen información sobre el recuento de mensajes, el volumen de mensajes y la actividad antispam y antivirus.

Zimbra Collaboration envía un usuario zimbra predeterminado con una contraseña deshabilitada. Requiere acceso a esta cuenta a través de la autenticación de clave pública ssh. En la mayoría de los sistemas operativos, esta combinación es aceptable, pero si ha modificado las reglas de correo no deseado para no permitir ningún acceso ssh a las cuentas deshabilitadas, debe definir una contraseña para la cuenta zimbra UNIX. Esto permitirá la autenticación de clave ssh para verificar las colas remotas.

**Configurar las claves SSH**

Para completar las claves SSH, realice lo siguiente como usuario de Zimbra (sudo su - zimbra) en cada servidor:

zmupdateauthkeys

La clave se actualiza en
/opt/zimbra/.ssh/authorized_keys.

Rif. j505838490
Caracas – Venezuela.

**Habilitar la visualización de estadísticas del servidor**

Para que las estadísticas del servidor se muestren en la consola de administración, se deben modificar los archivos de configuración de syslog.

Zimbra Collaboration admite el syslog predeterminado de un sistema operativo compatible. Según el sistema operativo que utilice, los pasos que se describen en esta sección podrían no ser correctos. Consulte la documentación de su sistema operativo para obtener información específica sobre cómo habilitar syslog.

En cada servidor, como root, escriba /opt/zimbra/libexec/zmsyslogsetup

Esto permite que el servidor muestre estadísticas.

En el servidor donde está instalado el logger, debe habilitar rsyslog para registrar estadísticas de máquinas remotas:

Rsyslog
Elimine los comentarios de las siguientes líneas en /etc/rsyslog.conf

Ubuntu 22.04 LTS

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
```

Reinicie rsyslog
systemctl restart rsyslog.service
systemctl status rsyslog.service

rsyslog RHEL or CentOS

Descomente las siguientes líneas en `/etc/rsyslog.conf`.

```
# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514

# Provides TCP syslog reception
#$ModLoad imtcp
#$InputTCPServerRun 514
```

**Entrenamiento de spam/ham en servidores MTA**

Las nuevas instalaciones de Zimbra 10 limitan el entrenamiento de spam/ham al primer MTA instalado. Si desinstala o mueve este MTA, deberá habilitar el entrenamiento de spam/ham en otro MTA, ya que un host debe tener esta opción habilitada para ejecutar zmtrainsa --cleanup. Para ello, configure zmlocalconfig -e zmtrainsa_cleanup_host=TRUE.