CAPACITACIÓN
CLOUD COMPUTING

dw training

2021

CONTENIDO

Laboratorio 1: IAM, creación de usuarios y administración de permisos.

Objetivos

- Crear las cuentas de AWS IAM necesarias para administrar tu cuenta de AWS en las aplicaciones.
- Crear el Role necesario para la comunicación entre tus EC2 y S3.
- Agregar y editar Policies para los usuarios IAM y los Roles.

Resumen

En este laboratorio crearás una cuenta de AWS con MFA activado. Una cuenta de IAM con permisos de administrador y un Role con que te permitirá comunicar tus aplicaciones entre los servicios de AWS.

Punto de partida

Entra a tu cuenta de AWS y dirígete a la sección de IAM https://console.aws.amazon.com/iam/home?#/home

Ejecución de Laboratorio:

1. Activar MFA en tu cuenta de AWS

Para activar el servicio de multi-factor authentication (MFA) en tu cuenta root de AWS deberás seguir los siguientes pasos. Deberás tener tu Smartphone a la mano con conexión a Internet.

1. En la pantalla principal del servicio IAM de AWS deberás seleccionar la pestaña Activate MFA on your root account.
2. Da click en el botón Manage MFA que aparece en la sección desplegada.
3. Verás un mensaje de alerta que deberás aceptar para continuar.
4. Selecciona la opción Multi-factor authentication (MFA) en el menú.
5. Presiona el botón azul que dice Activate MFA, verás una cuadro de diálogo con varias opciones.
6. Selecciona la opción Virtual MFA device y da click en el botón Continue.
7. Aparecerá otro cuadro de diálogo y verás los pasos a seguir para activar MFA en tu cuenta.
8. Da click en el enlace Show QR code. Es IMPORTANTE que le tomes una captura de pantalla al código QR para que puedas recuperar tu cuenta en caso de tener algún problema con tu Smartphone.
9. Escanea el código QR desde la app de tu Smarthphone. Una vez escaneado, deberás copiar en los campos MFA code 1 y MFA code 2 dos de los códigos que serán generados por la app automáticamente.
10. Una vez copiados los códigos, presiona el botón Assign MFA.
11. Deberás ver un mensaje de éxito en tu pantalla You have successfully assigned virtual MFA. Da click en el botón Close.

2. Crear Groups y IAM Users

Crear IAM Groups te ayudará a administrar los permisos de los diferentes tipos de usuarios en tu organización. Puedes crear Users y asignarlos a diferentes Groups con diferentes permisos.

- Crea un Group llamado Admins:
    1. Ve a la sección de Groups en la página de IAM https://console.aws.amazon.com/iam/home?#/groups.
    2. Da click en el botón Create New Group. Serás redireccionado al asistente de creación de Groups.
    3. Agrega en nombre Admins en el campo Group Name y da click en el botón Next Step.
    4. Busca la Policy llamada AdministratorAccess en el campo de búsqueda y seleccionala en el cuadro de la izquierda del nombre. Da click en el botón Next Step.
    5. Verás los detalles del Group que estás a punto de crear. Da click en el botón Create Group.

- Crea un User y asignarlo al Group llamado Admins:
    1. Ve a la sección de Users y da click en el botón Add user.
    2. Agrega el nombre de usuario en el campo User name, por ejemplo: *AndyJassy*.
    3. Selecciona el tipo de acceso del usuario, Programatic access y AWS Management Console access.
    4. Selecciona la opción de Custom password que aparece en la parte de abajo. Crea un password que contenga al menos 8 caracteres en total, letras mayúsculas y minúsculas, al menos un número y un carácter especial, ejemplo: !BestC0urse3ver!
    5. Deselecciona la casilla User must create a new password at next sign-in para que el usuario no tenga que hacer un nuevo password cuando inicie sesión por primera vez.
    6. Da click en el botón Next: Permissions.
    7. Selecciona la opción Add user to group y selecciona el Group llamado Admins de la lista. Da click en el botón Next: Tags y después da click en el botón Next: Review.
    8. Verás en tu pantalla un resumen de las características del User que estás a punto de crear. Da click en el botón Create user.
    9. IMPORTANTE: Deberás descargar en archivo .csv con las credenciales del User que acabas de crear. Da click en el botón Close.
    10. Abre un nuevo navegador e intenta iniciar sesion con tu nuevo usuario para confirmar que fue creado correctamente. Deberás tener acceso a todas las secciones de la consola de AWS.

3. Crear un Role para usar los diferentes servicios de AWS

Los Roles te permiten comunicar diferentes servicios de AWS entre sí. En esta serie de pasos crearás un Role para comunicar tus instancias EC2 con S3. De esta manera tus aplicaciones podrán administrar los archivos multimedia guardados en tus Buckets.

1. Entra a tu cuenta de AWS y dirígete a la sección de Roles de IAM https://console.aws.amazon.com/iam/home?#/roles
2. Da click en el botón Create role. Serás redirigido a la pantalla de creación de Roles.
3. Selecciona la opción de AWS service y después selecciona el servicio que usar el Rol que en este caso será EC2.
4. Una vez seleccionado el servicio de EC2, da click en el botón Next: Permission. Aparecerá una lista con todas las Policies predefinidas en AWS. Busca en el campo de búsqueda AmazonS3FullAccess y selecciona la Policy en el cuadro de la izquierda al lado del nombre. Una vez seleccionado presione el botón Next: Tags.
5. Agrega un tag llamado Name en la columna Key y agrega en nombre de tu Role como EC2-Permissions. Da click en el botón Next: Review.
6. Verás una pantalla con todos los detalles del Role que estás a punto de crear. Agrega nuevamente el nombre de tu Role en el campo Role name y da click en el botón Create role.
7. Una vez creado el Role aparecerá en la lista de Roles con el nombre EC2-Permissions

Laboratorio 2: Administración de Buckets y Objetos en AWS S3

Objetivos

- Crear y administrar Buckets y Objects dentro del servicio S3 de AWS.
- Guardar los archivos de configuración de nuestra aplicación web final.
- Administrar los tipos de acceso a los Objects dentro de nuestros Buckets.

Resumen

En este laboratorio crearás un Bucket dentro de S3 para guardar los archivos de configuración de tu aplicación final. También crearás una carpeta para almacenar y sincronizar las imágenes de tu aplicación y le darás acceso público a dichas imágenes para que puedan ser vistas desde Internet.

Punto de partida

Entra a tu cuenta de AWS y dirígete al servicio de S3 https://console.aws.amazon.com/s3/home

Ejecución de Laboratorio:

- Crear un Bucket en S3:

    1. Da click el botón Crear bucket. Aparecerá un cuadro de diálogo donde deberás agregar el nombre del Bucket en el campo Bucket name, recuerda que el nombre del Bucket debe de ser único entre todas las cuentas de AWS.
    2. Una vez que hayas elegido un nombre, debes de seleccionar la Región donde será creado tu Bucket. Elige la región que esté más cercana a tu posición actual. US West (Oregon) o US West (N. California) será la mejor opción en este caso.
    3. Una vez seleccionada la Región da click en el botón de Create. Si el nombre de tu Bucket ya existe verás un mensaje con esta leyenda: *Bucket name already exists*, cambia el nombre hasta que el mensaje no aparezca.
    4. Una vez creado, tu Bucket aparecerá en la lista de Buckets de S3.

- Crear una carpeta para guardar imágenes:

    1. Da click en el nombre del Bucket para ver el contenido del Bucket, deberá estar vacío en este momento.
    2. Da click en el botón Create folder y pon el nombre de images en el campo New folder apareció en la parte de abajo. Da click en el botón Save para guardar la carpeta en el Bucket.
    3. Deberás poder entrar a la carpeta que acabas de crear dando click en el nombre de la carpeta.
- Subir una imagen en la carpeta images de tu Bucket:

    1. Entra a la carpeta images de tu Bucket y da click en el botón Upload.
    2. En el cuadro de diálogo haz click en el botón Add files y selecciona una imagen de tu computadora.
    3. Una vez seleccionada la imagen haz click en el botón Upload. Espera a que la imagen se suba completamente a tu Bucket.
    4. Haz click en el nombre de la imagen que acabas de subir para ver los detalles del Object. Deberás ver la URL del objeto al final de la pantalla con este formato: https://{bucket-name}.s3-{region-name}.amazonaws.com/images/{file-name}.

- Hacer que la imagen sea pública:

    1. Selecciona el Bucket desde la pantalla principal de S3: https://console.aws.amazon.com/s3/home.
    2. Haz click en el botón Edit public access settings y des-selecciona la opción Block all public access que aparece en el cuadro de diálogo.
    3. Da click en el botón Save para guardar la configuración de tu Bucket.
    4. Escribe la palabra confirm en el nuevo cuadro de diálogo y da click en el botón Confirm.
    5. Entra a la carpeta images de tu Bucket y selecciona la imagen que harás pública. Una vez seleccionada la imagen da click en el menú Actions y selecciona la opción Make public. Haz click en el botón Make public en el cuadro de diálogo que apareció.
    6. Da click en el nombre de la imagen y después da click en la URL del objeto, deberás poder ver la imagen desde tu navegador.

Laboratorio 3: Computación en la Nube con EC2.

Objetivos

- Crear una instancia EC2 donde correrá nuestra aplicación web.
- Garantizar la seguridad y las configuraciones necesarias de la instancia EC2.
- Asignar los permisos necesarios a esa instancia para comunicarse con otros servicios de AWS.

Resumen

Crearás una instancia EC2 dentro del plan free tier con los requerimientos mínimos para correr una aplicación web. También asignamos los permisos necesarias para que la instancia EC2 pueda comunicarse con otros servicios de AWS.

Punto de partida

Entra a tu cuenta de AWS y dirígete a la sección de EC2 https://console.aws.amazon.com/ec2

Ejecución de Laboratorio:

- Crea una instancia EC2:
    1. En el panel principal de EC2 haz clic en el botón Launch Instance. Serás redireccionado a la página de creación de instancias EC2.
    2. El primer paso es seleccionar la imagen (Amazon Machine Image (AMI)) que se utilizará para crear la instancia EC2. Busca la imagen con el nombre Amazon Linux 2 AMI y haz clic en el botón Select. Serás redireccionado al siguiente paso.
    3. Selecciona el tipo de instancia que tenga la etiqueta Free tier eligible, por ejemplo: General purpose t2.micro. Una vez seleccionado, haz clic en el botón Next: Configure Instance Details. Serás redireccionado al siguiente paso.
    4. En este paso asegúrate de que el campo Number of instances tenga el valor de 1 para que solo se cree una instancia. En el campo IAM role deberás seleccionar el IAM Role que creamos en el Laboratorio 1 llamado EC2-Permissions.

5. Dirígete al fondo de la pantalla y haz clic en la leyenda Advanced Details. Verás una la sección para agregar los scripts de iniciación de la instancia. Selecciona la opción As text y copia los siguientes comandos en el campo de texto.

```
#!/bin/bash
yum install httpd php php-mysql -y
cd /var/www/html
wget https://wordpress.org/wordpress-5.1.1.tar.gz
tar -xzf wordpress-5.1.1.tar.gz
cp -r wordpress/* /var/www/html/
rm -rf wordpress
rm -rf wordpress-5.1.1.tar.gz
chmod -R 755 wp-content
chown -R apache:apache wp-content
service httpd start
chkconfig httpd on
```

Haz clic en el botón Next: Add Storage. Serás redireccionado al siguiente paso.

6. En la sección Add Storage agregaras un disco duro a to instancia. Para esta aplicación no necesitarás más de 8 gb de almacenamiento, pero puedes agregar hasta 30 gb para mantenerte dentro del Free tier eligible y que esto no genere costo extra en tu cuenta de AWS. Da clic en el botón Next: Add Tags.
7. En la sección Add Tags haz clic en el botón Add Tag y agrega un Tag llamado Name con el valor de Web Server. Haz clic en el botón Next: Configure Security Group.
8. En el paso Configure Security Group selecciona la opción Create a new security group y en el campo Security group name agrega el valor web-security-group y en el campo Description agrega el valor Web Security Group. Haz clic en el botón Review and Launch.
9. Revisa que tu instancia haya sido configurada correctamente y haz clic en el botón Launch.
10. Aparecerá un cuadro de diálogo con el titulo Select an existing key pair or create a new key pair. Elige la opción Create a new key pair y en el campo Key pair name agrega el valor dw-web-key y da clic en el botón Download Key Pair. Se descargará en tu computadora un archivo llamado dw-web-key.pem. **IMPORTANTE:** deberás resguardar el archivo en tu computadora, si lo pierdes no podrás acceder a tu instancia y si alguien más lo toma podrá acceder a la instancia.
11. Da clic en el botón Launch Instances. Deberás ver un mensaje de éxito con la leyenda Your instances are now launching. Da clic en el botón View Instances para ir a la lista de tus instancias EC2.

- Abre los puertos necesarios en el security group. Para que el servidor web pueda ser accedido desde cualquier navegador deberás abrir el puerto 80 en el security group de la instancia de EC2.
    1. Selecciona la instancia Web Server de la lista de instancias EC2. En la pestaña Description de la parte de abajo de tu pantalla, selecciona web-security-group en la sección Security groups.
    2. En la pantalla de Security Groups verás que web-security-group está seleccionado. Dirígete a la pestaña de Inbound que está en la parte de abajo y da clic en el botón Edit.
    3. En el cuadro de diálogo da clic en el botón Add Rule y selecciona la opción HTTP de la lista, deberá aparecer el puerto 80 en la lista de puertos y el source de ese registro deberá ser 0.0.0.0/0, ::/0.
    4. Haz clic en el botón Save y regresa a la pantalla de la lista de instancias EC2.
    5. Selecciona la instancia Web Server y copia la IP pública y pegala en tu navegador. Deberás poder ver la pantalla de bienvenida de una nueva instalación de WordPress.

Laboratorio 4: Configuración y administración de bases de datos en RDS.

Objetivos

Crear una instancia RDS que contenga una base de datos MySQL.

Implementar los mecanismos de seguridad necesarios para proteger tu base de datos.

Conectar la instalación de WordPress a la base de datos MySQL.

Resumen

Crearás una instancia RDS con las capacidades mínimas para poder hostear una base de datos MySQL. La base de datos guardará todos los registros generados por tu sitio en WordPress. Con esta configuración tu base de datos solo será accesada por WordPress y el administrador de base de datos.

Punto de partida

Entra a tu cuenta de AWS y ve la opción de Services y en sección Database haz clic en el link RDS https://us-west-2.console.aws.amazon.com/rds/home

Ejecución de Laboratorio:

- Crea un Security Group para la instancia RDS.
    1. En el menú principal del panel de AWS ve al servicio de EC2.
    2. Haz clic en la opción Security Groups del menú.
    3. Haz clic en el botón Create Security Group y llena los campos con los siguientes valores:
        - Security group name: db-wordpress-sg
        - Description: Wordpress database security group
    4. En la pestaña Inbound haz clic en el botón Add Rule y llena fila con los siguientes valores:
        - Type: MYSQL/Aurora
        - Protocol: TCP
        - Port Range: 3306
        - Source: Custom (En el campo de la derecha comienza a escribir sg- y selecciona web-security-group de la lista que aparecerá)
        - Description: EC2 Wordpress Instance
    5. Haz clic en el botón Create para guardar los cambios. Una vez creado el Security Group deberá aparecer en la lista.
    6. Regresa al servicio de RDS https://us-west-2.console.aws.amazon.com/rds/home

- Crear una base de datos MySQL para el sitio de WordPress.
    1. En la pantalla principal de RDS haz clic en la opción Databases. Después haz clic en el botón Create database, serás redirigido a la pantalla de creación de bases de datos.
    2. Selecciona la opción Standard Create y en la opción Engine type selecciona MySQL, MySQL Community, MySQL 5.7.22.
    3. A continuación en la sección de Templates selecciona la opción Free tier. Esto evitará que se generen cargos extras en tu cuenta de AWS.
    4. En la sección Settings pon los siguientes valores en los campos:
        - DB instance identifier: wordpress-db-instance
        - Master username: admin
        - Master password: S3cUre!pA55word
        - Confirm password: S3cUre!pA55word
    5. Ve a la sección de Additional connectivity configuration y haz clic en el menú Choose VPC security groups, selecciona la opción db-wordpress-sg y remueve la opción default.
    6. Por último haz clic en la sección Additional configuration y llena los campos con estos valores:
        - Initial database name: wordpress_db
        - Enable automatic backups: (deja la casilla des-seleccionada)
    7. Ve al fondo de la pantalla y asegúrate de que en la sección final aparezca esta leyenda: The Amazon RDS Free Tier is available to you for 12 months.
    8. Si todo está correcto, haz clic en el botón Create database. Deberás de ver un mensaje de éxito y tu instancia de base de datos aparecerá en la lista con el Status: Creating.
    9. Deberás esperar un par de minutos hasta que la instancia sea creada completamente.
- Configurar el sitio de WordPress con los datos de conexión a la base de datos.
    1. Una vez que la instancia wordpress-db-instance tenga un Status como Available haz clic en el nombre de la instancia para ver los detalles.
    2. En la sección de Connectivity & security deberás de poder ver los valores de Endpoint y Port. Copia en un documento en blanco los valores de la base de datos, por ejemplo: Endpoint: wordpress-db-instance.xxxxxxxxxxxx.us-west-2.rds.amazonaws.com Port: 3306 Username: admin Password: S3cUre!pA55word Database: wordpress_db
    3. Ve al servicio de EC2 en el menú principal de AWS y selecciona la instancia Web Server. Copia en valor del Public DNS (IPv4) y pegalo en tu navegador y presiona enter. Deberás poder ver la página de configuración de WordPress.
    4. Haz clic en el botón Let's go! y llena los campos con los siguientes valores:
        - Database Name:
        - Username: admin
        - Password: S3cUre!pA55word
        - Database Host: (Pon el Endpoint de tu base de datos)
        - Table Prefix: wp_
    5. Haz clic en Submit. Aparece un mensaje con este título: Sorry, but I can’t write the wp-config.php file.. Copia el código PHP que aparece en la parte de abajo para crear el archivo config.php en tu servidor web.
    6. Entra a tu servidor por medio de la conexión SSH.

- Copia el DNS público de tu servidor web. Para seleccionar tu servidor identifica el valor Public DNS (IPv4).
- Abre un cliente SSH (como PuTTY) o la terminal de Linux o Mac.
- Localiza la llave .pem que descargaste al crear el servidor.
- Cambia los permisos de tu llave .pem en la terminal. chmod 400 your_key_name.pem
- En la terminal usa este comando para hacer la conexión SSH a tu servidor web: ssh -i "your_key_name.pem" ec2-user@ec2-your-public-dns.us-west-2.compute.amazonaws.com

7. Una vez dentro del servidor ejecuta los siguientes pasos en la terminal: cd /var/www/html sudo touch wp-config.php
8. Abre el archivo wp-config.php dentro del servidor y pega el código PHP de la pantalla de wordpress. Puedes usar el editor vim o nano para esta tarea. Guarda el archivo y regresa a la pantalla de configuración de WordPress en tu navegador.
9. Haz clic en el botón Run the installation. Si todo está correcto, serás redireccionado a la pantalla con el mensaje: Welcome to the famous five-minute WordPress installation process!.
10. Agrega los valores que tú desees en los campos de configuración. Solo asegúrate de guardarlos para poder administrar el sitio de wordpress. Por ejemplo:
    - Site Title: Example Site
    - Username: admin
    - Password: AWSExpert**!
    - Email: myemail@address.com
11. Si todo está correcto, serás redireccionado a una pantalla con este mensaje: Success! WordPress has been installed. Thank you, and enjoy!. Deberás poder entrar al panel de administración de WordPress con el usuario y contraseña que configuraste.

Laboratorio 5: Routing y registros DNS.

Objetivos

En este laboratorio harás las configuraciones necesarias en tu proveedor de dominio y en AWS para configurar el blog de WordPress de tu dominio personal.

Resumen

- Registrar tu dominio personal en Route 53 para ser utilizado en AWS.
- Agregar los Name Server en tu proveedor de dominio.
- Crear un subdominio blog. para tu dominio personal.

Punto de partida

En el menú principal ve a la sección de Services y selecciona la opción Route 53.

Ejecución de Laboratorio:

- Crea una Hosted Zone con tu dominio personal.
    1. Selecciona la opción Hosted zones y haz clic en el botón Create Hosted Zone.
    2. Agrega tu dominio personal en el campo Domain Name, ejemplo: mexican.dev. Da clic en el botón Create para guardar los cambios.
    3. Deberás ver los dos registros creados automáticamente en tu pantalla. Uno de tipo NS y otro de tipo SOA.
- Copia los name server en tu proveedor de dominio.
    1. Selecciona el registro de tipo NS y copia los Name Server que aparecen en el campo de Value.
    2. Deberás iniciar sesión en tu administrador de nombre de dominio y personalizar los registros de Name Server para que tenga los valores que copiaste de Route 53. Es **IMPORTANTE** mencionar que cada administrador de dominios es diferente y deberás encontrar la opción de Name Server personalizados para poder completar este paso.
    3. Guarda la configuración de tu dominio en tu proveedor de dominio y regresa a AWS.
- Crea un A Record para el subdominio blog de tu dominio personal.
    1. Ve al servicio de EC2 y copia la IP pública de tu instancia Web Server. Busca el atributo IPv4 Public IP y copia la dirección IP.
    2. Regresa a Route 53 en la sección de Hosted zones y haz clic en tu dominio personal.
    3. Haz clic en el botón Create Record Set, deberás llenar los valores como:
        - Name: blog
        - Type: A - IPv4 address

- Alias: No
- TTL (Seconds): 60
- Values: (Pega la IPv4 pública de tu instancia Web Server)

4. Haz clic en el botón Create para guardar los cambios.
5. El subdominio blog. aparecerá en la lista de registros como tipo A récord y la IP de tu instancia EC2 como valor del registro.
6. Ingresa el dominio en tu navegador para ver tu página WordPress.
7. Si tu página no se ve probablemente se deba a un tema de distribución de DNS. Deberás esperar unos minutos hasta que el dominio sea propagado correctamente.

Laboratorio 6: Distribución de contenidos con CloudFront.

Objetivos

En este laboratorio sincronizarás con S3 todas las imágenes almacenadas en tu blog de WordPress. Una vez sincronizadas las imágenes estas podrán ser distribuidas a través de AWS CloudFront, para ello haremos las configuraciones necesarias en tu servidor web.

Resumen

- Configuraremos AWS Cli (https://aws.amazon.com/cli/) en nuestro servidor para sincronizar las imágenes periódicamente en S3.
- Crearemos la distribución de las imágenes con CloudFront.
- Modificaremos el archivo .htaccess del blog the WordPress para utilizar CloudFront como distribuidor de imágenes.

Punto de partida

Ingresa a tu cuenta de AWS y ve al servicio de EC2 (https://console.aws.amazon.com/ec2/home)

Ejecución de Laboratorio:

- Crea CRON de sincronización de imágenes de tu sitio WordPress a S3.
    1. Ingresa por SSH a tu instancia de EC2.
    2. Una vez dentro de tu servidor comprobaremos que AWS Cli esté correctamente instalado y que puedas conectarte al Bucket de S3 que creaste en el segundo laboratorio. Ejecuta este comando en tu consola: aws s3 ls. El Bucket que creaste deberá aparecer en la lista.
    3. Identifica donde se encuentran las imágenes almacenadas por WordPress, deberán estar en la siguiente ruta /var/www/html/wp-content/uploads sincronizamos el contenido de esa carpeta cada minuto con el Bucket de S3.
    4. Ejecuta los siguientes comandos para iniciar el servicio de Crontab dentro de tu servidor:

```
$ sudo service crond start
$ sudo chkconfig crond on
$ sudo crontab -e
```

    5. Dentro del editor de Crontab escribe la siguiente línea de texto y guarda los cambios:

```
* * * * * aws s3 sync /var/www/html/wp-content/uploads s3://nombre_de_tu_bucket/images/
```

6. Todo el contenido de la carpeta uploads de tu instalación de WordPress deberá aparecer en tu Bucket dentro de la carpeta de images.

- Cambia la configuración de privacidad de tu Bucket.
  1. En el servicio de S3 de AWS selecciona tu Bucket.
  2. Haz clic en el botón Edit public access settings.
  3. En el cuadro de diálogo des-selecciona la casilla Block all public access y haz clic en el botón Save. El tipo de acceso al Bucket deberá aparecer como Objects can be public.
  4. Entra a tu Bucket y selecciona la carpeta images. Haz clic en el menú Actions y selecciona la opción Make public. Haz clic en el botón Make public en el cuadro de diálogo.
  5. Navega dentro de las carpetas y copia el Object URL de una de las imágenes guardadas. Deberás poder ver la imagen en tu navegador sin ningún problema.
- Crea una distribución web de las imágenes guardadas en S3.
  1. Ve al servicio de CloudFront de AWS en https://console.aws.amazon.com/cloudfront/home.
  2. Haz clic en el botón Create Distribution y después en la sección Web haz clic en el botón Get Started.
  3. Serás redireccionado a la sección Create Distribution, llena los valores de los campos como se te indica a continuación:
     - Origin Domain Name: nombre_de_tu_bucket.s3.amazonaws.com
     - Origin Path: /images
     - Origin ID: S3-nombre_de_tu_bucket
  4. En el final de la pantalla haz clic en el botón Create Distribution.
  5. Serás redireccionado a la pantalla principal de CloudFront y verás tu distribución con Status: In Progress.
  6. El proceso de distribución tomará unos minutos para ser completado. Deberá de tener un Status: Deployed.
  7. Copia el Domain Name de tu distribución y comprueba que puedas ver la imagen de prueba en tu navegador. Ejemplo:
     - Reemplaza este dominio: https://dw-training-2019.s3-us-west-2.amazonaws.com/images/2019/11/IMG_20140513_001936.jpg
     - Por este dominio: http://d16afjxqdhbnfu.cloudfront.net/2019/11/IMG_20140513_001936.jpg
- Crea la configuración en tu instancia web para redirigir a CloudFront.
  1. Ingresa por SSH a tu instancia de EC2.
  2. En la carpeta /var/www/html de tu instancia, crea un archivo llamado '.htaccess' con el siguiente contenido:

     Options +FollowSymlinks RewriteEngine on rewriterule ^wp-content/uploads/(.*)$ http://tu_distribution_id.cloudfront.net/$1 [r=301,nc]

     # BEGIN WordPress

END WordPress

3. Guarda el archivo y ejecuta los siguientes comandos: chkconfig httpd on service httpd start
4. Ahora las imágenes de tu página de WordPress deberán ser cargadas en el navegador desde la distribución de CloudFront y no desde tu instancia de EC2.