

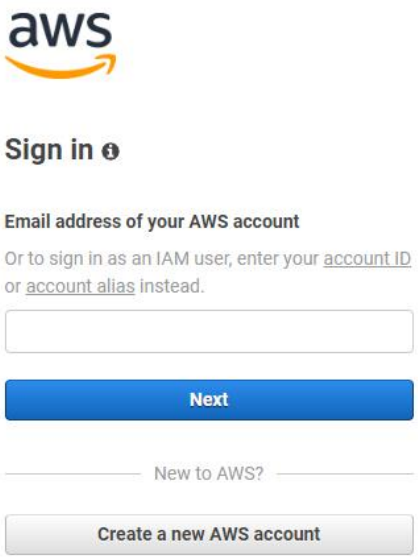
CenturyLink

Guía Protocolo de Pruebas AWS

A continuación, suministramos la información de URL y credenciales para las pruebas que se llevaran a cabo según lo indicado en el Anexo 5 - Protocolo de pruebas

Información de Acceso:

Portal de acceso: https://677970398382.signin.aws.amazon.com/console
IAM User name: cce-demo
password: L#m3n@2022col





Para la opción de inicio de sesión doble fator de autenticación, se debe instalar en el mobile del usuario una aplicación de Autenticación, ejemplo, Google Authenticator.

GUIAS Y REFERENCIAS:

TAREA 1

Creación de un usuario de IAM en su cuenta de AWS https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fIAM%2flatest%2fUserGuide%2fid%5fusers%5fcreate.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-6ce03c503b644e52f682bce837fb39e320af0e8e

Habilitación de un dispositivo de autenticación multifactor (MFA) virtual (consola)

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fIAM%2flatest%2fUserGuide%2fid%5fcredentials%5fmfa%5fenable%5fvirtual.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-3515c4c2488f52c3b7f868ac8ce5ecc1f39a5101

TAREA 2

Creación de casos de soporte y administración de casos

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fawssupport%2flatest%2fuser%2fcase%2dmanagement.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-e511562f4b3f70edc3cf1a98f9b22b8b7d6ef90c

TAREA 3

Validación de documentación AWS

https://docs.aws.amazon.com/es_es/

TAREA 4

Introducción a las instancias de Linux de Amazon EC2

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fAWSEC2%2flatest%2fUserGuide%2fEC2%5fGetStarted.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-dfbb3a56a23de0205477de744aea546d26bfb983

TAREA 5

Creación de una instancia de base de datos de Amazon RDS

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5

fes%2fAmazonRDS%2flatest%2fUserGuide%2fUSER%5fCreateDBInstance.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-9e5d81f5c856ddea866efe9779a1842ac370d8c3

TAREA 6

Balanceador de cargas

https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/application/create-application-load-balancer.html

TAREA 7

Crear un grupo de seguridad

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fvpc%2flatest%2fuserguide%2fVPC%5fSecurityGroups.html%23creating%2dsecurity%2dgroups&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-927116f44d67893444094afe94843477d924a807

TAREA 8

Crear una subred en la VPC

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fvpc%2flatest%2fuserguide%2fworking%2dwith%2dvpcs.html%23AddaSubnet&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-a513d50bd0763f560485a96cba2de7b08ab25620

Creación y aceptación de interconexiones de VPC

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fvpc%2flatest%2fpeering%2fcreate%2dvpc%2dpeering%2dconnection.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-fd3da7ebcc7a2ace23037999ee3c525713e9fe15

TAREA 9

Crear instancias de Amazon EBS

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fAWSEC2%2flatest%2fUserGuide%2febs%2dcreating%2dsnapshot.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-e5f8366fa2fef57fbff98e8c5fe40bc3a8cfad39

TAREA 10

Crear un grupo de Auto Scaling mediante una configuración de lanzamiento

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fautoscaling%2fec2%2fuserguide%2fcreate%2dasg.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-62ec39c136552ba8eb5bd7c9f0c5ea8b546ff36b

TAREA 11 y TAREA 12

Cambie el tipo de instancia

https://imss91-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fdocs.aws.amazon.com%2fes%5fes%2fAWSEC2%2flatest%2fUserGuide%2fec2%2dinstance%2dresize.html&umid=BBFCE711-CAF5-B805-BD2D-8D3AC9DA6F67&auth=19120be9529b25014b618505cb01789c5433dae7-2aa548cd8c789720799713acec36221dbcc4b3db

TAREA 13

Copias de seguridad

https://aws.amazon.com/es/blogs/aws-spanish/aws-backup-administre-de-forma-centralizada-sus-copias-de-seguridad-en-la-nube/

Amazon EBS snapshots

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html

TAREA 14

Creación de informes de uso y costo

https://docs.aws.amazon.com/es_es/cur/latest/userguide/cur-create.html

TAREA 15

Validar tareas anteriores de creación de instancias

TAREA 16

Previsión con CostExplorer

https://docs.aws.amazon.com/es_es/awsaccountbilling/latest/aboutv2/ce-forecast.html

1. Habilitación de un dispositivo de autenticación multifactor (MFA) virtual (Consola)

Puede utilizar un dispositivo móvil, como, por ejemplo, un smartphone o una tablet, como un dispositivo de autenticación multifactor (MFA) virtual. Para ello, instale una aplicación para móviles compatible con AWS que genere un código de autenticación de seis dígitos. Dado que estas aplicaciones se puede ejecutar en dispositivos móviles desprotegidos, MFA virtual podría no proporcionar el mismo nivel de seguridad que los dispositivos U2F o los dispositivos de MFA físicos. Recomendamos que utilice un dispositivo MFA virtual mientras espera la aprobación de compra de hardware o mientras espera a que llegue su hardware.

La mayoría de aplicaciones móviles de MFA virtual admiten la creación de varios dispositivos virtuales, lo que le permite utilizar la misma aplicación para varias cuentas o usuarios de AWS. Sin embargo, solo puede habilitar un dispositivo MFA por usuario.

Para aplicaciones de MFA virtual que puede utilizar en smartphones o tablets, consulte Multi-Factor Authentication. Tenga en cuenta que de AWS requiere una aplicación MFA virtual que genere una contraseña de un solo uso (OTP) de seis dígitos.

importante

Cuando configure un dispositivo MFA virtual para que funcione con AWS, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. De ese modo, si pierde el teléfono o tiene que volver a instalar la aplicación de software de MFA por cualquier motivo, puede volver a configurar la aplicación para que utilice la misma MFA virtual. Así evita tener que crear un nuevo dispositivo MFA virtual en AWS para el usuario o el usuario raíz.

1.1 Permisos necesarios

Para administrar dispositivos MFA virtuales para su usuario de IAM, debe contar con los permisos de la siguiente política: AWS: permite a los usuarios de IAM autenticados por MFA administrar su propio dispositivo MFA en la página My Security Credentials (Mis credenciales de seguridad).

1.2 Habilite un dispositivo MFA virtual para un usuario de IAM (Consola)

Puede utilizar IAM en la Consola de administración de AWS para habilitar y administrar un dispositivo MFA virtual para un usuario de IAM en su cuenta. Para habilitar y administrar un

dispositivo MFA utilizando la AWS CLI o la API de AWS, consulte Activación y administración de dispositivos MFA virtuales (AWS CLI o API de AWS).

nota

Debe tener acceso físico al hardware que alojará el dispositivo MFA virtual del usuario para poder configurar la MFA. Por ejemplo, puede configurar MFA para un usuario que use un dispositivo MFA virtual que se ejecute en un smartphone. En ese caso, debe tener el smartphone disponible para completar el asistente. Por este motivo, puede interesarle que los usuarios puedan configurar y administrar sus propios dispositivos MFA virtuales. En ese caso, debe conceder a los usuarios los permisos necesarios para realizar las acciones de IAM necesarias. Para obtener más información y consultar un ejemplo de una política de IAM que conceda dichos permisos, consulte AWS: permite a los usuarios de IAM autenticados por MFA administrar su propio dispositivo MFA en la página My Security Credentials (Mis credenciales de seguridad).

Para habilitar un dispositivo MFA virtual para un usuario de IAM (consola)

1. Inicie sesión en la Consola de administración de AWS y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione **Users**.
3. En la lista **User Name (Nombre de usuario)**, elija el nombre del usuario de MFA previsto.
4. Seleccione la **pestaña de credenciales de** seguridad. Al lado de **Assigned MFA device (Dispositivo MFA asignado)**, seleccione **Manage (Administrar)**.
5. En el asistente **Manage MFA Device (Administrar dispositivo MFA)**, elija **Virtual MFA device (Dispositivo MFA virtual)** y, a continuación, elija **Continue (Continuar)**.

   IAM generará y mostrará la información de configuración del dispositivo MFA virtual, incluido un gráfico de código QR. El gráfico es una representación de la "clave de configuración secreta" que se puede introducir manualmente en dispositivos que no admiten códigos QR.

6. Abra su aplicación de MFA virtual. (Para ver una lista de las aplicaciones que puede utilizar para alojar dispositivos MFA virtuales, consulte Autenticación multifactor). Si la aplicación de MFA virtual admite varias cuentas (varios dispositivos de MFA virtuales), elija la opción para crear una nueva cuenta (un nuevo dispositivo MFA virtual).
7. Determine si la aplicación MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones:

- Desde el asistente, elija **Show QR code (Mostrar código QR)** y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a **Scan code (Escanear código)** y, a continuación, utilizar la cámara del dispositivo para escanear el código.
- En el asistente **Manage MFA Device (Administrar dispositivo MFA)**, elija **Show secret key (Mostrar clave secreta)** y, a continuación, escriba la clave secreta en su aplicación de MFA.

Cuando haya terminado, el dispositivo MFA virtual comenzará a generar contraseñas de uso único.

8. En el asistente **Manage MFA Device (Administrar dispositivo MFA)**, en el cuadro **MFA code 1 (Código MFA 1)** escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA virtual. Espere hasta 30 segundos a que el dispositivo genere una nueva contraseña de uso único. A continuación, escriba la otra contraseña de uso único en el cuadro**MFA code 2 (Código MFA 2)**. Elija **Assign MFA (Asignar MFA)**.

   importante

   Envíe su solicitud inmediatamente después de generar los códigos. Si genera los códigos y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente al usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas de un solo uso basadas en el tiempo (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

Ahora el dispositivo MFA virtual ya está listo para usarlo con AWS. Para obtener más información sobre el uso de MFA con la Consola de administración de AWS, consulte Uso de dispositivos MFA con la página de inicio de sesión del IAM.

1.3 Habilitación de un dispositivo MFA virtual para su usuario raíz de la cuenta de AWS (consola)

Puede utilizar la Consola de administración de AWS para configurar y habilitar un dispositivo MFA virtual para su usuario raíz. Para habilitar dispositivos MFA para la cuenta de AWS, debe haber iniciado sesión en AWS con las credenciales de usuario raíz. No es posible habilitar un dispositivo MFA para Usuario de la cuenta raíz de AWS en la consola IAM o con AWS CLI, AWS API, Herramientas para Windows PowerShell, ni ninguna de las otras herramientas de línea de comandos.

de Si su dispositivo de MFA se ha perdido, ha sido robado o no funciona, puede iniciar sesión con otros factores de autenticación. Si no puede iniciar sesión con su dispositivo MFA, puede

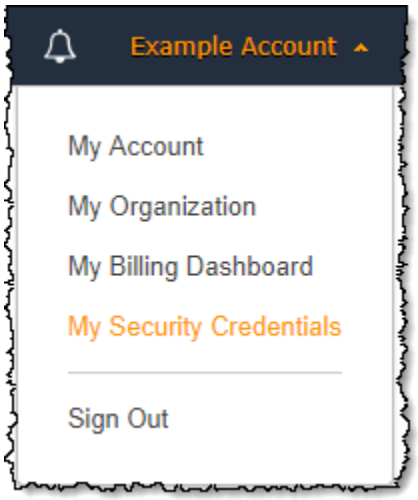
hacerlo verificando su identidad con el correo electrónico y teléfono que están registrados en su cuenta. Antes de habilitar MFA para su usuario usuario raíz, revise la configuración de la cuenta y la información de contacto para asegurarse de que tiene acceso al correo electrónico y al número de teléfono. Para obtener más información acerca de cómo iniciar sesión con factores de autenticación alternativos, consulte ¿Qué pasa si un dispositivo de MFA se pierde o deja de funcionar?. Para deshabilitar esta característica, póngase en contacto con AWS Support.

nota

Puede ver texto diferente, como, por ejemplo, **Iniciar sesión mediante MFA** y **Solución de problemas con el dispositivo de autenticación**. Sin embargo, se proporcionan las mismas características. En cualquier caso, si no puede verificar la dirección de correo electrónico y el número de teléfono de su cuenta mediante factores de autenticación alternativos, póngase en contacto con AWS Support para desactivar la configuración de MFA.

Para configurar y habilitar un dispositivo MFA virtual para usarlo con su usuario usuario raíz (consola)

1. Inicie sesión en Consola de administración de AWS.
2. Aplique alguna de las siguientes acciones:
    - **Opción 1**: elija **Dashboard (Panel)** y en **Security Status (Estado de seguridad)** amplíe **Activate MFA on your usuario raíz (Activar MFA en su usuario raíz)**.
    - **Opción 2**: en la parte derecha de la barra de navegación, elija su nombre de cuenta y seleccione **My Security Credentials (Mis credenciales de seguridad)**. Si es necesario, elija **Continue to Security Credentials (Continuar a credenciales de seguridad)**. A continuación, amplíe la sección **Multi-Factor Authentication (MFA) (Autenticación multifactor [MFA])** en la página.



3. Seleccione **Manage MFA (Administrar MFA)** o **Activate MFA (Activar MFA)**, en función de la opción que haya elegido en el paso anterior.
4. En el asistente, elija **Virtual MFA device (Dispositivo MFA virtual)** y, a continuación, seleccione **Continue (Continuar)**.
5. Confirme que el dispositivo tenga instalada una aplicación de MFA virtual y, a continuación, elija **Continue (Continuar)**. IAM generará y mostrará la información de configuración del dispositivo MFA virtual, incluido un gráfico de código QR. El gráfico es una representación de la clave de configuración secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
6. Con el asistente **Manage MFA Device (Administrar dispositivo MFA)** abierto, abra la aplicación de MFA virtual en el dispositivo.
7. Si la aplicación de MFA virtual es compatible con varias cuentas (varios dispositivos MFA virtuales), elija la opción para crear una nueva cuenta (un nuevo dispositivo virtual).
8. La forma más sencilla de configurar la aplicación consiste en utilizar la aplicación para escanear el código QR. Si no puede analizar el código, puede escribir la información de configuración manualmente.
    - En el asistente, para utilizar el código QR para configurar el dispositivo MFA virtual, elija **Show QR code (Mostrar código QR)**. A continuación, siga las instrucciones de la aplicación para escanear el código. Por ejemplo, puede ser necesario pulsar una vez el icono de la cámara o un comando similar a **Scan account barcode (Escanear código de barras de la cuenta)** y, a continuación, utilizar la cámara del dispositivo para escanear el código QR.
    - En el asistente **Manage MFA Device (Administrar dispositivo MFA)**, elija **Show secret key (Mostrar clave secreta)** y, a continuación, escriba la clave secreta en su aplicación de MFA.

importante

Haga una copia de seguridad segura del código QR o la clave de configuración secreta, o asegúrese de habilitar varios dispositivos MFA virtuales para su cuenta. Un dispositivo MFA virtual puede dejar de estar disponible si, por ejemplo, pierde el smartphone donde se aloja el dispositivo MFA virtual. Si esto ocurre, no podrá iniciar sesión en su cuenta y tendrá que ponerse en contacto con el servicio de atención al cliente para eliminar la protección de MFA de la cuenta.

nota

El código QR y la clave de configuración secreta generada por IAM están vinculados a su cuenta de AWS y no se pueden utilizar con otra cuenta. Sin embargo, se pueden volver a utilizar para configurar un dispositivo MFA nuevo para su cuenta en caso de que pierda el acceso al dispositivo MFA original.

El dispositivo comienza a generar números de seis dígitos.

9. En el asistente **Manage MFA Device (Administrar dispositivo MFA)**, en el cuadro **MFA Code 1 (Código MFA 1)**, escriba el número de seis dígitos que el dispositivo MFA muestra actualmente. Espere hasta 30 segundos a que el dispositivo genere un número nuevo y, a continuación, escriba el número de seis dígitos nuevo en el cuadro **MFA Code 2 (Código MFA 2)**.

   importante

   Envíe su solicitud inmediatamente después de generar los códigos. Si genera los códigos y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente al usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas de un solo uso basadas en el tiempo (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

10. Elija **Assign MFA (Asignar MFA)** y, a continuación, elija **Finish (Finalizar)**.

El dispositivo ya está listo para usarlo con AWS. Para obtener más información sobre el uso de MFA con la Consola de administración de AWS, consulte Uso de dispositivos MFA con la página de inicio de sesión del IAM.

1.4 Reemplazar o "rotar" un dispositivo MFA virtual

Solo puede tener un único dispositivo MFA asignado a un usuario a la vez. Si el usuario pierde un dispositivo o debe reemplazarlo por cualquier motivo, primero debe desactivar el antiguo dispositivo. Después, puede añadir el nuevo dispositivo para el usuario.

- Para desactivar el dispositivo que tenga asociado actualmente a otro usuario de IAM, consulte Desactivación de dispositivos MFA.
- Para añadir un dispositivo MFA virtual de sustitución para otro usuario de IAM, siga los pasos que se indican en el procedimiento Habilite un dispositivo MFA virtual para un usuario de IAM (Consola) anterior.
- Para añadir un dispositivo MFA de sustitución virtual para el Usuario de la cuenta raíz de AWS, siga los pasos indicados en el procedimiento Habilitación de un dispositivo MFA virtual para su usuario raíz de la cuenta de AWS (consola) que aparece en secciones anteriores de este tema.

2. Aprovisionamiento de Instancias EC2 o máquinas virtuales

Antes de poder lanzar y conectarse a una instancia Amazon EC2, tiene que crear un par de claves, a menos que ya disponga de una. Puede crear un par de claves utilizando la consola de Amazon EC2 y, a continuación, puede lanzar la instancia EC2.

nota

No se admite el uso de Amazon EFS con instancias Amazon EC2 de Microsoft Windows.

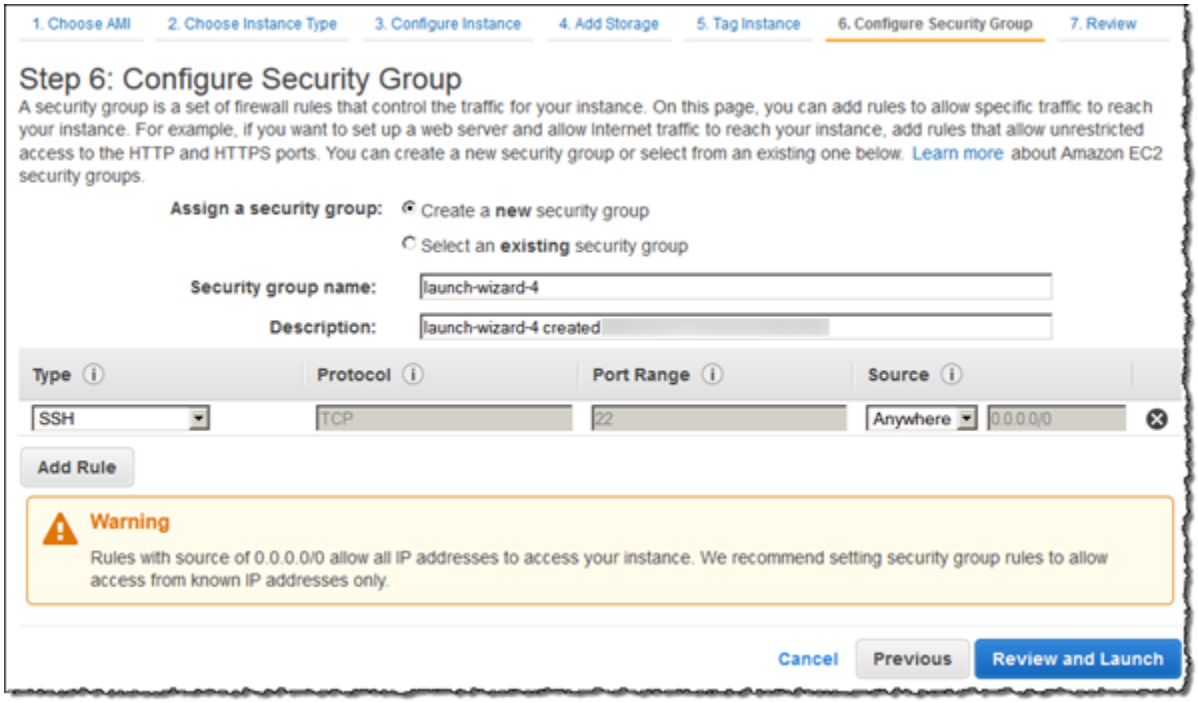
Para crear un par de claves

- Siga los pasos de Configuración con Amazon EC2 en la **Guía del usuario de Amazon EC2 para instancias de Linux** para crear un par de claves. Si ya dispone de un par de claves, no es necesario crear uno nuevo y puede utilizar el par de claves existente para este ejercicio.

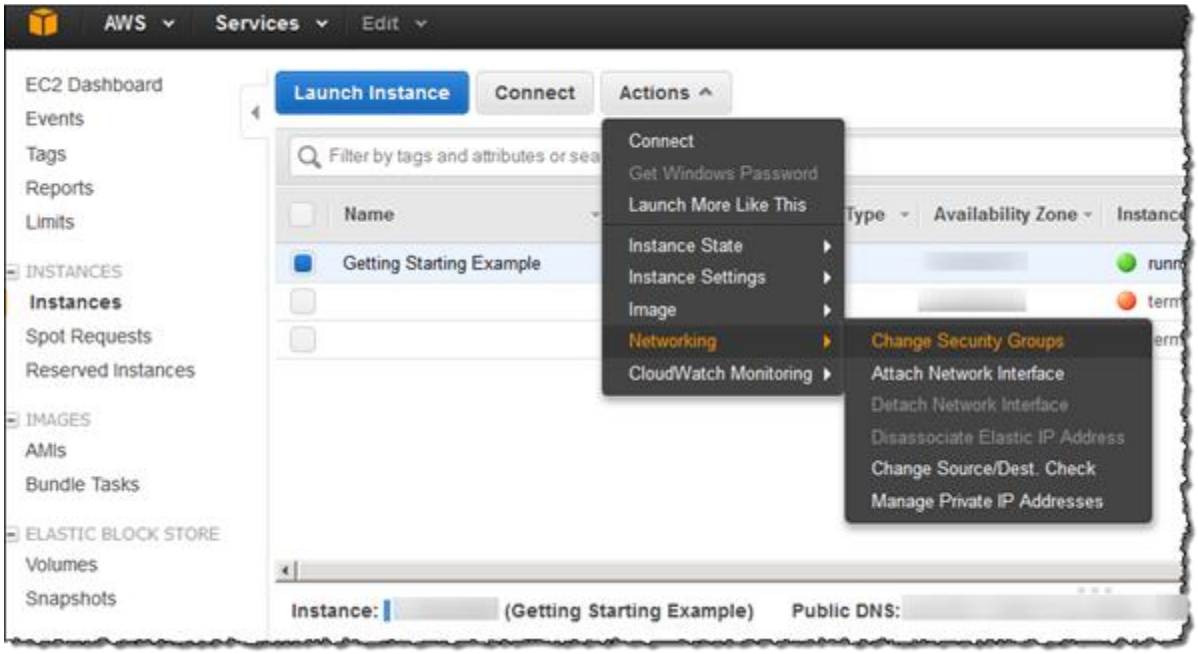
Para lanzar la instancia EC2

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Elija **Launch Instance**.
3. En **Step 1: Choose an Amazon Machine Image (AMI) (Paso 1: Elegir una Amazon Machine Image (AMI))**, busque una AMI de Amazon Linux en la parte superior de la lista y elija **Select (Seleccionar)**.
4. En el **Step 2: Choose an Instance Type (Paso 2: Elegir la instancia c5.xlarge (4vcpus y 8 GB RAM)**, seleccione **Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia)**.
5. En **Step 3: Configure Instance Details (Paso 3: Configurar detalles de la instancia)**, en el campo **Number of instances** indique la cantidad de maquinas a crear, para nuestro caso **100 instancias**, luego elija **Network (Red)** y, a continuación, elija la entrada para su VPC predeterminada. La URL debería parecerse a esta: `vpc-xxxxxxx (172.31.0.0/16) (default)`.
    a. Seleccione **Subnet (Subred)** y, a continuación, elija una subred en cualquier zona de disponibilidad.
    b. Elija **Next: Add Storage (Siguiente: Añadir almacenamiento)**.
6. Elija **Next: Add Tags**.
7. Asigne un nombre a la instancia y elija **Next: Configure Security Group (Siguiente: Configurar grupo de seguridad)**.

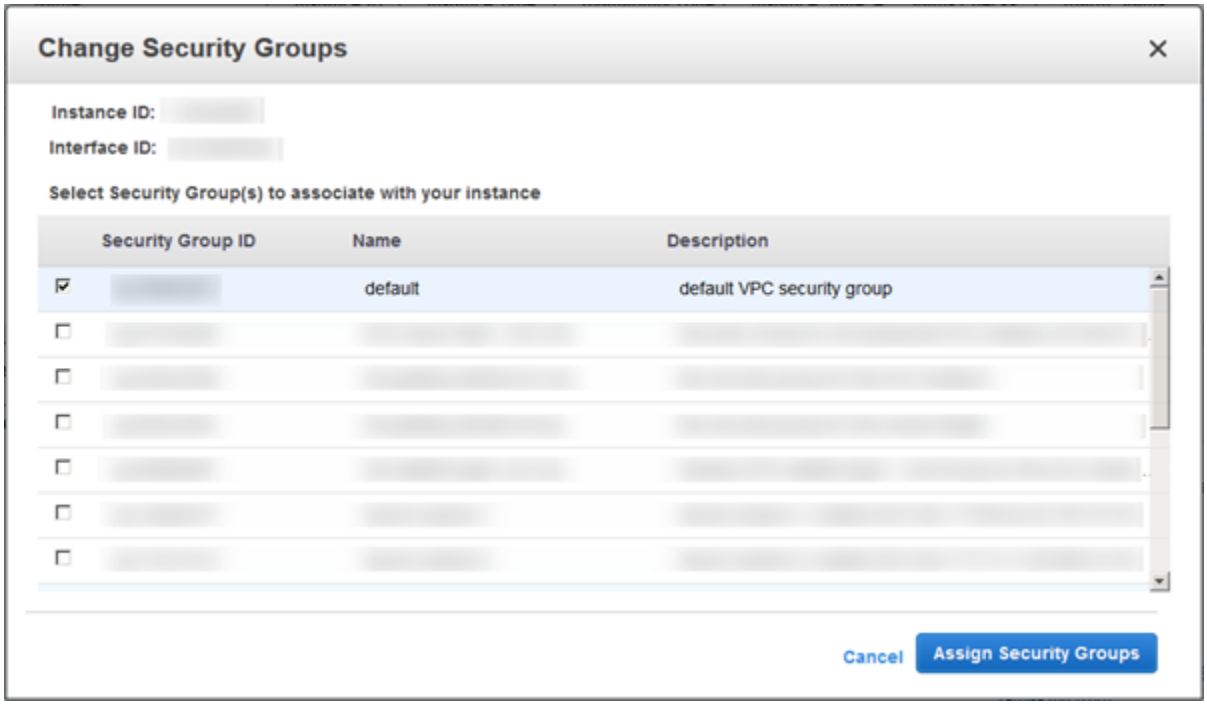
8. En **Step 6: Configure Security Group (Paso 6: Configurar grupo de seguridad)**, revise el contenido de esta página, asegúrese de que **Assign a security group (Asignar un grupo de seguridad)** está establecido en **Create a new security group (Crear un nuevo grupo de seguridad)** y compruebe que la regla de entrada que se está creando tenga los siguientes valores predeterminados.
    a. **Tipo:** SSH
    b. **Protocolo:** TCP
    c. **Rango de puerto:** 22
    d. **Origen:** cualquiera 0.0.0.0/0



9. Elija **Review and Launch (Revisar y lanzar)**.
10. Elija **Launch**.
11. Seleccione la casilla de verificación para el par de claves que ha creado y, a continuación, elija **Launch Instances (Lanzar instancias)**.
12. Elija **View Instances (Ver instancias)**.
13. Elija el nombre de la instancia que acaba de crear en la lista y, a continuación, elija **Actions (Acciones)**.
    a. En el menú que se abre, elija **Networking (Redes)** y, a continuación, elija **Change Security Groups (Cambiar grupos de seguridad)**.



b. Seleccione la casilla de verificación junto al grupo de seguridad con la descripción **default VPC security group (grupo de seguridad de VPC predeterminado)**.
c. Seleccione **Assign Security Groups (Asignar grupos de seguridad)**.



14. nota

15. En este paso, asigna el grupo de seguridad predeterminado de su VPC a la instancia Amazon EC2. Esto garantiza que la instancia sea miembro del grupo de seguridad que el

destino de montaje del sistema de archivos de Amazon EFS autoriza para conectar en Paso 2: Crear su sistema de archivos de Amazon EFS.

16. Al utilizar el grupo de seguridad predeterminado de su VPC, con sus reglas de entrada y salida predeterminadas, es posible que abra esta instancia y este sistema de archivos a posibles amenazas potenciales desde la VPC. Asegúrese de seguir Paso 5: Limpiar recursos y proteger la cuenta de AWS al final de este ejercicio de introducción para eliminar los recursos expuestos al grupo de seguridad predeterminado de su VPC para este ejemplo. Para obtener más información, consulte Grupos de seguridad para instancias Amazon EC2 y destinos de montaje.
17. Seleccione su instancia de la lista.
18. En la pestaña **Description (Descripción)**, asegúrese de que dispone de dos entradas junto a **grupos de seguridad**—: una para el grupo de seguridad de VPC predeterminado y otra para el grupo de seguridad que creó al lanzar la instancia.
19. Apunte los valores que aparecen junto a **VPC ID (ID de la VPC)** y **Public DNS (DNS público)**. Necesita dichos valores más adelante en este ejercicio.

3. Aprovisionamiento de una instancia de base de datos de RDS

En este paso, va a crear una instancia de base de datos MySQL en Amazon RDS para alojar los datos utilizados por una aplicación web.

importante

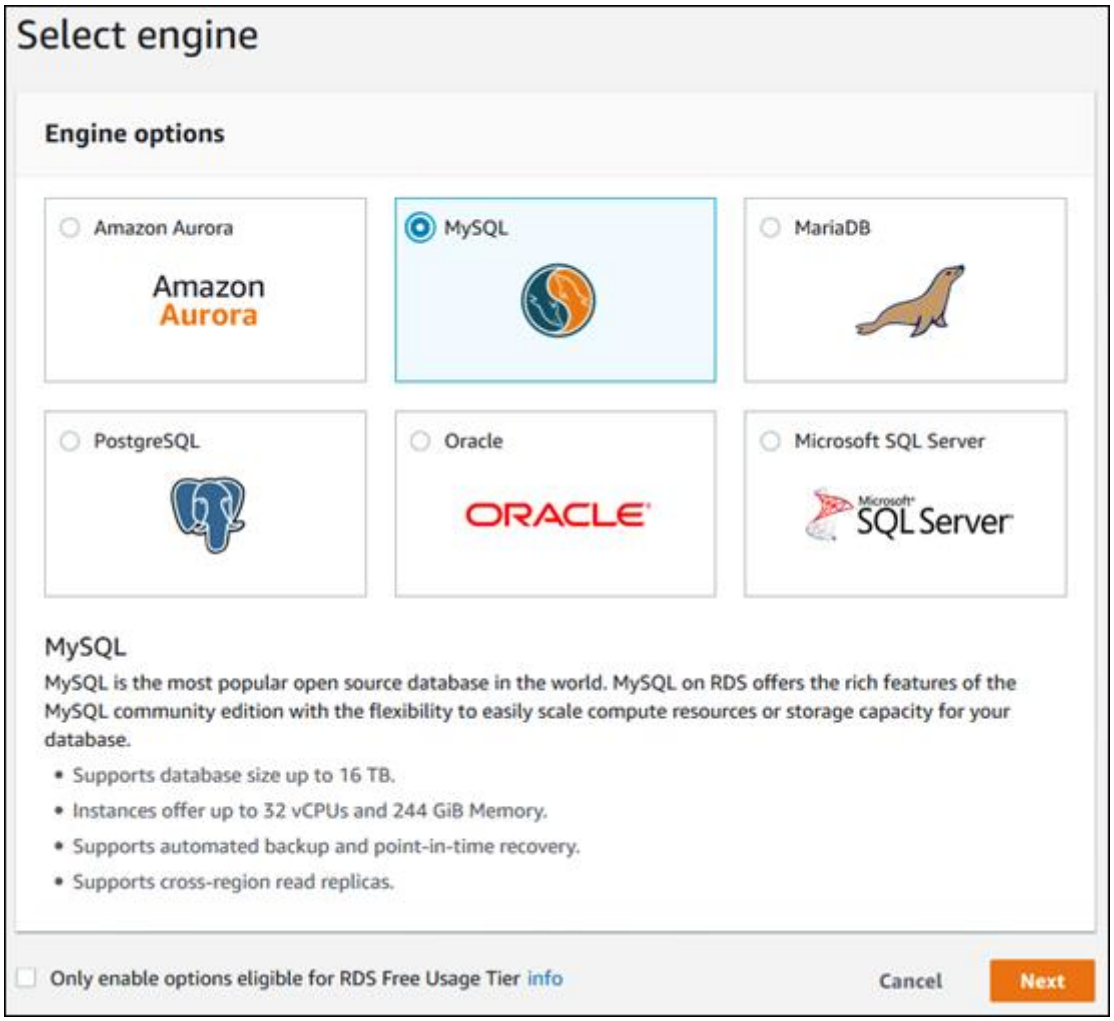
Antes de comenzar este paso, debe disponer de una VPC con subredes públicas y privadas y sus correspondientes grupos de seguridad. Si no dispone de ella, consulte Tutorial: Creación de una Amazon VPC para utilizarla con una instancia de base de datos. Realice los pasos que se indican en Creación de una VPC con subredes públicas y privadas, Creación de las subredes adicionales, Creación de un grupo de seguridad de VPC para un servidor web público y enCreación de un grupo de seguridad de VPC para una instancia privada de base de datos.

Para lanzar una instancia de base de datos MySQL

1. Inicie sesión en la Consola de administración de AWS y abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. En la esquina superior derecha de la Consola de administración de AWS, elija la región de AWS en la que desea crear la instancia de base de datos. En este ejemplo se utiliza la región EE.UU. Oeste (Oregón).
3. En el panel de navegación, seleccione **Databases (Bases de datos)**.

Si el panel de navegación está cerrado, elija el icono de menú en la parte superior izquierda para abrirlo.

4. Elija **Create database (Crear base de datos)** para abrir la página **Select engine (Seleccionar motor)**.
5. En la página **Select engine**, que se muestra a continuación, elija **MySQL** y, a continuación, **Next**.



6. En la página **Choose use case (Elegir caso de uso)**, elija **Dev/Test – MySQL** y, a continuación, elija **Next (Siguiente)**.
7. En la página **Specify DB details**, que se muestra a continuación, defina estos valores:
   - **License model:** utilice el valor predeterminado.
   - **DB engine version:** utilice el valor predeterminado.
   - **DB instance class:** `db.t2.small`
   - **Multi-AZ Deployment (Implementación Multi-AZ):** `No`
   - **Storage type:** `General Purpose (SSD)`
   - **Allocated storage:** `20 GiB`

- **DB Instance Identifier (Identificador de instancias de bases de datos):** `tutorial-db-instance`
- **Master username:** `tutorial_user`
- **Master password:** elija una contraseña.
- **Confirm password:** vuelva a introducir la contraseña.

4. Creación de un balanceador de carga clásico

En este tutorial, encontrará una introducción práctica sobre el uso de Classic Load Balancers a través de la Consola de administración de AWS, una interfaz web. Crearemos un balanceador de carga que recibe el tráfico HTTP público y lo envía a las instancias EC2.

Tenga en cuenta que puede crear el balanceador de carga para usarlo con EC2-Classic o con una VPC. Algunas de las tareas descritas en este tutorial se aplican únicamente a los balanceadores de carga de una VPC.

Tareas

- Antes de empezar
- Paso 1: Seleccionar un tipo de balanceador de carga
- Paso 2: Definir el balanceador de carga
- Paso 3: Asignar grupos de seguridad al balanceador de carga de una VPC
- Paso 4: Configurar las comprobaciones de estado de las instancias EC2
- Paso 5: Registrar instancias EC2 con el balanceador de carga
- Paso 6: Agregar etiquetas al balanceador de carga (opcional)
- Paso 7: Crear y probar el balanceador de carga
- Paso 8: Eliminar el balanceador de carga (opcional)

4.1 Antes de empezar

- Realice los pasos que se indican en Preparar la VPC y las instancias EC2.
- Lance las instancias EC2 que desee registrar con el balanceador de carga. Asegúrese de que los grupos de seguridad de estas instancias permitan el acceso HTTP en el puerto 80.
- Instale un servidor web, por ejemplo, Apache o Internet Information Services (IIS), en cada instancia, escriba su nombre de DNS en el campo de direcciones de un navegador web conectado a Internet y compruebe que el navegador muestra la página predeterminada del servidor.

4.2 Paso 1: Seleccionar un tipo de balanceador de carga

Elastic Load Balancing admite tres tipos de balanceadores de carga: Application Load Balancers, Network Load Balancers y Classic Load Balancers. En este tutorial, va a crear un Classic Load Balancer. Si prefiere crear un Balanceador de carga de aplicaciones, consulte Introducción a los Application Load Balancers en la **Guía del usuario de Application Load Balancers**. Para crear un balanceador de carga de red, consulte Introducción a los balanceadores de carga de red en la **Guía del usuario de los balanceadores de carga de red**.

Para crear un Classic Load Balancer

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija una región para el balanceador de carga. No olvide seleccionar la misma región que seleccionó para las instancias EC2.
3. En el panel de navegación, en **LOAD BALANCING**, elija **Load Balancers**.
4. Elija **Create Load Balancer**.
5. Para **Classic Load Balancer (Balanceador de carga clásico)**, elija **Create (Crear)**.

4.3 Paso 2: Definir el balanceador de carga

Debe proporcionar una configuración básica para el balanceador de carga como, por ejemplo, un nombre, una red y un agente de escucha.

Un **agente de escucha** es un proceso que comprueba solicitudes de conexión. El agente de escucha se configura con un protocolo y un puerto para las conexiones frontend (entre el cliente y el balanceador de carga) y otro protocolo y otro puerto para las conexiones backend (entre el balanceador de carga y la instancia). En este tutorial, vamos a configurar un agente de escucha que acepta solicitudes HTTP en el puerto 80 y se las envía a las instancias en el puerto 80 a través de HTTP.

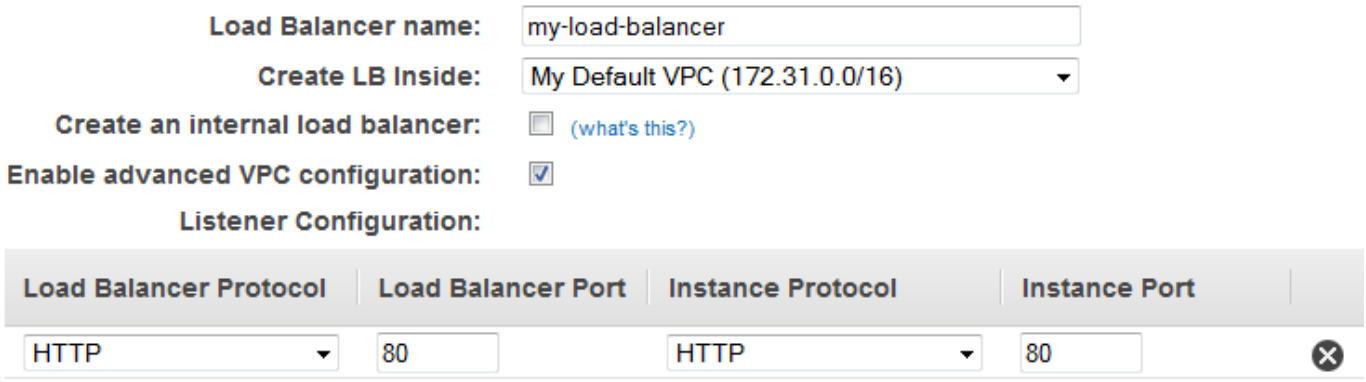
Para definir el balanceador de carga y el agente de escucha

1. En **Load Balancer name**, escriba el nombre del balanceador de carga.

   El nombre del Classic Load Balancer debe ser único en el conjunto de Classic Load Balancers de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar por un guion.

2. En **Create LB inside**, seleccione la misma red que seleccionó para las instancias: EC2-Classic o una VPC específica.

3. [Default VPC] Si seleccionó una VPC predeterminada y quiere elegir las subredes para el balanceador de carga, seleccione **Enable advanced VPC configuration**.
4. Deje la configuración predeterminada del agente de escucha.

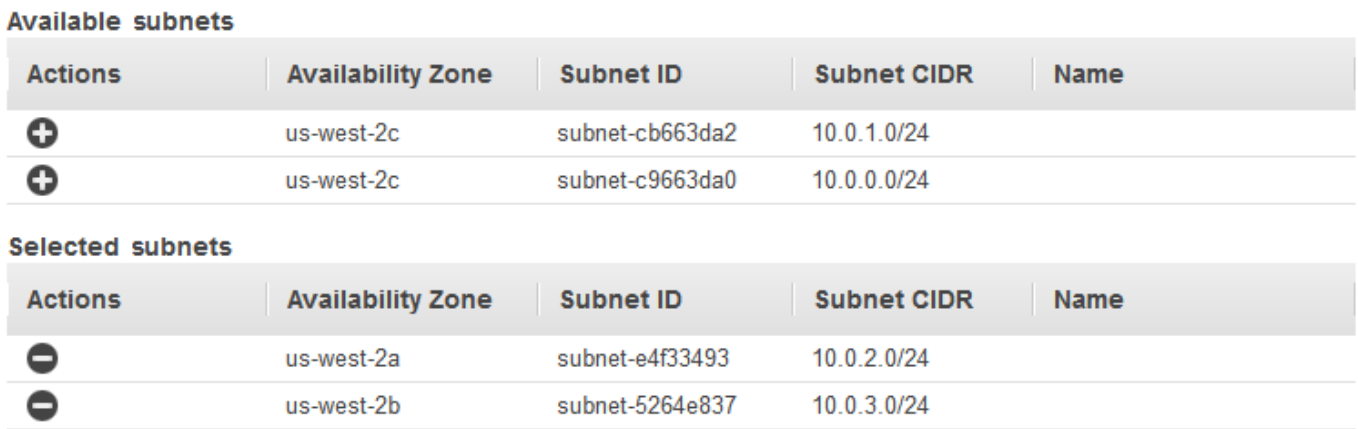


5. [EC2-VPC] En **Available subnets** (Subredes disponibles), seleccione al menos una subred pública disponible con el icono de adición. La subred se situará bajo **Selected subnets**. Para mejorar la disponibilidad del balanceador de carga, seleccione varias subredes públicas.

   nota

   Si seleccionó EC2-Classic como red o tiene una VPC predeterminada pero no seleccionó **Enable advanced VPC configuration** (Habilitar configuración de VPC avanzada), no verá la interfaz de usuario para seleccionar subredes.

   Puede agregar, como máximo, una subred por cada zona de disponibilidad. Si selecciona una segunda subred en una zona de disponibilidad en la que ya existe una subred seleccionada, esta subred sustituirá a la que está seleccionada actualmente en la zona de disponibilidad.



6. Elija **Next: Assign Security Groups** (Siguiente: Asignar grupos de seguridad).

4.4 Paso 3: Asignar grupos de seguridad al balanceador de carga de una VPC

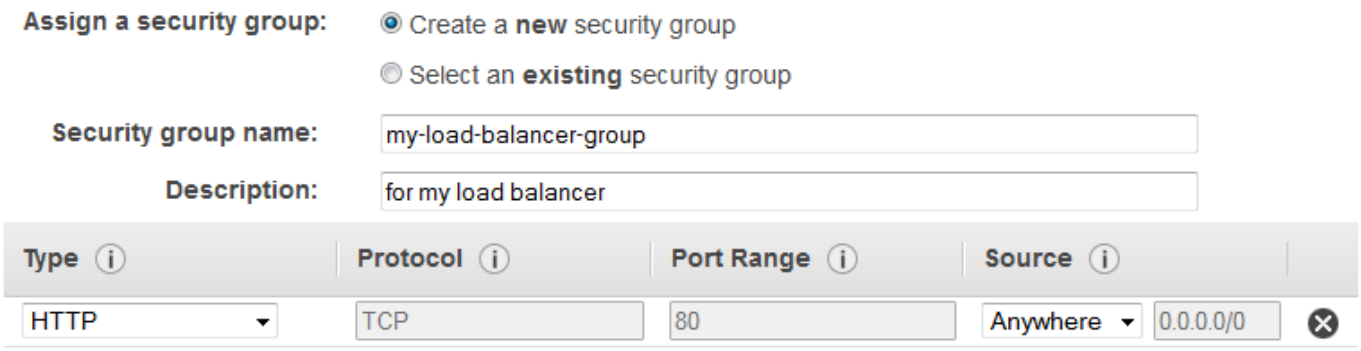
Si seleccionó una VPC como red, debe asignar al balanceador de carga un grupo de seguridad que permita el tráfico entrante en los puertos especificados para el balanceador de carga y las comprobaciones de estado del balanceador de carga.

nota

Si seleccionó EC2-Classic como red, puede continuar en el siguiente paso. De forma predeterminada, Elastic Load Balancing proporciona un grupo de seguridad para los balanceadores de carga de EC2-Classic.

Para asignar un grupo de seguridad al balanceador de carga

1. En la página **Assign Security Groups** (Asignar grupos de seguridad), seleccione **Create a new security group** (Crear un grupo de seguridad nuevo).
2. Escriba un nombre y una descripción para el grupo de seguridad o deje el nombre y la descripción predeterminados. Este nuevo grupo de seguridad contiene una regla que permite el tráfico en el puerto que se configuró para usarlo con el balanceador de carga.



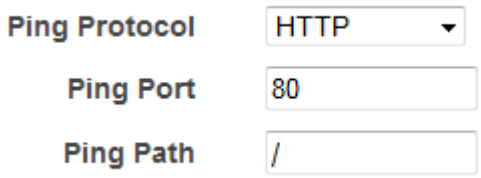
3. Elija **Next: Configure Security Settings**.
4. En este tutorial, no se utiliza un agente de escucha seguro. Elija **Next: Configure Health Check** (Siguiente: Configurar comprobación de estado) para continuar con el siguiente paso.

4.5 Paso 4: Configurar las comprobaciones de estado de las instancias EC2

Elastic Load Balancing comprueba automáticamente el estado de las instancias EC2 registradas en el balanceador de carga. Si Elastic Load Balancing detecta una instancia en mal estado, deja de enviar tráfico a dicha instancia y lo redirecciona a las instancias en buen estado. En este paso, se personalizan las comprobaciones de estado del balanceador de carga.

Para configurar comprobaciones de estado para sus instancias

1. En la página **Configure Health Check** (Configurar comprobación de estado), deje **Ping Protocol** (Protocolo de ping) establecido en HTTP y **Ping Port** (Puerto de ping) establecido en 80.
2. En **Ping Path**, sustituya el valor predeterminado por una barra diagonal sencilla ("/"). Esto le indica a Elastic Load Balancing que envíe consultas de comprobación de estado a la página de inicio predeterminada del servidor web; por ejemplo, `index.html`.



3. En **Advanced Details** (Detalles avanzados), deje los valores predeterminados.
4. Elija **Next: Add EC2 Instances** (Siguiente: Agregar instancias EC2).

4.6 Paso 5: Registrar instancias EC2 con el balanceador de carga

El balanceador de carga distribuye el tráfico entre las instancias que están registradas en el mismo.

nota

Al registrar una instancia con una interfaz de red elástica" (ENI), el balanceador de carga direcciona el tráfico a la dirección IP principal de la interfaz principal (eth0) de la instancia.

Para registrar instancias EC2 con el balanceador de carga

1. En la página **Add EC2 Instances** (Agregar instancias EC2), seleccione las instancias que registrar con su balanceador de carga.
2. Mantenga habilitados el balanceo de carga entre zonas y el vaciado de conexiones.
3. Elija **Next: Add Tags**.

Si lo prefiere, puede registrar las instancias en el balanceador de carga más adelante con las siguientes opciones:

- Seleccione las instancias en ejecución después de crear el balanceador de carga. Para obtener más información, consulte Registro de instancias en el balanceador de carga.

- Configure Auto Scaling para que registre las instancias automáticamente al lanzarlas. Para obtener más información, consulte Configuración de una aplicación con escalado y balanceo de carga aplicados en la **Guía del usuario de Amazon EC2 Auto Scaling**.

4.7 Paso 6: Agregar etiquetas al balanceador de carga (opcional)

Puede etiquetar su balanceador de carga o continuar en el paso siguiente. Tenga en cuenta que puede etiquetar el balanceador de carga más adelante; para obtener más información, consulte Etiquetado del balanceador de carga clásico.

Para agregar etiquetas al balanceador de carga

1. En la página **Add Tags**, especifique una clave y un valor para la etiqueta.
2. Para agregar otra etiqueta, seleccione **Create Tag** y especifique una clave y un valor para la etiqueta.
3. Una vez que haya terminado la adición de etiquetas, seleccione **Review and Create**.

4.8 Paso 7: Crear y probar el balanceador de carga

Antes de crear el balanceador de carga, revise la configuración que ha seleccionado. Después de crearlo, puede comprobar si el tráfico se envía a las instancias EC2.

Para crear y probar el balanceador de carga

1. En la página **Review**, elija **Create**.
2. Una vez que se le notifique que el balanceador de carga se ha creado correctamente, elija **Close**.
3. Seleccione el nuevo balanceador de carga.
4. En la pestaña **Description** (Descripción), compruebe la fila **Status** (Estado). Si se indica que algunas de las instancias no están operativas, es probable que se deba a que el proceso de registro aún está en curso. Para obtener más información, consulte Solución de problemas del balanceador de carga clásico: registro de instancias.
5. Cuando al menos una de las instancias EC2 esté operativa, puede probar el balanceador de carga. Copie la cadena de **DNS name** (Nombre DNS) (por ejemplo, my-load-balancer-1234567890.us-west-2.elb.amazonaws.com) y péguela en el campo de direcciones de un navegador web conectado a Internet. Si el balanceador de carga está en ejecución, consulte la página predeterminada del servidor.

4.9 Monitorización del balanceador de carga clásico

Puede utilizar las siguientes características para monitorizar los balanceadores de carga, analizar los patrones de tráfico y solucionar los problemas de los balanceadores de carga y de las instancias backend.

Métricas de CloudWatch

Elastic Load Balancing publica los puntos de datos en Amazon CloudWatch sobre los balanceadores de carga y las instancias backend. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos en un conjunto ordenado de datos de series temporales que reciben el nombre de **métricas**. Puede utilizar estas métricas para comprobar que el sistema funcione de acuerdo con lo esperado. Para obtener más información, consulte Métricas de CloudWatch para el balanceador de carga clásico.

Registros de acceso de Elastic Load Balancing

Los registros de acceso de Elastic Load Balancing capturan información detallada sobre las solicitudes realizadas al balanceador de carga y la almacenan en archivos registro en el bucket de Amazon S3 que especifique. Cada registro contiene detalles como la hora de recepción de la solicitud, la dirección IP del cliente, las latencias, la ruta de solicitud y las respuestas de servidor. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar los problemas con las aplicaciones backend. Para obtener más información, consulte Registros de acceso del balanceador de carga clásico.

Registros de CloudTrail

AWS CloudTrail permite realizar un seguimiento de las llamadas a la API de Elastic Load Balancing realizadas desde la cuenta de AWS o en nombre de ella. CloudTrail almacena la información en archivos registro en el bucket de Amazon S3 que especifique. Puede utilizar estos archivos registro para monitorizar la actividad de los balanceadores de carga determinando las solicitudes que se han llevado a cabo, las direcciones IP de origen desde las que proceden las solicitudes, quién ha efectuado la solicitud, cuándo se ha realizado, etc. Para obtener más información, consulte Registrar llamadas a la API del Classic Load Balancer a través de AWS CloudTrail.

5. Uso de VPC y subredes

Los procedimientos siguientes describen la creación manual de VPC y subredes. También tendrá que añadir manualmente gateways y tablas de ruteo. De manera alternativa, puede utilizar el asistente de Amazon VPC para crear una VPC y sus subredes, gateways y tablas de ruteo en un solo paso. Para obtener más información, consulte Escenarios y ejemplos.

Tareas

- Creación de una VPC
- Creación de una subred en la VPC
- Asociación de un bloque de CIDR IPv4 secundario con su VPC
- Asociación de un bloque de CIDR IPv6 a su VPC
- Asociación de un bloque de CIDR IPv6 a su subred
- Lanzamiento de una instancia en su subred
- Eliminación de su subred
- Desvinculación de un bloque de CIDR IPv4 de su VPC
- Anulación de la asociación de un bloque de CIDR IPv6 a su VPC o subred
- Eliminación de su VPC

5.1 Creación de una VPC

Puede crear una VPC vacía mediante la consola de Amazon VPC.

Para crear una VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Your VPCs**, **Create VPC**.
3. Especifique los siguientes detalles de VPC según sea necesario y elija **Create VPC**.
    - **Name tag**: indique, de manera opcional, un nombre para su VPC. Esta acción creará una etiqueta con una clave de `Name`y el valor que especifique.
    - **IPv4 CIDR block**: especifique un bloque de CIDR IPv4 para la VPC. Se recomienda especificar un bloque de CIDR de los rangos de direcciones IP privadas (no direccionables públicamente) tal como se especifica en RFC 1918. Por ejemplo, `10.0.0.0/16` o `192.168.0.0/16`.

      nota

      Puede especificar un rango de direcciones IPv4 direccionables públicamente; sin embargo, actualmente solo se admite el acceso directo a Internet desde bloques

de CIDR direccionables públicamente en una VPC. Las instancias de Windows no se podrán iniciar correctamente si se lanzan en una VPC con rangos que oscilan desde `224.0.0.0` a `255.255.255.255` (rangos de direcciones IP de clase D y clase E).

- **IPv6 CIDR block**: asocie, de manera opcional, un bloque de CIDR IPv6 a su VPC eligiendo un **bloque de CIDR IPv6 proporcionado por Amazon**.
- **Tenancy (Propiedad)**: seleccione una opción de propiedad. La tenencia dedicada garantiza que las instancias se ejecutan en hardware de un solo propietario. Para obtener más información, consulte Instancias dedicadas en la **Guía del usuario de Amazon EC2 para instancias de Linux**.

También puede utilizar una herramienta de la línea de comandos.

Para crear una VPC con una herramienta de la línea de comandos

- create-vpc (AWS CLI)
- New-EC2Vpc (Herramientas de AWS para Windows PowerShell)

Para describir una VPC con una herramienta de la línea de comandos

- describe-vpcs (AWS CLI)
- Get-EC2Vpc (Herramientas de AWS para Windows PowerShell)

Para obtener más información acerca de las direcciones IP, consulte Direcciones IP en su VPC.

Una vez creada la VPC, podrá crear las subredes. Para obtener más información, consulte Creación de una subred en la VPC.

5.2 Creación de una subred en la VPC

Para agregar una nueva subred a su VPC, deberá especificar un bloque de CIDR IPv4 para la subred del rango de su VPC. Puede especificar la zona de disponibilidad en la que desea que se encuentre la subred. Puede tener varias subredes en la misma zona de disponibilidad.

También puede especificar un bloque de CIDR IPv6 para su subred si el bloque de CIDR IPv6 está asociado a su VPC.

Para agregar una subred a su VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Subnets**, **Create Subnet**.
3. Especifique los detalles de la subred según sea necesario y elija **Create Subnet**.

- **Name tag**: indique, de manera opcional, un nombre para su subred. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
- **VPC**: elija la VPC para la que va a crear la subred.
- **Availability Zone**: elija, de manera opcional, la zona de disponibilidad en la que residirá su subred, o bien deje el valor predeterminado **No Preference** para que AWS elija una zona de disponibilidad por usted.
- **IPv4 CIDR block**: especifique un bloque de CIDR IPv4 para su subred. Por ejemplo, `10.0.1.0/24`. Para obtener más información, consulte Tamaño de subred Y VPC para direcciones IPv4.
- **IPv6 CIDR block**: (opcional) si ha asociado un bloque de CIDR IPv6 a su VPC, elija **Specify a custom IPv6 CIDR**. Especifique la pareja de valores hexadecimales de la subred, o bien deje el valor predeterminado.

4. (Optional) Si es necesario, repita los pasos anteriores para crear más subredes en su VPC.

También puede utilizar una herramienta de la línea de comandos.

Para agregar una subred con una herramienta de la línea de comandos

- create-subnet (AWS CLI)
- New-EC2Subnet (Herramientas de AWS para Windows PowerShell)

Para describir una subred con una herramienta de la línea de comandos

- describe-subnets (AWS CLI)
- Get-EC2Subnet (Herramientas de AWS para Windows PowerShell)

Una vez creada la subred, podrá hacer lo siguiente:

- Configurar el direccionamiento. Para convertir su subred en una subred pública, debe adjuntar un puerto de enlace a Internet a su VPC. Para obtener más información, consulte Creación y asociación de un puerto de enlace a Internet. A continuación, podrá crear una tabla de ruteo personalizada y agregar una ruta al puerto de enlace a Internet. Para obtener más información, consulte Crear una tabla de ruteo personalizada. Para obtener más opciones de direccionamiento, consulte Tablas de ruteo.
- Modificar la configuración de la subred para especificar que todas las instancias que se lancen en la subred reciban una dirección IPv4 pública, una dirección IPv6 o ambas cosas. Para obtener más información, consulte Comportamiento de las direcciones IP de su subred.

- Crear o modificar sus grupos de seguridad según sea necesario. Para obtener más información, consulte Grupos de seguridad de su VPC.
- Crear o modificar las ACL de red según sea necesario. Para obtener más información, consulte ACL de red.
- Compartir la subred con otras cuentas. Para obtener más información, consulte Cómo compartir una subred.

5.3 Asociación de un bloque de CIDR IPv4 secundario con su VPC

Puede agregar otro bloque de CIDR IPv4 a su VPC. No se olvide consultar las restricciones aplicables.

Después de haber asociado un bloque de CIDR, el estado cambia a `associating`. El bloque de CIDR está listo para usar cuando se encuentra en el estado `associated`.

Para agregar un bloque de CIDR a su VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Your VPCs**.
3. Seleccione la VPC y elija **Actions**, **Edit CIDRs**.
4. Elija **Add IPv4 CIDR** y escriba el bloque de CIDR que se agregará, por ejemplo, `10.2.0.0/16`. Seleccione el icono de marca de verificación.
5. Seleccione la opción **Close**.

También puede utilizar una herramienta de la línea de comandos.

Para agregar un bloque de CIDR con una herramienta de la línea de comandos

- associate-vpc-cidr-block (AWS CLI)
- Register-EC2VpcCidrBlock (Herramientas de AWS para Windows PowerShell)

Después de haber agregado los bloques de CIDR IPv4 que necesita, puede crear las subredes. Para obtener más información, consulte Creación de una subred en la VPC.

5.4 Asociación de un bloque de CIDR IPv6 a su VPC

Es posible asociar un bloque de CIDR IPv6 a cualquier VPC existente. La VPC no puede tener ningún bloque de CIDR IPv6 asociado.

Para asociar un bloque de CIDR IPv6 a una VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, elija **Your VPCs**.
3. Seleccione su VPC, elija **Actions**, **Edit CIDRs**.
4. Elija **Add IPv6 CIDR**. Una vez añadido el bloque de CIDR IPv6, elija **Close**.

También puede utilizar una herramienta de la línea de comandos.

Para asociar un bloque de CIDR IPv6 a una VPC con una herramienta de la línea de comandos

- associate-vpc-cidr-block (AWS CLI)
- Register-EC2VpcCidrBlock (Herramientas de AWS para Windows PowerShell)

5.5 Asociación de un bloque de CIDR IPv6 a su subred

Puede asociar un bloque de CIDR IPv6 a una subred existente de su VPC. La subred no puede tener ningún bloque de CIDR IPv6 asociado.

Para asociar un bloque de CIDR IPv6 a una subred con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Subnets**.
3. Seleccione su subred, elija **Subnet Actions**, **Edit IPv6 CIDRs**.
4. Elija **Add IPv6 CIDR**. Especifique la pareja de valores hexadecimales para la subred (por ejemplo, `00`) y confirme la entrada seleccionando el icono de marca de verificación.
5. Seleccione la opción **Close**.

También puede utilizar una herramienta de la línea de comandos.

Para asociar un bloque de CIDR IPv6 a una subred con una herramienta de la línea de comandos

- associate-subnet-cidr-block (AWS CLI)
- Register-EC2SubnetCidrBlock (Herramientas de AWS para Windows PowerShell)

5.6 Lanzamiento de una instancia en su subred

Una vez creada la subred y configurado el direccionamiento, podrá lanzar la instancia en su subred mediante la consola de Amazon EC2.

Para lanzar una instancia en su subred privada con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En el panel, elija **Launch Instance**.
3. Siga las indicaciones del asistente. Seleccione una AMI y un tipo de instancia y, a continuación, elija **Next: Configure Instance Details**.

   nota

   Si desea que su instancia se comunique mediante IPv6, debe seleccionar un tipo de instancia compatible. Todos los tipos de instancia de la generación actual admiten direcciones IPv6.

4. En la página **Configure Instance Details**, asegúrese de haber seleccionado la VPC necesaria en la lista **Network**. A continuación, seleccione la subred en la que desea lanzar la instancia. Deje las demás opciones predeterminadas de la página y elija **Next: Add Storage**.
5. En las páginas siguientes del asistente, podrá configurar el almacenamiento de su instancia y añadir etiquetas. En la página **Configure Security Group**, elija uno de los grupos de seguridad existentes de su propiedad, o bien siga las instrucciones del asistente para crear un nuevo grupo de seguridad. Elija **Review and Launch** cuando haya terminado.
6. Revise la configuración y elija **Launch**.
7. Seleccione un par de claves de su propiedad o cree uno nuevo. A continuación, elija **Launch Instances** cuando haya terminado.

También puede utilizar una herramienta de la línea de comandos.

Para lanzar una instancia en su subred privada con una herramienta de la línea de comandos

- run-instances (AWS CLI)
- New-EC2Instance (Herramientas de AWS para Windows PowerShell)

5.7 Eliminación de su subred

Si ya no necesita su subred, puede eliminarla. Para ello, antes deberá terminar las instancias de la subred.

Para eliminar su subred con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Termine todas las instancias de la subred. Para obtener más información, consulte Terminar una instancia en la **Guía del usuario de EC2**.

3. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
4. En el panel de navegación, elija **Subnets**.
5. Seleccione la subred que desea eliminar y elija **Subnet Actions (Acciones de subred)** y, a continuación, **Delete Subnet (Eliminar subred)**.
6. En el cuadro de diálogo **Delete Subnet**, elija **Yes, Delete**.

También puede utilizar una herramienta de la línea de comandos.

Para eliminar una subred con una herramienta de la línea de comandos

- delete-subnet (AWS CLI)
- Remove-EC2Subnet (Herramientas de AWS para Windows PowerShell)

5.8 Desvinculación de un bloque de CIDR IPv4 de su VPC

Si su VPC tiene varios bloques de CIDR IPv4 asociados a ella, puede desvincular un bloque de CIDR IPv4 de la VPC. No se puede desvincular el bloque de CIDR IPv4 principal. Solo se puede desvincular un bloque de CIDR completo, es decir, no se puede desvincular un subconjunto de un bloque de CIDR o un rango fusionado de bloques de CIDR. Primero debe eliminar todas las subredes del bloque de CIDR.

Para eliminar un bloque de CIDR de una VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Your VPCs**.
3. Seleccione la VPC y elija **Actions**, **Edit CIDRs**.
4. En **VPC IPv4 CIDRs**, elija el botón de eliminación (una cruz) correspondiente al bloque de CIDR que se eliminará.
5. Seleccione la opción **Close**.

También puede utilizar una herramienta de la línea de comandos.

Para eliminar un bloque de CIDR IPv4 de una VPC con una herramienta de la línea de comandos

- disassociate-vpc-cidr-block (AWS CLI)
- Unregister-EC2VpcCidrBlock (Herramientas de AWS para Windows PowerShell)

5.9 Anulación de la asociación de un bloque de CIDR IPv6 a su VPC o subred

Si ya no desea que su VPC o subred admitan IPv6 pero desea seguir utilizando su VPC o su subred para crear y comunicarse con recursos IPv4, puede anular la asociación del bloque de CIDR IPv6.

Para anular la asociación de un bloque de CIDR IPv6, primero deberá anular la asignación de las direcciones IPv6 asignadas a las instancias de su subred. Para obtener más información, consulte Anulación de la asignación de una dirección IPv6 de una instancia.

Para desvincular un bloque de CIDR IPv6 de una subred con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Subnets**.
3. Seleccione su subred, elija **Subnet Actions**, **Edit IPv6 CIDRs**.
4. Elimine el bloque de CIDR IPv6 de la subred seleccionando el icono con forma de equis.
5. Seleccione la opción **Close**.

Para desvincular un bloque de CIDR IPv6 de una VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija **Your VPCs**.
3. Seleccione su VPC, elija **Actions**, **Edit CIDRs**.
4. Elimine el bloque de CIDR IPv6 seleccionando el icono con forma de equis.
5. Seleccione la opción **Close**.

nota

La anulación de la asociación de un bloque de CIDR IPv6 no elimina automáticamente las reglas del grupo de seguridad, las reglas de ACL de red ni las rutas de las tablas de ruteo configuradas para las redes IPv6. Por lo tanto, deberá modificar o eliminar manualmente dichas reglas o rutas.

También puede utilizar una herramienta de la línea de comandos.

Para desvincular un bloque de CIDR IPv6 de una subred con una herramienta de la línea de comandos

- disassociate-subnet-cidr-block (AWS CLI)
- Unregister-EC2SubnetCidrBlock (Herramientas de AWS para Windows PowerShell)

Para desvincular un bloque de CIDR IPv6 de una VPC con una herramienta de la línea de comandos

- disassociate-vpc-cidr-block (AWS CLI)
- Unregister-EC2VpcCidrBlock (Herramientas de AWS para Windows PowerShell)

6. Comprobar capacidades de autoescalemiento

Puede crear una configuración de lanzamiento y un grupo de Auto Scaling en un único procedimiento mediante el asistente de lanzamiento de Amazon EC2. Esto resulta útil si va a lanzar varias instancias y desea crear una nueva configuración de lanzamiento y un nuevo grupo de Auto Scaling desde la configuración que ha seleccionado en el asistente de lanzamiento de Amazon EC2. No puede utilizar esta opción para crear un grupo de Auto Scaling utilizando una configuración de lanzamiento existente.

Para crear una configuración de lanzamiento y un grupo de Auto Scaling con el asistente de lanzamiento

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija **Launch Instance**.
3. Elija una AMI, seleccione un tipo de instancia en la página siguiente y después haga clic en **Next: Configure Instance Details**.
4. En **Number of instances**, especifique el número de instancias que desea lanzar y seleccione **Launch into Auto Scaling Group**. No es necesario que añada otros detalles de configuración en la página.
5. En la página de confirmación, seleccione **Create Launch Configuration**.
6. Estará ahora en el paso 3 del asistente de configuración de lanzamiento. La AMI y el tipo de instancia ya están seleccionados de acuerdo con las opciones seleccionadas en el asistente de lanzamiento de Amazon EC2. Especifique un nombre para la configuración de lanzamiento, establezca las demás opciones según sea necesario y seleccione **Next: Add Storage**.
7. Configure cualquier otro volumen y seleccione **Next: Configure Security Group**.
8. Cree un nuevo grupo de seguridad o seleccione un grupo existente y haga clic en **Review**.
9. Examine los detalles de la configuración de lanzamiento y seleccione **Create launch configuration** para elegir un par de claves y crear la configuración de lanzamiento.
10. En la página **Configure Auto Scaling group details (Configurar los detalles del grupo de)**, la configuración de lanzamiento que ha creado ya está seleccionada y el número de

instancias que ha especificado en el asistente de lanzamiento de Amazon EC2 se indica en **Group size (Tamaño del grupo)**. Escriba un nombre para el grupo, especifique una VPC y una subred (si es necesario) y seleccione **Next: Configure scaling policies**.

11. En la página **Configure scaling policies**, elija una de las siguientes opciones y haga clic en **Review**:
    - Para ajustar manualmente el tamaño del grupo de Auto Scaling en función de las necesidades, elija **Keep this group at its initial size (Conservar el tamaño inicial de este grupo)**. Para obtener más información, consulte Escalado manual de Amazon EC2 Auto Scaling.
    - Para ajustar automáticamente el tamaño del grupo de Auto Scaling en función de los criterios que se especifiquen, elija **Use scaling policies to adjust the capacity of this group (Usar las políticas de escalado para ajustar la capacidad de este grupo)** y siga las instrucciones. Para obtener más información, consulte Configurar políticas de escalado.
12. Si lo desea, en la página **Review**, puede agregar etiquetas o notificaciones y editar otros detalles de configuración. Cuando haya terminado, seleccione **Create Auto Scaling group (Crear grupo de)**.

7. Cambio del tipo de instancia

A medida que sus necesidades cambian, podría descubrir que su instancia está sobreutilizada (el tipo de instancia es demasiado pequeña) o infrautilizada (el tipo de instancia es demasiado grande). Si es así, puede cambiar el tamaño de la instancia. Por ejemplo, si la instancia `t2.micro` es demasiado pequeña para su carga de trabajo, puede cambiarla por otro tipo de instancia que sea adecuada para la carga de trabajo.

También puede ser conveniente migrar un tipo de instancia de una generación anterior al tipo de instancia de una generación actual para sacar partido de algunas características, como la compatibilidad con IPv6, por ejemplo.

Si el dispositivo raíz de la instancia es un volumen de EBS, puede cambiar el tamaño de la instancia simplemente cambiando el tipo de instancia, lo que se conoce como **redimensionamiento**. Si el dispositivo raíz de la instancia es un volumen del almacén de instancias, debe migrar la aplicación a una instancia nueva con el tipo de instancia que necesita. Para obtener más información acerca de los volúmenes de dispositivo raíz, consulte Almacenamiento del dispositivo raíz.

Al cambiar el tamaño de una instancia, debe seleccionar un tipo de instancia que sea compatible con la configuración de la instancia. Si el tipo de instancia que desea no es compatible con la configuración de la instancia que tiene, debe migrar la aplicación a una instancia nueva con el tipo de instancia que necesita.

importante

Al redimensionar una instancia, la instancia redimensionada suele tener el mismo número de volúmenes del almacén de instancias que especificó cuando lanzó la instancia original. Con tipos de instancia que admiten volúmenes de almacenes de instancia NVMe (que están disponibles de forma predeterminada), la instancia redimensionada podría tener volúmenes de almacenamiento de instancia adicionales, en función de la AMI. De lo contrario, puede migrar la aplicación a una instancia con un nuevo tipo de instancia manualmente, especificando el número de volúmenes de almacenes de instancia que necesita al lanzar la nueva instancia.

Contenido

- Compatibilidad con el redimensionamiento de instancias
- Redimensionamiento de una instancia respaldada por Amazon EBS
- Migración de una instancia con respaldo en el almacén de instancias
- Migración a una nueva configuración de instancia

7.1 Compatibilidad con el redimensionamiento de instancias

Solo es posible redimensionar una instancia si el tipo de instancia actual y el nuevo tipo de instancia que desea son compatibles de las siguientes formas:

- **Tipo de virtualización**: las AMI de Linux utilizan uno de estos tipos de virtualización: paravirtual (PV) o máquina virtual de hardware (HVM). No puede redimensionar una instancia que se ha lanzado desde una AMI PV en un tipo de instancia que solo es HVM. Para obtener más información, consulte Tipos de virtualización de AMI de Linux. Para comprobar el tipo de virtualización de la instancia, consulte el campo **Virtualization (Virtualización)** en el panel de detalles de la pantalla **Instances (Instancias)** de la consola de Amazon EC2.
- **Arquitectura**: las AMI son específicas de la arquitectura del procesador, por lo que debe seleccionar un tipo de instancia con la misma arquitectura de procesador que el tipo de instancia actual. Por ejemplo:
    - Las instancias A1 son las únicas instancias que admiten procesadores basados en la arquitectura Arm. Si redimensiona un tipo de instancia con un procesador

basado en la arquitectura Arm, se limita a los tipos de instancias que admiten un procesador basado en la arquitectura Arm.
    - Los siguientes tipos de instancia son los únicos tipos de instancia que admiten AMIs de 32 bits: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` y `c1.medium`. Si va a redimensionar una instancia de 32 bits, está limitado a estos tipos de instancias.
- **Red**: los tipos de instancias más recientes deben lanzarse en una VPC. Por lo tanto, no puede redimensionar una instancia en la plataforma EC2-Classic a un tipo de instancia que solo está disponible en una VPC, a menos que tenga una VPC no predeterminada. Para comprobar si la instancia está en una VPC, compruebe el valor de **VPC ID (ID de la VPC)** en el panel de detalles de la pantalla **Instances (Instancias)** de la consola de Amazon EC2. Para obtener más información, consulte Migración de una instancia de Linux en EC2-Classic a una instancia de Linux en una VPC.
- **Redes mejoradas**: los tipos de instancias que admiten redes mejoradas requieren que los controladores necesarios estén instalados. Por ejemplo, los tipos de instancias A1, C5, C5d, C5n, I3en, M5, M5a, M5ad, M5d, `p3dn.24xlarge`, R5, R5a, R5ad, R5d, T3, T3a y z1d requieren AMI respaldadas por EBS con los controladores Elastic Network Adapter (ENA) instalados. Para cambiar el tamaño de una instancia existente a un tipo de instancia que admita redes mejoradas, primero tendrá que instalar los controladores ENA o los controladores ixgbevf en la instancia, según corresponda.
- **NVMe**: los volúmenes de EBS se exponen como dispositivos de bloques NVMe en las instancias basadas en Nitro. Si redimensiona una instancia de un tipo de instancia que no admite NVMe a un tipo de instancia que admite NVMe, primero debe instalar los controladores NVMe en la instancia. Además, los nombres de los dispositivos que especifique en el mapeo de dispositivos de bloques se cambian por los nombres de los dispositivos NVMe (`/dev/nvme[0-26]n1`). Por lo tanto, para montar sistemas de archivos en el momento del arranque usando `/etc/fstab`, debe utilizar el UUID o la etiqueta en lugar de los nombres de los dispositivos.
- **AMI**: para obtener más información sobre las AMI necesarias para los tipos de instancias que admiten las redes mejoradas y NVMe, consulte las Notas de la versión en la documentación siguiente.
    - Instancias de uso general
    - Instancias optimizadas para computación
    - Instancias optimizadas para memoria
    - Instancias optimizadas para almacenamiento

7.2 Redimensionamiento de una instancia respaldada por Amazon EBS

Debe detener la instancia respaldada por Amazon EBS para poder cambiar su tipo de instancia. Cuando se para y se inicia una instancia, tenga en cuenta lo siguiente:

- La instancia se mueve a un nuevo hardware, pero el ID de instancia no cambia.
- Si la instancia tiene una dirección IPv4 pública, liberamos la dirección y le asignamos una nueva dirección IPv4 pública. La instancia conserva sus direcciones IPv4 privadas, las direcciones IP elásticas y las direcciones IPv6.
- Si la instancia pertenece a un grupo de Auto Scaling el servicio Amazon EC2 Auto Scaling marca la instancia detenida como en mal estado y podría terminarla y lanzar una instancia de sustitución. Para evitar esto, puede suspender los procesos de escalado del grupo mientras redimensiona la instancia. Para obtener más información, consulte Suspender y reanudar procesos de escalado en la **Guía del usuario de Amazon EC2 Auto Scaling**.
- Si la instancia está en un grupo de ubicación en clúster y después de cambiar el tipo de instancia comienza a experimentar errores, pruebe lo siguiente: detenga todas las instancias del grupo de ubicación en clúster, cambie la instancia a otro tipo y reinicie todas las instancias del grupo de ubicación en clúster.
- Asegúrese de tener previsto un tiempo de inactividad mientras la instancia está detenida. La parada y el redimensionamiento de una instancia puede tardar unos minutos y el tiempo que se tarda en reiniciar la instancia es variable, en función de los scripts de inicio de la aplicación.

Para obtener más información, consulte Detener e iniciar la instancia.

Utilice el siguiente procedimiento para redimensionar una instancia respaldada por Amazon EBS utilizando la Consola de administración de AWS.

Para redimensionar una instancia respaldada por Amazon EBS

1. (Opcional) Si el nuevo tipo de instancia requiere controladores que no están instalados en la instancia existente, debe conectarse a la instancia e instalar primero los controladores. Para obtener más información, consulte Compatibilidad con el redimensionamiento de instancias.
2. Abra la consola de Amazon EC2.
3. En el panel de navegación, seleccione **Instances (Instancias)**.
4. Seleccione la instancia y elija **Actions (Acciones)**, **Instance State (Estado de la instancia)** y **Stop (Detener)**.

5. En el cuadro de diálogo de confirmación, elija **Yes, Stop (Sí, detener)**. Puede que transcurran unos minutos hasta que la instancia se detenga.
6. Con la instancia aún seleccionada, elija **Actions**, **Instance Settings**, **Change Instance Type**. Esta acción estará deshabilitada si el estado de la instancia no es `stopped`.
7. En el cuadro de diálogo **Change Instance Type (Cambiar tipo de instancia)**, haga lo siguiente:
    a. En **Instance Type (Tipo de instancia)**, seleccione el tipo de instancia que desea. Si el tipo de instancia que desea no aparece en la lista, eso significa que no es compatible con la configuración de la instancia (por ejemplo, debido al tipo de virtualización). Para obtener más información, consulte Compatibilidad con el redimensionamiento de instancias.
    b. (Opcional) Si el tipo de instancia que ha seleccionado admite la optimización de EBS, seleccione **EBS-optimized (Optimizada para EBS)** para habilitar la optimización de EBS o anule la selección de **EBS-optimized (Optimizada para EBS)** para deshabilitarla. Si el tipo de instancia que ha seleccionado está optimizado para–EBS de manera predeterminada, la opción **EBS-optimized (Optimizada para EBS)** estará seleccionada y no podrá anular la selección.
    c. Elija **Apply (Aplicar)** para aceptar la nueva configuración.
8. Para reiniciar la instancia detenida, seleccione la instancia y elija **Actions**, **Instance State**, **Start**.
9. En el cuadro de diálogo de confirmación, elija **Yes, Start (Sí, iniciar)**. Puede que transcurran unos minutos hasta que la instancia pase al estado `running`.
10. (Solución de problemas) Si la instancia no arranca, es posible que no se cumpla uno de los requisitos para el nuevo tipo de instancia. Para obtener más información, consulte el tema donde se explica porqué no arranca una instancia de Linux después de cambiar su tipo.

7.3 Migración de una instancia con respaldo en el almacén de instancias

Si desea mover la aplicación desde una instancia con respaldo en el almacén de instancias a una instancia con respaldo en el almacén de instancias de un tipo diferente, debe migrarla creando una imagen de la instancia y luego lanzando una nueva instancia desde esta imagen con el tipo de instancia que necesita. Para garantizar que los usuarios puedan seguir utilizando las aplicaciones que aloja en la instancia de manera ininterrumpida, debe volver a asociar con la nueva instancia cualquier dirección IP elástica que estuviera asociada con la instancia original. Luego, puede terminar la instancia original.

Para migrar una instancia con respaldo del almacén de instancias

1. Realice un backup de los datos de los volúmenes de almacén de instancias que necesite conservar en un almacenamiento persistente. Para migrar datos en los volúmenes de EBS que necesite conservar, realice una instantánea de los volúmenes (consulte Creación de instantáneas de Amazon EBS) o separe el volumen de la instancia para poder adjuntarlo a la nueva instancia más adelante (consulte Separación de un volumen de Amazon EBS de una instancia).
2. Cree una AMI desde la instancia con respaldo en el almacén de instancias cumpliendo los requisitos previos y siguiendo los procedimientos de Creación de una AMI de Linux con respaldo en el almacén de instancias. Cuando haya terminado de crear una AMI desde la instancia, regrese a este procedimiento.
3. Abra la consola de Amazon EC2 y, en el panel de navegación, seleccione **AMIs**. En la lista de filtros, seleccione **Owned by me (De mi propiedad)** y la imagen que creó en el paso anterior. Observe que **AMI Name (Nombre de AMI)** es el nombre que especificó al registrar la imagen y **Source (Origen)** es el bucket de Amazon S3.

   nota

   Si no ve la AMI que creó en el paso anterior, compruebe que ha seleccionado la región en la que creó la AMI.

4. Elija **Launch**. Cuando especifique opciones para la instancia, asegúrese de seleccionar el nuevo tipo de instancia que desee. Si el tipo de instancia que desea no se puede seleccionar, eso significa que no es compatible con la configuración de la AMI que ha creado (por ejemplo, debido al tipo de virtualización). También puede especificar cualquier volumen de EBS que haya separado de la instancia original.

   Puede que transcurran unos minutos hasta que la instancia pase al estado `running`.

5. (Opcional) Puede terminar la instancia con la que ha comenzado si ya no la necesita. Seleccione la instancia y compruebe que está a punto de terminar la instancia original, no la nueva (por ejemplo, compruebe el nombre o la hora de lanzamiento). Haga clic en **Actions (Acciones)**, **Instance State (Estado de la instancia)** y **Terminate (Terminar)**.

7.4 Migración a una nueva configuración de instancia

Si la configuración actual de la instancia es incompatible con el tipo de instancia nuevo que desea, no podrá redimensionar la instancia a ese tipo de instancia. En su lugar, puede migrar la aplicación a una nueva instancia con una configuración que sea compatible con el nuevo tipo de instancia que desea.

Si desea moverse desde una instancia que se ha lanzado desde una AMI PV a un tipo de instancia que solo es HVM, este es el proceso general:

Para migrar la aplicación a una instancia compatible

1. Realice un backup de los datos de los volúmenes de almacén de instancias que necesite conservar en un almacenamiento persistente. Para migrar datos en los volúmenes de EBS que necesite conservar, cree una instantánea de los volúmenes (consulte Creación de instantáneas de Amazon EBS) o separe el volumen de la instancia para poder adjuntarlo a la nueva instancia más adelante (consulte Separación de un volumen de Amazon EBS de una instancia).
2. Lance una instancia nueva. Seleccione lo siguiente:
    - Una AMI de HVM
    - El tipo de instancia solo HVM
    - Si utiliza una dirección IP elástica, seleccione la VPC en la que se está ejecutando actualmente la instancia original.
    - Los volúmenes de EBS que ha separado de la instancia original y que desea adjuntar a la nueva instancia o los volúmenes de EBS nuevos basados en las instantáneas que ha creado.
    - Si desea permitir el mismo tráfico para obtener acceso a la nueva instancia, seleccione el grupo de seguridad que está asociado a la instancia original.
3. Instale la aplicación y todo el software necesario en la instancia.
4. Realice un backup de los datos de los volúmenes de almacén de instancias de la instancia original.
5. Si utiliza una dirección IP elástica, asígnela a la instancia que acaba de lanzar de la siguiente manera:
    - En el panel de navegación, elija **Elastic IPs (Direcciones IP elásticas)**.
    - Seleccione la dirección IP elástica que está asociada a la instancia original y haga clic en **Actions (Acciones)** y **Disassociate address (Desasociar dirección)**. Cuando se le pida que confirme, elija **Disassociate address (Desasociar dirección)**.
    - Con la dirección IP elástica aún seleccionada, haga clic en **Actions (Acciones)** y en **Associate address (Asociar dirección)**.
    - En **Instance (Instancia)**, seleccione la nueva instancia y luego elija **Associate (Asociar)**.
6. (Opcional) Puede terminar la instancia original si ya no la necesita. Seleccione la instancia y compruebe que está a punto de terminar la instancia original, no la nueva (por ejemplo, compruebe el nombre o la hora de lanzamiento). Elija **Actions (Acciones)**, **Instance State (Estado de la instancia)**, **Terminate (Terminar)**.

8. Creación de un plan de copias de seguridad

Cuando se crea un plan de copias de seguridad, se añade al conjunto de planes de su cuenta.

8.1 Mediante la Consola de administración de AWS

AWS Backup ofrece tres formas de empezar utilizando la consola de AWS Backup.

- Empiece a partir de un plan existente: puede crear un nuevo plan de copias de seguridad basado en las configuraciones de un plan existente. Puede comenzar desde un plan de copias de seguridad existente que ha creado o comenzar a partir de un plan existente creado por AWS Backup. Los planes de copias de seguridad creados por AWS Backup se basan en las prácticas recomendadas de copia de seguridad y en las configuraciones de política de copia de seguridad comunes. Cuando seleccione un plan de copia de seguridad existente las configuraciones de dicho plan de copia de seguridad se rellenan automáticamente para el nuevo plan de copias de seguridad. Luego podrá cambiar cualquier configuración en función de sus necesidades de copias de seguridad.
- Crear un nuevo plan desde cero: puede crear un nuevo plan de copias de seguridad especificado cada uno de los detalles de la configuración de copia de seguridad. Puede elegir entre las configuraciones predeterminadas recomendadas.
- Definir un plan con JSON: puede modificar la expresión JSON de planes de copia de seguridad que ya existen y, a continuación, crear nuevos planes de copias de seguridad basados en las configuraciones definidas en la expresión JSON. A continuación, puede compartir planes de copia de seguridad con otras cuentas de AWS, lo que a su vez le permite asegurarse de que las cuentas de AWS de su organización compartan las mismas configuraciones de copia de seguridad.

Para obtener instrucciones paso a paso para crear un plan de copias de seguridad, consulte Creación de un plan de copias de seguridad mediante la modificación de uno existente en la sección Introducción.

8.2 Opciones de plan de copias de seguridad y configuración

Al definir un plan de copias de seguridad en la consola de AWS Backup, configure las siguientes opciones:

8.2.1 Nombre del plan de copias de seguridad

Debe proporcionar un nombre único de plan de copias de seguridad.

8.2.2 Reglas de copia de seguridad

Los planes de copias de seguridad se componen de una o más reglas de copia de seguridad. Cada regla de copia de seguridad consta de los siguientes elementos.

8.2.2.1 Nombre de la regla de copia de seguridad

Los nombres de la regla de copia de seguridad distinguen mayúsculas de minúsculas. Deben contener de 1 a 63 caracteres alfanuméricos o guiones.

8.2.2.2 Frecuencia de copia de seguridad

La frecuencia de copia de seguridad determina la frecuencia con la que se crea una copia de seguridad. Puede elegir una frecuencia de cada 12 horas, diaria, semanal o mensual. Al seleccionar cada semana, puede especificar en qué días de la semana desea que se lleven a cabo las copias de seguridad. Al seleccionar mensual, puede elegir un día determinado del mes.

8.2.2.3 Periodo de copia de seguridad

Los periodos de copia de seguridad constan de la hora de comienzo del periodo de copia de seguridad y de la duración del periodo indicada en horas. Los trabajos de copia de seguridad comienzan dentro de este periodo. Si no está seguro de qué periodo de copia de seguridad utilizar, puede optar por usar el periodo de copia de seguridad predeterminado que AWS Backup recomienda. El valor predeterminado del periodo de copia de seguridad está establecido para comenzar a las 5 de la mañana UTC y dura 8 horas.

nota

Puede personalizar la frecuencia de las copias de seguridad y la hora de inicio del periodo de copia de seguridad mediante una expresión cron. Para obtener más información acerca de las expresiones cron, consulte Programar expresiones para reglas en la **Guía del usuario de Amazon CloudWatch Events**.

8.2.2.4 Ciclo de vida

El ciclo de vida define el momento en que se migra una copia de seguridad al almacenamiento en frío y cuándo dicho recurso vence. AWS Backup migra y da por vencidas automáticamente las copias de seguridad en función del ciclo de vida que se defina. Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola el valor de "expire after days" (número de días tras los cuales caducará) debe tener 90 días más que el valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío). El valor de "transition to cold after days"

(número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

nota

Actualmente, solo las copias de seguridad de sistema de archivos Amazon EFS se pueden migrar a almacenamiento en frío. La expresión de almacenamiento en frío se omite para las copias de seguridad de Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS) Amazon DynamoDB y AWS Storage Gateway.

8.2.2.5 Almacén de copias de seguridad

Un almacén de copias de seguridad es un contenedor que sirve para organizar sus copias de seguridad. Las copias de seguridad creadas por una regla de copia de seguridad se organizan en el almacén de copia de seguridad que especifique en la regla de copia de seguridad. Puede utilizar los almacenes de copias de seguridad para establecer la clave de cifrado de AWS Key Management Service (AWS KMS) que se utiliza para cifrar las copias de seguridad del almacén de copias de seguridad y para controlar el acceso a las copias de seguridad de dicho almacén. Puede añadir también etiquetas a los almacenes de copias de seguridad para organizarlos. Si no desea utilizar el almacén predeterminado, puede crear el suyo propio. Para obtener instrucciones paso a paso para la creación de un almacén de copias de seguridad, consulte Crear un almacén de copias de seguridad.

8.2.2.6 Etiquetas añadidas a puntos de recuperación

Las etiquetas que enumere aquí se añaden automáticamente a las copias de seguridad cuando se crean.

8.2.3 Etiquetas añadidas a planes de copias de seguridad

Estas etiquetas están asociadas con el propio plan de copias de seguridad para ayudarle a organizar y realizar un seguimiento de su plan de copias de seguridad.

9. Creación de Snapshots EBS

Puede crear una instantánea de un momento determinado de un volumen de EBS y utilizarla como punto de referencia de nuevos volúmenes o para hacer una copia de seguridad de los datos. Si hace instantáneas periódicas de un volumen, serán incrementales, es decir, solo los bloques del dispositivo que han cambiado después de la última instantánea se guardan en la nueva. Aunque las instantáneas se guarden de forma incremental, su proceso de eliminación está diseñado para que solo tenga que retener la instantánea más reciente para restaurar el volumen completo.

Las instantáneas se realizan de una manera asíncrona, es decir, la instantánea de un momento dado se crea inmediatamente, pero su estado es `pending` hasta que se completa (cuando todos los bloques modificados se han trasferido a Amazon S3), algo que puede tardar varias horas si las instantáneas iniciales son grandes o si las siguientes tienen muchos bloques que han cambiado. Mientras se completa, no le afectan las lecturas y escrituras continuas en el volumen.

Puede tomar una instantánea de un volumen adjunto que esté en uso. Sin embargo, las instantáneas solo capturan los datos que se han escrito en el volumen de Amazon EBS en el momento que se lanza el comando snapshot. Esto puede excluir los datos que las aplicaciones o el sistema operativo hayan guardado en la memoria caché. Si puede poner en pausa la escritura de archivos en el volumen el tiempo suficiente para tomar una instantánea, esta instantánea debería ser completa. Sin embargo, si no puede detener la escritura en los archivos del volumen, debe desmontarlo de la instancia, emitir el comando snapshot y después volver a montar el volumen para asegurarse de que la instantánea esté completa y sea coherente. Puede volver a montar y usar el volumen siempre que el estado de la instantánea sea `pending`.

Para facilitar la administración de las instantáneas, puede etiquetarlas durante la creación o añadirles etiquetas más tarde. Por ejemplo, puede aplicar etiquetas que describan el volumen original a partir del que se creó la instantánea o el nombre del dispositivo utilizado para adjuntar el volumen original a una instancia. Para obtener más información, consulte Etiquetado de los recursos de Amazon EC2.

9.1 Cifrado de instantáneas

Las instantáneas que se crean a partir de volúmenes cifrados se cifran automáticamente. Los volúmenes que se crean a partir de instantáneas cifradas también se cifran automáticamente. Los datos de los volúmenes cifrados y cualquier instantánea asociada se protegen tanto en movimiento como parados. Para obtener más información, consulte Amazon EBS Encryption.

De manera predeterminada, solo puede crear volúmenes de instantáneas que sean de su propiedad. Sin embargo, puede compartir las instantáneas no cifradas con cuentas de AWS específicas o puede compartirlas con toda la comunidad de AWS haciéndolas públicas. Para obtener más información, consulte Uso compartido de una instantánea de Amazon EBS.

Puede compartir una instantánea cifrada solo con cuentas específicas de AWS. Para que otras personas usen la instantánea cifrada que ha compartido, debe también compartir la clave CMK empleada para cifrarla. Los usuarios con acceso a la instantánea cifrada deben crear una copia personal de la misma y usarla para restaurar el volumen. La copia de una instantánea cifrada y compartida también se puede cifrar de nuevo con una clave diferente. Para obtener más información, consulte Uso compartido de una instantánea de Amazon EBS.

nota

Si copia una instantánea y la cifra con una nueva CMK, siempre se crea una copia completa (no incremental), lo que se traduce en costos de almacenamiento y retrasos adicionales.

9.2 Instantáneas de varios volúmenes

Puede crear instantáneas de varios volúmenes, que son instantáneas de un momento dado de todos los volúmenes de EBS asociados a una única instancia EC2. También puede crear políticas de ciclo de vida para automatizar la creación y la retención de instantáneas de varios volúmenes. Para obtener más información, consulte Automatización del ciclo de vida de instantáneas de Amazon EBS.

Después de crear las instantáneas, cada una de ellas se trata como una instantánea individual. Puede realizar todas las operaciones relacionadas con las instantáneas, como restaurar, eliminar y copiar entre cuentas/regiones, como lo haría con una única instantánea de volumen. También puede etiquetar las instantáneas de varios volúmenes como lo haría con una única instantánea de volumen. Le recomendamos que etiquete sus instantáneas de varios volúmenes para gestionarlas de manera conjunta durante el proceso de restauración, copia o retención.

Las instantáneas coherentes frente a bloqueos de varios volúmenes se restauran habitualmente como un conjunto. Resulta útil identificar las instantáneas que se encuentran en un conjunto coherente frente a bloqueos etiquetando dicho conjunto con el ID de la instancia, el nombre u otros datos relevantes. También puede elegir copiar automáticamente las etiquetas del volumen de origen en las instantáneas correspondientes. Esta opción sirve de ayuda para configurar los metadatos de la instantánea, como las políticas de acceso, la información adjunta y la asignación de costos, para que coincidan con el volumen de origen.

Tras su creación, una instantánea de varios volúmenes actúa como cualquier otra instantánea. Puede llevar a cabo todas las operaciones, como restaurar, eliminar y copiar entre regiones y cuentas. También puede etiquetar sus instantáneas. Le recomendamos que etiquete sus instantáneas de varios volúmenes para gestionarlas de manera conjunta durante el proceso de restauración, copia o retención.

Tras crear las instantáneas, estas aparecerán en la consola de EC2 creadas en el momento dado exacto. Las instantáneas se gestionan de manera conjunta y, por tanto, si cualquier instantánea del conjunto de volúmenes da error, el resto de las instantáneas mostrarán un estado de error.

9.3 Consideraciones

Las siguientes consideraciones se aplican a la creación de instantáneas:

- Al crear una instantánea para un volumen de EBS que actúa como dispositivo raíz, debe parar la instancia antes de tomar la instantánea.
- No puede crear instantáneas a partir de instancias para las que la hibernación está habilitada.
- No puede crear instantáneas a partir de instancias hibernadas.
- Aunque puede tomar una instantánea de un volumen mientras una instantánea previa de dicho volumen se encuentra en estado `pending`, muchas instantáneas `pending` de un volumen pueden reducir el rendimiento del volumen hasta que terminan.
- Existe un límite de cinco instantáneas `pending` para un único volumen `gp2`, `io1` o Magnético, y de una instantánea `pending`para un único volumen `st1` o `sc1`. Si recibe un error `ConcurrentSnapshotLimitExceeded` mientras intenta crear varias instantáneas a la vez del mismo volumen, espere hasta que una o varias de las instantáneas `pending` se hayan completado antes de crear otra instantánea del volumen.
- Cuando se crea una instantánea de un volumen con un código de producto de AWS Marketplace, dicho código se propaga en la instantánea.

9.4 Creación de instantáneas

Utilice el siguiente procedimiento para crear una instantánea desde el volumen especificado.

Para crear una instantánea con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en **Elastic Block Store**, seleccione **Snapshots (Instantáneas)**.

3. Elija **Create Snapshot (Crear instantánea)**.
4. En **Select resource type (Seleccionar tipo de recurso)**, elija **Volume (Volumen)**.
5. En **Volume (Volumen)**, seleccione el volumen.
6. (Opcional) Escriba una descripción de la instantánea.
7. (Opcional) Elija **Add Tag (Añadir etiqueta)** para añadir etiquetas a su instantánea. Para cada etiqueta, proporcione un valor y una clave de etiqueta.
8. Elija **Create Snapshot (Crear instantánea)**.

Para crear una instantánea mediante la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceso a Amazon EC2.

- create-snapshot (AWS CLI)
- New-EC2Snapshot (Herramientas de AWS para Windows PowerShell)

9.5 Creación de una instantánea de varios volúmenes

Utilice el siguiente procedimiento para crear una instantánea desde los volúmenes de una instancia.

Para crear instantáneas de varios volúmenes con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en **Elastic Block Store**, seleccione **Snapshots (Instantáneas)**.
3. Elija **Create Snapshot (Crear instantánea)**.
4. En **Select resource type (Seleccionar tipo de recurso)**, elija **Instance (Instancia)**.
5. Seleccione el ID de la instancia para la que desea crear copias de seguridad simultáneas de todos los volúmenes de EBS adjuntos. Las instantáneas de varios volúmenes admiten hasta 40 volúmenes de EBS por instancia.
6. (Opcional) Establezca **Exclude root volume (Excluir volumen raíz)**.
7. (Opcional) Active el indicador **Copy tags from volume (Copiar etiquetas del volumen)** para copiar automáticamente las etiquetas del volumen de origen en las instantáneas correspondientes. Esta opción configura los metadatos de la instantánea, como las políticas de acceso, la información adjunta y la asignación de costos, para que coincidan con el volumen de origen.
8. (Opcional) Elija **Add Tag (Añadir etiqueta)** para añadir etiquetas a su instantánea. Para cada etiqueta, proporcione un valor y una clave de etiqueta.
9. Elija **Create Snapshot (Crear instantánea)**.

Las instantáneas se administran de manera conjunta durante la creación de la instantánea. Si una de las instantáneas del conjunto de volúmenes da error, el resto de las instantáneas pasarán a presentar el estado de error en el conjunto de volúmenes. Puede monitorizar el progreso de las instantáneas con CloudWatch Events. Después de que finalice el proceso de creación de la instantánea, CloudWatch genera un evento que contiene el estado y toda la información relevante de las instantáneas de la instancia afectada.

Para crear instantáneas de varios volúmenes con la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte Acceso a Amazon EC2.

- create-snapshots (AWS CLI)
- New-EC2SnapshotBatch (Herramientas de AWS para Windows PowerShell)

10. Creación de un informe de uso y costo de AWS

Para crear un AWS Cost and Usage report, utilice la página **Informes** de la consola de Billing and Cost Management.

Para crear un AWS Cost and Usage report

1. Sign in to the Consola de administración de AWS and open the Billing and Cost Management console athttps://console.aws.amazon.com/billing/home#/.
2. En el panel de navegación, seleccione **Cost and Usage Reports (Informes de uso y costo)**.
3. Elija **Create report**.
4. En **Nombre del informe**, escriba un nombre para su informe.
5. En **Additional report details (Detalles adicionales del informe)**, seleccione **Include resource IDs (Incluir ID de recurso)** para incluir el ID de cada recurso individual en el informe.
6. En **Data refresh settings (Configuración de actualización de datos)**, seleccione si desea que el AWS Cost and Usage report se actualice cada vez que AWS aplique reembolsos, créditos o tarifas de soporte a su cuenta después de finalizada la factura. Cuando se actualiza un informe, se carga uno nuevo en Amazon S3.

   nota

Los informes de facturación detallados (DBR) no se actualizan automáticamente, tanto si selecciona **Data refresh settings (Configuración de actualización de datos)** como si no. Para actualizar un DBR, abra una incidencia de soporte técnico. Para obtener más información, consulte Cómo ponerse en contacto con el servicio de atención al cliente en referencia a su factura.

7. Seleccione **Siguiente**.
8. En **S3 bucket (Bucket de S3)**, seleccione **Configure (Configuración)**.
9. En el cuadro de diálogo **Configure S3 Bucket (Configurar bucket de S3)**, realice una de las acciones siguientes:
    - Seleccione un bucket existente de la lista desplegable y elija **Siguiente**.
    - Escriba un nombre de bucket y la región en la que desee crear un nuevo bucket y elija **Siguiente**.
10. Seleccione **I have confirmed that this policy is correct (He confirmado que esta política es correcta)** y elija **Save (Guardar)**.
11. En **Report path prefix (Prefijo de ruta de informe)**, escriba el prefijo de la ruta de informe que desee anexar al nombre del informe.

    Este paso es opcional para Amazon Redshift o Amazon QuickSight, pero es obligatorio para Amazon Athena.

    Si no especifica un prefijo, el prefijo predeterminada será el nombre que especificó para la informe en el paso 4 y el intervalo de fechas del informe en el siguiente formato:

    ```
    /report-name/date-range/
    ```

12. En **Time granularity (Grado de detalle de tiempo)**, seleccione **Por hora** si desea que los conceptos del informe se añadan hora a hora. Por el contrario, si desea que las partidas del informe se añadan por días, seleccione **A diario**.
13. En **Report versioning (Control de versiones de informe)**, elija si desea que cada versión del informe sobrescriba la versión anterior del mismo o que se facilite además de las versiones anteriores.
14. En **Enable report data integration for (Habilitar la integración de datos de informe para)**, seleccione si desea cargar el AWS Cost and Usage report de Amazon Redshift, Amazon QuickSight o Amazon Athena. El informe está comprimido en los siguientes formatos:
    - **Amazon Redshift o Amazon QuickSight**: compresión .gz
    - **Athena**: compresión Parquet
15. Seleccione **Siguiente**.

16. Tras terminar de revisar la configuración de su informe, elija **Review and Complete**.

nota

AWS puede tardar hasta 24 horas en comenzar a suministrar informes a su bucket de Amazon S3. Una vez que se inicia la entrega, AWS actualiza los archivos del AWS Cost and Usage report al menos una vez al día.