

Redes de Computadoras

Práctica 7

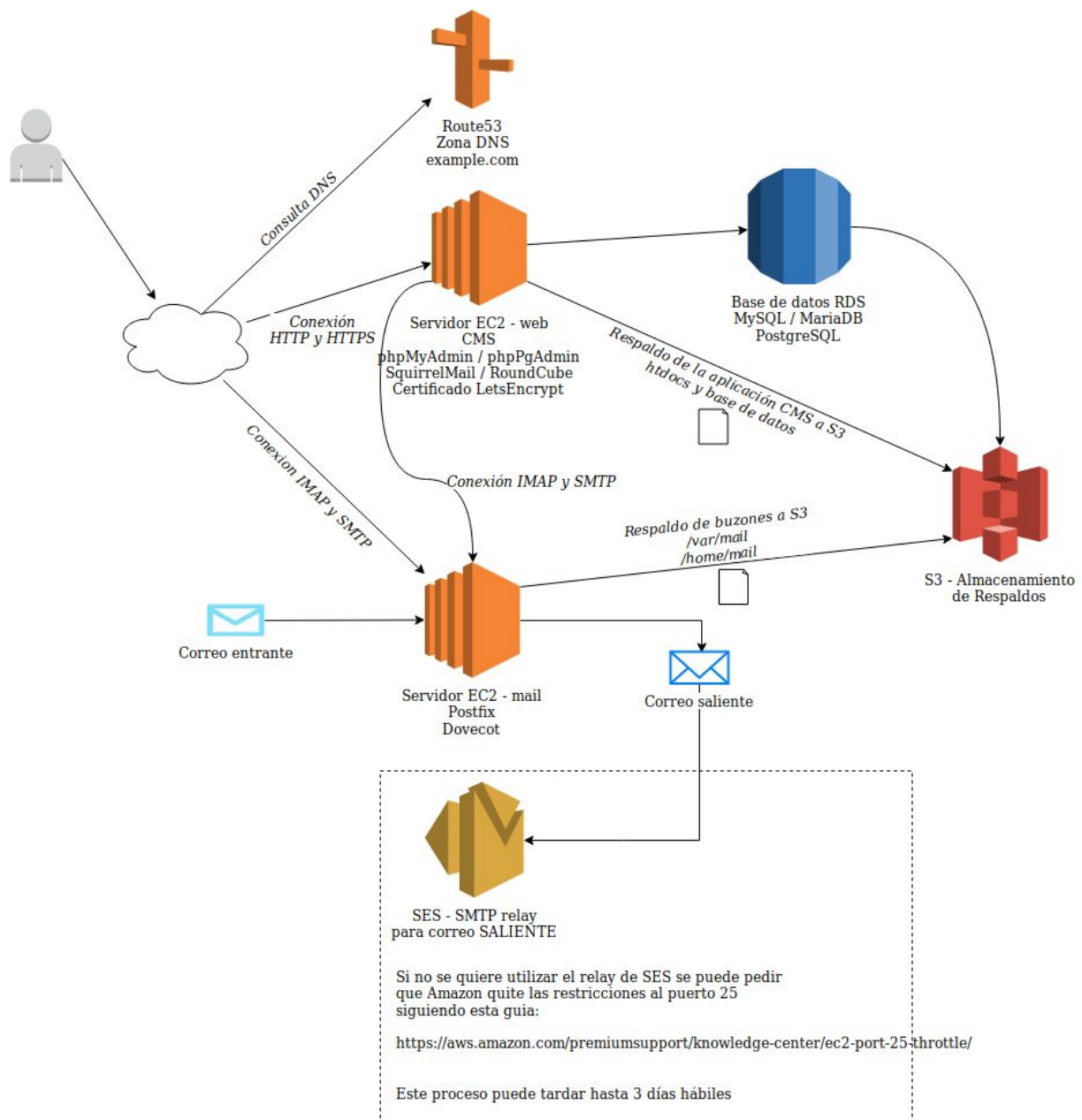
Fecha de entrega: 31 Mayo 2019

Especificaciones

- Esta práctica puede realizarse en equipos de a lo más 4 integrantes.
- Documentar práctica en un archivo README.md con capturas de pantalla de los pasos seguidos.
- Adjuntar en el repositorio los principales archivos de configuración de los servicios.

Objetivo

Implementar la siguiente infraestructura en Amazon Web Services:



Registros DNS

Haciendo uso del servicio Route53, crear los siguientes registros para los servicios implementados:

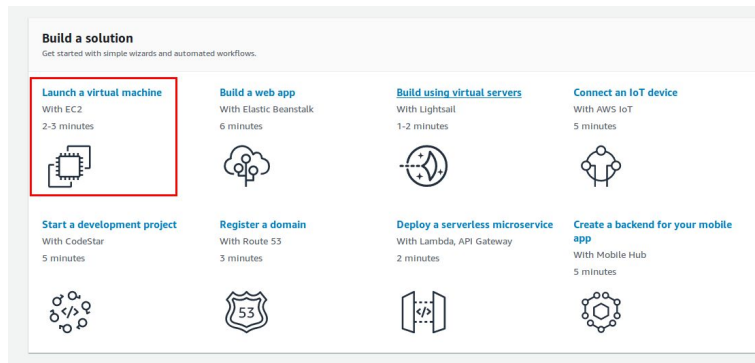
- Registro A principal para que el servidor web que apunte a su dirección IP elástica:
A example.com => IP pública fija de web
- Registro CNAME para www
CNAME www.example.com => example.com
- Registro CNAME que apunte al nombre DNS de la instancia RDS [8]:
CNAME db.example.com => myexampledb.a1b2c3d4wxyz.us-west-2.rds.amazonaws.com
- Registro A para que el servidor de correo que apunte a su dirección IP elástica:
A mail.example.com => IP pública fija de mail
- Registro MX para especificar que el servidor de correo corresponde al dominio:
MX example.com => mail.example.com
- Registro SPF para definir al servidor de correo y el servidor web como hosts desde los cuales puede originarse correo desde el dominio.
SPF example.com => mx, mail.example.com, example.com y www.example.com
- Registros CNAME para los servicios SMTP e IMAP que apunten al nombre DNS del servidor de correo:
CNAME smtp.example.com => mail.example.com
CNAME imap.example.com => mail.example.com
- Los registros DNS que sean necesarios para configurar y validar el certificado de letsencrypt.org. Pueden requerir registros CNAME o TXT.

Adjuntar

- Captura de pantalla de registros creados en la entrega
- Un archivo llamado **dig.log** que contenga la salida de todas las búsquedas de los registros DNS solicitados con el programa **dig**

Servidor web

Crear una cuenta para *AWS Educate* e implementar los servicios indicados creando el número necesario de máquinas virtuales. Para crear una nueva máquina virtual, ingresar a la consola de administración de Amazon y seleccionar el apartado *Launch a virtual machine*:



Asociar una **IP elástica** que sirve para tener una dirección IP homologada estática y crear el registro DNS solicitado.

Base de datos

Base de datos con la que se conectará la aplicación en el servidor web. Puede utilizarse como manejador a MySQL, MariaDB o PostgreSQL. Utilizar el servicio Amazon RDS para su creación [1]:

Certificado SSL

Configurar el agente **certbot** de letsencrypt.org para generar y validar el certificado SSL que deberá ser instalado en el servidor web y el servidor de correo para tener conexiones válidas por SSL y TLS.

Servidor web

Crear una máquina virtual con Ubuntu y asignar una dirección IP elástica para mantener siempre la misma dirección IP pública [2]. Instalar en ella un servidor web (**Apache** o **nginx**) y una aplicación web utilizando un CMS (Drupal, Wordpress o MediaWiki). Configurar la aplicación para que se conecte a la base de datos RDS de manera remota.

Instalar el certificado SSL en `/etc/ssl/certs/server.crt` y la llave privada en `/etc/ssl/private/server.key`. Configurar el servidor web para que lea este certificado y que la conexión por HTTPS sea válida (no deben de agregarse excepciones de seguridad para ingresar al sitio <https://www.example.com/>) [9][10][11]

Servidor de correo

Crear una máquina virtual con Ubuntu e instalar en ella **postfix** para permitir el envío y recepción de correos por medio del protocolo SMTP, así como **dovecot** para que los usuarios puedan acceder a sus correos por medio del protocolo IMAP.

Al igual que al servidor web, se le deberá de asignar una dirección IP elástica al servidor de correo y crear sus registros DNS.

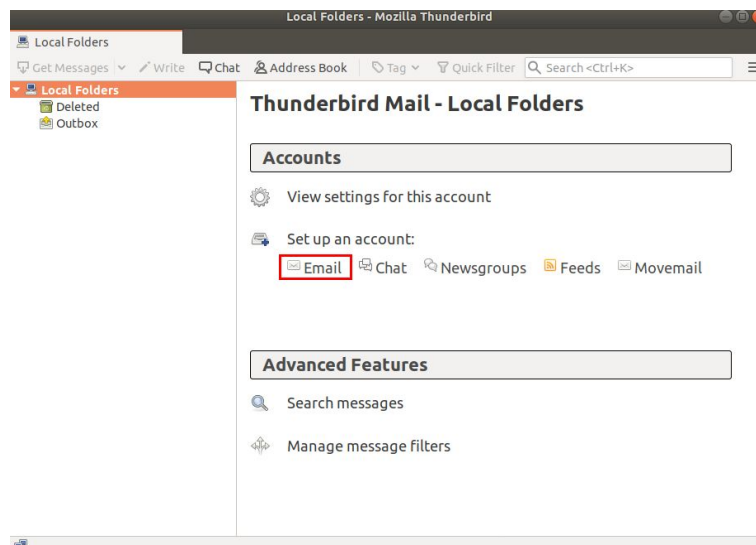
Instalar el certificado SSL en `/etc/ssl/certs/server.crt` y la llave privada en `/etc/ssl/private/server.key`. Configurar el servidor de correo **postfix** y **dovecot** para que lea este certificado y que la conexión por SSL sea válida (no deben de agregarse excepciones de seguridad para conectarse con un cliente de correo) [12][13]

Debido a restricciones que implementa Amazon sobre el puerto 25 para evitar SPAM, se debe de implementar alguna de las siguientes dos soluciones:

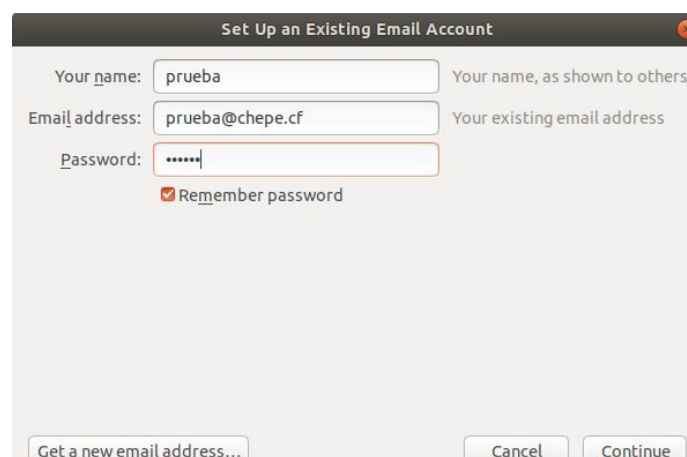
- A. Pedir que Amazon remueva la restricción al puerto 25 [3]. Esto puede tardar hasta 3 días hábiles.
- B. Utilizar Amazon SES como relay SMTP para enviar los correos salientes. Los correos entrantes se reciben normal por el puerto 25 [4][5][6].

Para comprobar que el servidor de correo esté funcionando correctamente, se puede realizar una conexión con con k9 mail en Android o bien con Thunderbird en Windows, macOS o GNU/Linux de la siguiente manera:

Agregar una cuenta de correo:



Ingresar datos del usuario en el servidor:



Ingresar a la configuración manual de la cuenta:

Your name: Your name, as shown to others

Email address: Your existing email address

Password:

☒ Remember password

Configuration found by trying common server names

Incoming: IMAP, imap.chepe.cf, STARTTLS

Outgoing: SMTP, smtp.chepe.cf, STARTTLS

Username: prueba

Manual config Cancel Done

Configurar datos de acuerdo a la configuración de los servicios en el servidor:

Your name: Your name, as shown to others

Email address: Your existing email address

Password:

☒ Remember password

The following settings were found by probing the given server

	Server hostname	Port	SSL	Authentication
Incoming: IMAP	imap.chepe.cf	143	None	Normal password
Outgoing: SMTP	smtp.chepe.cf	25	None	Normal password

Username: Incoming: Outgoing:

Advanced config Cancel Re-test Done

Se mostrará el inbox del usuario, de igual manera se podrán enviar correos desde la cuenta:

Local Folders

Get Messages Write Chat Address Book Tag Quick Filter Search <Ctrl+K>

Local Folders

- Deleted
- Outbox
- prueba@chepe.cf**
 - Inbox

Thunderbird Mail - Local Folders

Accounts

View settings for this account

Set up an account:

Email Chat Newsgroups Feeds Movemail

Advanced Features

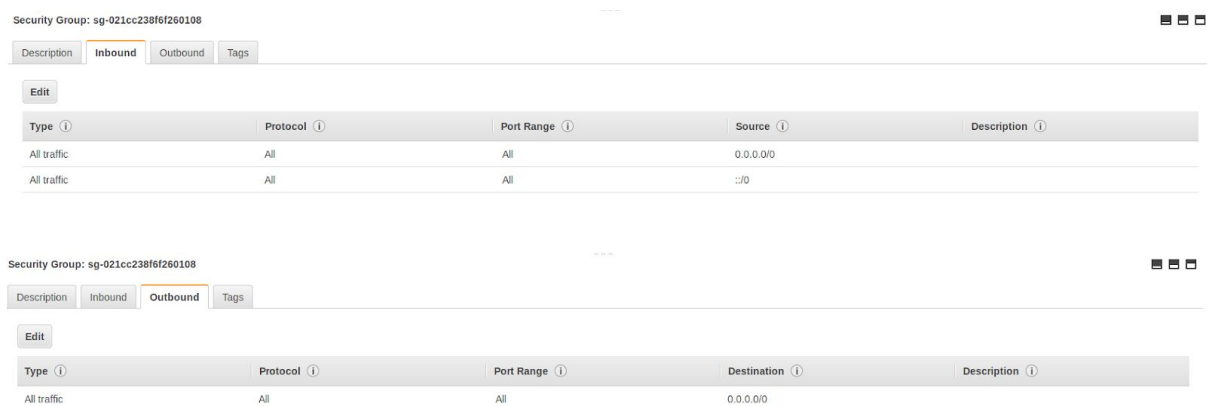
Search messages

Manage message filters

Adicionalmente, se debe de poder cifrar la comunicación con el servidor de correo, es decir, permitir que se utilicen los protocolos SUBMISSION (587/tcp con STARTTLS) e IMAPS (993/tcp con SSL).

Reglas de firewall

Utilizar iptables para crear las reglas de firewall en los servidores web y de correo. Amazon provee **grupos de seguridad** para implementar reglas de firewall para los servidores, por lo que éstas deberán ser configuradas para quitar restricciones en el tráfico de entrada y salida:



The image shows two screenshots of the AWS IAM console's Security Groups page. The top screenshot shows the 'Inbound' tab for a security group with two rules: 'All traffic' from '0.0.0.0/0' and 'All traffic' from ':::0'. The bottom screenshot shows the 'Outbound' tab for the same security group with one rule: 'All traffic' to '0.0.0.0/0'.

Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	:::0	

Type	Protocol	Port Range	Destination	Description
All traffic	All	All	0.0.0.0/0	

De manera que las únicas reglas de firewall en funcionamiento sean las de iptables. Se debe de restringir el tráfico en los servidores únicamente a los puertos necesarios para permitir el funcionamiento de los servicios (tener cuidado de también permitir la comunicación entre ustedes y el servicio de SSH).

Adjuntar las reglas de iptables en entrega, censurando las direcciones IP públicas de los integrantes del equipo, si es que se configuró alguna regla para éstas.

Puntos extra

Respaldo de archivos

Crear respaldos via CRON en el servicio S3 (Simple Storage Service) de lo siguiente:

- Copia del certificado y la llave privada de los servicios.
- Respallos de las configuraciones de los servidores.
- Respallos de la base de datos RDS utilizando **mysqldump** o **pg_dump**.
- Respaldo en archivo.tar.gz del directorio /var/mail
- Respaldo en archivo.tar.gz de los buzones de correo.

Se puede utilizar alguna de las siguientes herramientas para enviar el respaldo a S3

- aws-cli [23] [24]
- duck [25]

- rclone [26]

Administrador web de la base de datos

- Instalar en el servidor web un sitio que permita administrar remotamente la base de datos (phpMyAdmin, phpPgAdmin) que apunte la instancia de RDS (db.example.com).
- Para acceder a este sitio se debe de configurar un VirtualHost [14][15] adicional al creado para el CMS (www.example.com), al cual se debe de poder acceder por medio de otro nombre (e.g. admin.example.com).
- Este nuevo nombre deberá de tener su registro CNAME correspondiente apuntando al servidor donde está hospedado el sitio.

Webmail

- Instalar en el servidor web un sitio que le permita a los usuarios acceder a sus correos del servidor de correo, así como enviarlos (SquirrelMail o Roundcube).
- El sitio debe de configurarse para conectarse a imap.example.com y a smtp.example.com.
- Al igual que en el caso anterior, se debe de crear un nuevo VirtualHost para el sitio, con un nombre (e.g. webmail.example.com) al que se le asigne el registro CNAME correspondiente apuntando al servidor donde está hospedado el sitio.

Referencias

1. <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html>
2. https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html
3. <https://aws.amazon.com/premiumsupport/knowledge-center/ec2-port-25-throttle/>
4. <https://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-an-email-using-smtp.html>
5. <https://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-smtp.html>
6. <https://docs.aws.amazon.com/ses/latest/DeveloperGuide/postfix.html#send-email-postfix>
7. <https://docs.aws.amazon.com/quickstarts/latest/s3backup/welcome.html>
8. <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-rds-db.html>
9. <https://letsencrypt.org/getting-started/>
10. <https://certbot.eff.org/lets-encrypt/ubuntubionic-apache>
11. <https://certbot.eff.org/lets-encrypt/ubuntubionic-nginx>
12. <https://robpickering.com/using-lets-encrypt-tls-certificates-for-smtp-imap-and-http/>
13. <https://upcloud.com/community/tutorials/secure-postfix-using-lets-encrypt/>
14. <https://httpd.apache.org/docs/2.4/vhosts/examples.html>
15. <https://httpd.apache.org/docs/2.4/vhosts/>
16. https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html
17. http://www.postfix.org/BASIC_CONFIGURATION_README.html
18. <https://wiki2.dovecot.org/BasicConfiguration>
19. <https://wiki.dovecot.org/SSL>

20. <https://wiki.dovecot.org/SSL/DovecotConfiguration>
21. <https://roundcube.net/download/>
22. <https://squirrelmail.org/docs/admin/admin-3.html#ss3.1>
23. <https://docs.aws.amazon.com/cli/latest/userguide/install-linux.html>
24. <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-configure.html>
25. <https://cyberduck.io/s3/>
26. <https://rclone.org/s3/>